แนวทางการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ขององค์กรในยุคดิจิทัล

น.ส.ชรินทร์ทิพย์ ปั้นสุวรรณ

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาศิลปศาสตรดุษฎีบัณฑิต
สาขาวิชาอาชญาวิทยาและงานยุติธรรม ภาควิชาสังคมวิทยาและมานุษยวิทยา
คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2565

Guidelines on Corporate Governance for Responding to Cybersecurity Threats in the Digital Age

Miss Charinthip Pansuwan

A Dissertation Submitted in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy in Criminology and Criminal Justice
Department of Sociology and Anthropology
FACULTY OF POLITICAL SCIENCE
Chulalongkorn University
Academic Year 2022

หัวข้อวิทยานิพนธ์	แนวทางการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ขององค์กรในยุคดิจิทัล
โดย	น.ส.ชรินทร์ทิพย์ ปั้นสุวรรณ
สาขาวิชา	อาชญาวิทยาและงานยุติธรรม
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	รองศาสตราจารย์ ดร.สุมนทิพย์ จิตสว่าง

คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาศิลปศาสตรดุษฎีบัณฑิต

---------- คณบดีคณะรัฐศาสตร์
(รองศาสตราจารย์ ดร.ปกรณ์ ศิริประกอบ)

คณะกรรมการสอบวิทยานิพนธ์

---------- ประธานกรรมการ
(ศาสตราจารย์ ดร.ศรีสมบัติ โชคประจักษ์ชัด)

---------- อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(รองศาสตราจารย์ ดร.สุมนทิพย์ จิตสว่าง)

---------- กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.ฐิติยา เพชรมุนี)

---------- กรรมการภายนอกมหาวิทยาลัย
(รองศาสตราจารย์วันชัย มีชาติ)

---------- กรรมการภายนอกมหาวิทยาลัย
(พลตำรวจโท ดร.พรชัย ขันตี)

ชรินทร์ทิพย์ ปั้นสุวรรณ : แนวทางการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ขององค์กรในยุคดิจิทัล. (Guidelines on Corporate Governance for Responding to Cybersecurity Threats in the Digital Age) อ.ที่ปรึกษาหลัก : รศ. ดร.สุมนทิพย์ จิตสว่าง

การวิจัยนี้มีวัตถุประสงค์เพื่อ 1) ศึกษาสถานการณ์ภัยคุกคามไซเบอร์หน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศด้านสาธารณสุขและสาธารณูปโภค 2) ศึกษาโครงสร้างการกำกับดูแล การขับเคลื่อนการบังคับใช้นโยบายและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ในการบริหารจัดการความเสี่ยง เพื่อสร้างความตระหนักและเฝ้าระวังภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ และ 3) ศึกษาแนวทางการเตรียมแผนการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์และการกำกับดูแลการบริหารจัดการที่ดีด้านเทคโนโลยีดิจิทัลในองค์กร เพื่อลดความเสี่ยงและป้องกันภัยคุกคามทางไซเบอร์ในอนาคต การศึกษาวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพโดยการศึกษาจากเอกสารและการวิจัยภาคสนามโดยการเก็บข้อมูลจากผู้ให้ข้อมูลสำคัญที่เป็นผู้ปฏิบัติงานระดับผู้บริหารและเจ้าหน้าที่ด้านความมั่นคงปลอดภัยไซเบอร์ รวมทั้งสิ้นจำนวน 22 คน เพื่ออธิบายถึงลักษณะภัยคุกคามทางไซเบอร์ตลอดจนการกำกับดูแลและรับมือภัยคุกคามทางไซเบอร์ขององค์กร

ผลการศึกษาพบว่า 1) ปัญหาภัยคุกคามทางไซเบอร์หน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศทั้งในประเทศและต่างประเทศที่กำลังทวีความรุนแรงมากขึ้น ได้แก่ โรงพยาบาล การไฟฟ้า และการประปา ส่งผลกระทบต่อความมั่นคงปลอดภัยและการให้บริการด้านสาธารณสุข ด้านสาธารณูปโภคที่สำคัญของประเทศ รวมไปถึงภาคการเงินการธนาคารและหน่วยงานด้านยุติธรรม 2) หลายหน่วยงานมีความตระหนักรู้ในการริเริ่มจัดทำนโยบาย แนวทางปฏิบัติและจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง รวมถึงการประเมินความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ 3) หน่วยงานภาครัฐมีแนวทางที่เหมาะสมในการดำเนินงานเพื่อลดแรงเสียดทานและความเสี่ยงต่างๆให้น้อยที่สุด อย่างไรก็ตาม ภาครัฐควรให้ความสำคัญและควรปรับปรุงกฎหมายไซเบอร์ให้มีการบังคับใช้และบทลงโทษที่ชัดเจน ด้วยการใช้มาตรการทางกฎหมายอาจไม่ใช่แค่เพื่อแก้ปัญหาด้านความมั่นคงปลอดภัยไซเบอร์เท่านั้น แต่ยังเสริมสร้างความตระหนักรู้และพัฒนาสิทธิรับรู้ข้อมูลข่าวสารในกระบวนการธรรมรัฐไทย

สาขาวิชา	อาชญาวิทยาและงานยุติธรรม	ลายมือชื่อนิสิต .....
ปีการศึกษา	2565	ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

6381008724 : MAJOR CRIMINOLOGY AND CRIMINAL JUSTICE
KEYWORD: Cyber Threats; Critical Information Infrastructure (CII); Cybersecurity Governance; Cyber Risk Management

Charinthip Pansuwan : Guidelines on Corporate Governance for Responding to Cybersecurity Threats in the Digital Age. Advisor: Assoc. Prof. SUMONTHIP CHITSAWANG, Ph.D.

This research aims to: 1) study cybersecurity threats to Critical Information Infrastructure (CII) in public health and public utilities; 2) study supervision structure, the enforcement of cybersecurity policies and measures in risk management to raise awareness and monitor cybersecurity threats; and 3) study guidelines on corporate governance for responding to cybersecurity threats and good digital governance in the organization to mitigate risks and prevent future possible cyber threats. This study is a qualitative research work that relies on the schemes of documentary research and field research to collect information from key informants, with 22 executive practitioners and cybersecurity officers to describe cyber threats and how to create a corporate governance for responding to cybersecurity threats.

It is found that 1) cybersecurity threats to Critical Information Infrastructure (CII) both found in domestic and international sources such as in hospitals, electricity and water supply are becoming increasingly severe affecting the security of public health, services public utilities as well as banking and justice organization; 2) many agencies are aware to take initiatives to formulate policies, practices and prioritization in cyber risk management, including risk assessments to ensure that they are at an acceptable level; and 3) government agencies have developed applicable guidelines for enterprise operations to reduce friction and risks to a minimum. However, the government should pay more attention to improving cyber laws with clear enforcement and penalties in conjunction. Legal measures that might not only solve cybersecurity problems but also raise awareness and promote the right to receive information in the Thai state justice process.

Field of Study:	Criminology and Criminal Justice	Student's Signature .....
Academic Year:	2022	Advisor's Signature .....

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้ด้วยความอนุเคราะห์จากผู้มีพระคุณหลายท่านที่ให้การสนับสนุนและจากการทุ่มเทกายและใจของผู้วิจัยตลอดระยะเวลาของการศึกษา ขอกราบขอบพระคุณคณาจารย์ทุกท่านจากภาควิชาสังคมวิทยาและมานุษยวิทยา คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ที่อบรมสั่งสอนให้วิชาความรู้และถ่ายทอดประสบการณ์อันมีค่าคุณอนันต์ให้แก่นิสิต โดยเฉพาะอย่างยิ่ง รองศาสตราจารย์ ดร.สุมนทิพย์ จิตสว่าง ผู้เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก ซึ่งได้กรุณาให้คำปรึกษาและข้อเสนอแนะในการจัดทำวิทยานิพนธ์ อีกทั้งให้กำลังใจและมีเมตตามาโดยตลอด และขอกราบขอบพระคุณคณะกรรมการสอบวิทยานิพนธ์ ได้แก่ ศาสตราจารย์ ดร.ศรีสมบัติ โชคประจักษ์ชัด รองศาสตราจารย์วันชัย มีชาติ ผู้ช่วยศาสตราจารย์ ดร.ฐิติยา เพชรมุนี และพลตำรวจโท ดร.พรชัย ขันตี ที่กรุณาให้ข้อเสนอแนะและข้อคิดเห็นที่เป็นประโยชน์ต่อการปรับปรุงแก้ไขวิทยานิพนธ์เล่มนี้ให้ครบถ้วนและสมบูรณ์มากยิ่งขึ้น

ขอกราบขอบพระคุณ ดร.นัทธี จิตสว่าง ที่เป็นผู้จุดประกายแนวคิดและความสนใจในด้านอาชญากรรมไซเบอร์สู่การต่อยอดในเส้นทางวิชาชีพ ขอขอบคุณเพื่อนๆ พี่ น้อง นิสิตสาขาอาชญาวิทยาและงานยุติธรรม ทั้งผู้ที่คอยเป็นแรงผลักดันให้ตัดสินใจเรียนต่อในระดับปริญญาดุษฎีบัณฑิต และทุกท่านที่ให้ความปรารถนาดี ให้คำแนะนำ และให้กำลังใจที่มีคุณค่าตลอดมา รวมถึงเจ้าหน้าที่ประจำหลักสูตร และผู้มีส่วนร่วมในการวิจัยทุกท่านที่ให้ความช่วยเหลือในการดำเนินการวิจัยทั้งเอกสารและข้อมูลที่เป็นประโยชน์แก่ผู้วิจัยจนสำเร็จตามเป้าหมาย

ขอกราบขอบพระคุณบิดา มารดา และครอบครัว ผู้เป็นแรงขับเคลื่อนและสนับสนุนทุกความสำเร็จในชีวิต ขอขอบคุณผู้บังคับบัญชาและเพื่อนร่วมงานทุกท่านที่สนับสนุนโอกาสทางการศึกษาและให้ความสะดวกตลอดระยะเวลาของการศึกษาวิจัยจนสำเร็จลุล่วงมาได้ด้วยดี

สุดท้ายนี้ ขอขอบคุณตัวเองที่แม้เผชิญกับอุปสรรคนานัปการ แต่สามารถผ่านมาได้ด้วยความพยายามและอดทนอยู่เสมอ และผู้วิจัยหวังเป็นอย่างยิ่งว่า วิทยานิพนธ์ฉบับนี้จะเป็นประโยชน์ต่อการศึกษาให้กับผู้ที่สนใจและหน่วยงานที่เกี่ยวข้องเพื่อเป็นแนวทางในการกำกับดูแล การรับมือ การเฝ้าระวังและสร้างความตระหนักรู้ด้านภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ไม่มากก็น้อย

ชรินทร์ทิพย์ ปั้นสุวรรณ

สารบัญ

หน้า

สารบัญตาราง

สารบัญภาพ

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญของปัญหา

วิวัฒนาการความก้าวหน้าทางเทคโนโลยีสารสนเทศและการสื่อสารจากอดีตสู่ยุคปัจจุบัน มีประโยชน์ต่อการพัฒนาประเทศให้เจริญก้าวหน้า โดยเป็นเรื่องที่เกี่ยวกับความเป็นอยู่ของสังคมสมัยใหม่ ก่อให้เกิดการเปลี่ยนแปลงวิถีชีวิตรวมถึงกลายเป็นสิ่งที่สำคัญและจำเป็นในการปฏิบัติงานของทุกองค์กร จนกล่าวได้ว่า โลกเข้าสู่สังคมฐานความรู้ (Knowledge-based Society) ที่มีการเชื่อมโยงข้อมูลเป็นระบบเครือข่าย โดยเฉพาะอย่างยิ่งเครือข่ายอินเตอร์เน็ตได้ถูกนำมาใช้อย่างแพร่หลายในทุกบริบทของสังคม ผลจากการพัฒนาด้านวิทยาศาสตร์และเทคโนโลยีหลายทศวรรษที่ผ่านมา ทำให้เกิดการปฏิวัติสารสนเทศ (Information Revolution) สู่การพัฒนาสาขาคอมพิวเตอร์และการติดต่อสื่อสารอย่างก้าวกระโดดจนก่อให้เกิดพื้นที่มิติใหม่ที่เรียกว่า “โลกไซเบอร์” (Cyberspace) ด้วยเหตุนี้ ความมั่นคงแห่งชาติ (National Security) จึงได้รับผลกระทบจากการปฏิวัติและปรากฏการณ์นี้โดยตรง เห็นได้จากมีผู้กล่าวถึง “ความมั่นคงปลอดภัยด้านไซเบอร์” (Cyber Security) ในบริบทความมั่นคงแห่งชาติมากขึ้น ด้วยคุณลักษณะของโลกไซเบอร์ ความล่อแหลมที่มีอยู่ภายใน ภัยคุกคามที่เป็นไปได้ รวมถึงประเด็นที่เกี่ยวข้องกับการป้องกัน (Defense) การยับยั้ง (Deterrence) และการโจมตี (Attack) ในโลกไซเบอร์มากขึ้น (Satter, 2017) แม้ว่าในปัจจุบันยังไม่มีกลไกทางกฎหมายระหว่างประเทศใดที่จะสามารถระบุและควบคุมความสัมพันธ์ระหว่างรัฐในโลกไซเบอร์นี้ได้ ดังนั้น ประเทศไทยรวมถึงนานาอารยะประเทศยังคงต้องค้นหารูปแบบและวิธีการที่เหมาะสมในการจัดการกับภัยคุกคามนี้อย่างต่อเนื่องจนถึงปัจจุบัน

ทว่า โลกไซเบอร์มักจะมาพร้อมกับภัยคุกคามที่มีจำนวนผู้ที่ตกเป็นเหยื่อ (Victims) จากการถูกโจมตีหรือจากภัยคุกคามเหล่านั้นเพิ่มขึ้นอย่างรวดเร็ว จนกลายเป็นปัญหาสังคมที่มีความซับซ้อน ก่อให้เกิดอาชญากรรมไซเบอร์ (Cyber Crime) และอาชญากรรมอื่น ๆ ที่เชื่อมโยงออกไปไม่จบไม่สิ้น การโจมตีบนโลกไซเบอร์ถูกออกแบบมาเพื่อสร้างความเสียหายในการแสวงหาผลประโยชน์จากการคุกคามเป็นหลัก ซึ่งรูปแบบการโจมตีที่หลากหลายบวกกับการพัฒนาของเทคโนโลยีขั้นสูงอย่างต่อเนื่องไม่แตกต่างกับระบบรักษาความปลอดภัย (Security System) และมีไว้เพื่อป้องกันภัยคุกคาม

จากผู้ที่ประสงค์ร้ายต่อธุรกิจข้อมูลที่เป็นความลับขององค์กรหรือข้อมูลส่วนตัวของบุคคลทั่วไปที่องค์กรมีอยู่ รวมไปถึงข้อมูลในเครื่องคอมพิวเตอร์ส่วนบุคคลจากผู้ที่ต้องการคุกคามผู้ใช้คอมพิวเตอร์บนโลกอินเตอร์เน็ตหรือจากระบบรักษาความปลอดภัยในเครื่องคอมพิวเตอร์เอง การโจมตีทางไซเบอร์ (Cyber Attack) ได้เน้นการกำหนดเป้าหมายอย่างชัดเจน โดยจะสร้างเป้าหมายเฉพาะบุคคลและองค์กร ทั้งนี้การขยายตัวของการโจมตีทางไซเบอร์ทั่วโลกเกิดขึ้นอย่างรวดเร็ว บ่อยครั้ง และรุนแรง เรื่องราวของภัยคุกคามในโลกไซเบอร์แต่ละประเภท จะมีลักษณะการโจมตีเป็นของตัวเอง ถึงแม้อาจจะมีความคล้ายคลึงกันบ้าง แต่หากจะทำความเข้าใจเกี่ยวกับ “ภัยคุกคาม” (Threat) เหล่านี้มากเพียงใด ก็อาจไม่มากพอ เพราะสิ่งเหล่านี้พยายามหา “ช่องโหว่” (Vulnerability) หรือความหละหลวมที่เป็นความอ่อนแอของระบบคอมพิวเตอร์ หรือระบบเครือข่ายที่เปิดโอกาสให้สิ่งที่เป็นภัยคุกคามสามารถเข้าถึงสารสนเทศในระบบได้ นำไปสู่ความเสียหายต่อข้อมูลสารสนเทศ

ประเทศไทยเป็นประเทศหนึ่งที่กำลังประสบกับปัญหาภัยคุกคามทางไซเบอร์ที่เข้ามาก่อกวนและสร้างความเสียหายให้กับประเทศมาแล้วไม่น้อย หากมองถึงภัยคุกคามที่เกิดขึ้นในช่วง 5 ปีที่ผ่านมาจากสถิติภัยคุกคาม ประจำปี พ.ศ. 2560 – 2564 ที่มีการจำแนกตามประเภทภัยคุกคาม มีดังนี้

ตารางที่ 1 สถิติภัยคุกคามประจำปี 2560-2564 (Incident Report Statistics 2560 - 2564)

ประเภทภัยคุกคาม / ปี	**2560**	**2561**	**2562**	**2563**	**2564**
เนื้อหาที่เป็นภัยคุกคาม (Abusive Content)	0	1	124	4	14
การโจมตีสภาพความพร้อมใช้งานระบบ (Availability)	540	0	79	101	5
การฉ้อโกงหลอกลวง (Fraud)	841	929	912	576	212
ความพยายามรวบรวมข้อมูลของระบบ	8	0	60	46	248

ประเภทภัยคุกคาม / ปี	2560	2561	2562	2563	2564
(Information Gathering)					
การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต (Information Security)	68	18	165	46	30
ความพยายามจะบุกรุกเข้าระบบ (Intrusion Attempts)	939	1102	467	145	224
การบุกรุกระบบได้สำเร็จ (Intrusions)	570	335	218	173	183
การโจมตีด้วยชุดคำสั่งไม่พึงประสงค์ (Malicious Code)	271	127	436	687	479
ช่องโหว่ (Vulnerability)	0	0	0	471	674
ภัยคุกคามอื่นๆ นอกเหนือจากที่กำหนดไว้ข้างต้น (Other)	0	8	9	1	0
รวม	3237	2520	2470	2250	2069

ที่มา: สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2565

จากตารางที่ 1 จะเห็นได้ว่าสถิติภัยคุกคามตลอดระยะเวลา 5 ปี จำนวนตัวเลขของภัยคุกคามแต่ละประเภทมีความผันผวน จากการสังเกตพบว่า ในปี พ.ศ. 2564 ภัยคุกคามที่เกิดขึ้นมากที่สุดคือภัยคุกคามประเภทช่องโหว่ หรือ Vulnerability จำนวนรวมทั้งสิ้น 674 ครั้ง การเกิดภัยคุกคาม

ประเภทนี้ค่อนข้างสูงเมื่อเทียบกับภัยคุกคามประเภทอื่น ๆ และยังเป็นปัญหาที่สำคัญที่หลายธุรกิจองค์กรในประเทศไทยยังคงเฝ้าระวัง เนื่องด้วยจุดอ่อนหรือช่องโหว่ของโปรแกรม ระบบ หรือเครือข่ายมีความแตกต่างกัน การปรับเปลี่ยนรูปแบบการโจมตีไปตามช่องโหว่ที่เกิดขึ้น เพื่อแสวงหาผลประโยชน์จากช่องโหว่ของซอฟต์แวร์ (Software) ที่ผู้พัฒนาซอฟต์แวร์ยังไม่เคยประสบพบเจอ แต่ผู้ที่ค้นพบช่องโหว่ก่อน คือ นักเจาะระบบ หรือ แฮกเกอร์ (Hacker) ซึ่งการโจมตีช่องโหว่ในลักษณะดังกล่าวเรียกว่า “Zero-day” โดยแฮกเกอร์จะสร้างโค้ดใหม่ขึ้นมาหรือเรียกกันว่า Exploit Code ที่ถูกใช้เป็นใบเบิกทางในการทำอาชญากรรมไซเบอร์ได้หลากหลายวิธี เช่น ลงมือด้วยตนเอง ส่งมัลแวร์ไปบุกรุก สร้างฐานบอตเน็ต (Botnet) หรือนำช่องโหว่ไปวางจำหน่ายบนเว็บมืด (Dark Web) เมื่อช่องโหว่เริ่มเป็นที่รู้จัก ผู้พัฒนาจะพยายามหาทางปิดช่องโหว่เพื่อหยุดการโจมตี อย่างไรก็ตาม การปิดช่องโหว่ไม่ใช่เรื่องง่าย เพราะจำเป็นต้องใช้เวลาค้นคว้าว่า การโจมตีที่เกิดขึ้นได้เพราะช่องโหว่อะไร มีองค์ประกอบอะไรที่เกี่ยวข้องบ้าง ซึ่งอาจต้องใช้ระยะเวลานานกว่าที่นักพัฒนาจะสามารถพัฒนาซอฟต์แวร์หรือโปรแกรมคอมพิวเตอร์ ที่ถูกเขียนออกมาเพื่อซ่อมแซมหรือแก้ไขจุดบกพร่องของซอฟต์แวร์เวอร์ชั่นเดิมที่เรียกว่า “แพทช์” (Patch) ได้สำเร็จ และที่น่าเป็นกังวลคือ ไม่ใช่ว่าผู้ใช้ทุกคนที่จะยอมอัพเดตแพทช์ (Update Patch) เพื่อปิดช่องโหว่ อาจด้วยความไม่รู้หรือไม่ต้องการอัพเดต ซึ่งขึ้นอยู่กับความสนใจใคร่รู้ของแต่ละบุคคล ความตระหนักรู้ของผู้บริหารและบุคลากรในการเฝ้าระวังภัยคุกคามทางไซเบอร์ให้กับองค์กร

การแสวงหาผลประโยชน์จากการแฮกช่องโหว่ของโปรแกรมควบคุมเครือข่ายและการทำงานของระบบ (Botnet) รวมถึงการแพร่ระบาดโปรแกรมไม่พึงประสงค์ (Malware) เพื่อสร้างความเสียหายต่อระบบ ทำให้ป้องกันได้ยาก ดังนั้น การกระทำที่เป็นอันตรายต่อระบบเครือข่ายเหล่านี้ ถือเป็นภัยคุกคามรูปแบบใหม่ที่เรียกว่า “ภัยคุกคามด้านไซเบอร์”(Cyber Threats) ซึ่งอาจเกิดจากการกระทำในระดับบุคคล องค์กร หรือรัฐได้ ถือเป็นภัยคุกคามใหญ่หลวงต่อผลประโยชน์ทางเศรษฐกิจตลอดจนความมั่นคงของประเทศ นอกจากนี้ ภัยคุกคามทางไซเบอร์ยังรวมไปถึงการโจมตีในระดับประเทศ กล่าวคือ การโจมตีประเทศอื่นผ่านการโจรกรรมข้อมูลโดยมีวัตถุประสงค์เพื่อสืบเสาะข้อมูลลับ หรือเพื่อเข้ามาต่อรอง ประนีประนอม และควบคุมฝ่ายตรงข้ามกับรัฐบาล (นัทธมน เพชรกล้า, 2564) โดยเฉพาะอย่างยิ่ง การแฮกระบบของหน่วยงานโครงสร้างพื้นฐานที่สำคัญด้านสาธารณสุขและด้านสาธารณูปโภค ที่ทำให้การบริการต่างๆ หยุดชะงัก หรือไม่สามารถใช้งานได้

ส่งผลกระทบในวงกว้างและสร้างความเดือดร้อนให้กับประชาชน ดังเช่น สถานการณ์ภัยคุกคามไซเบอร์ในต่างประเทศที่เคยเกิดขึ้นมาแล้วเมื่อวันที่ 27 เมษายน พ.ศ. 2550 ประเทศเอสโตเนียซึ่งเป็นประเทศเล็กๆทางตอนเหนือของยุโรป ต้องเผชิญกับปัญหาการโจมตีทางไซเบอร์ หลังธนาคาร สื่อ และหน่วยงานราชการหลายแห่งโดนแฮกจนเกิดความปั่นป่วนกว่า 22 วัน ซึ่งถูกโจมตีด้วยระบบคำสั่ง ดีดีโอเอส (Distribute Denial of Service: DDOS) หรือการโจมตีเซิร์ฟเวอร์ด้วยการระดมคำสั่ง ส่งผลให้การบริการโดยโครงข่ายอินเทอร์เน็ตทั้งหมดถูกระงับ ประชาชนเอสโตเนียไม่สามารถใช้บริการธนาคารออนไลน์, เว็บไซต์สื่อ หรือบริการอิเล็กทรอนิกส์ของรัฐบาลได้ สาเหตุมาจากความขัดแย้งกับประเทศรัสเซีย กรณีที่เอสโตเนียตัดสินใจย้ายอนุสรณ์สถานสงครามยุคโซเวียตออกจากเมืองหลวง แม้รัสเซียจะไม่เคยยอมรับว่าเป็นผู้อยู่เบื้องหลังการโจมตี แต่เอสโตเนียปักใจเชื่อเช่นนั้น และเรียกการโจมตีนี้ว่า “สงครามไซเบอร์ (Cyber Warfare)” ที่สร้างผลกระทบความมั่นคงของประเทศได้ไม่แพ้สงครามที่ใช้อาวุธทำลายล้าง นับจากนั้น เอสโตเนียจึงทุ่มสรรพกำลังและงบประมาณเพื่อสร้างระบบความมั่นคงปลอดภัยไซเบอร์ (Cyber Security System) อย่างจริงจัง (ประชาชาติธุรกิจ, 2564)

ในขณะที่ประเทศลิทัวเนียซึ่งเป็นประเทศที่พัฒนาแล้ว และมีระบบเศรษฐกิจก้าวหน้ารายได้สูงอีกทั้งมีดัชนีการพัฒนามนุษย์อยู่ในระดับสูงมากของประเทศในกลุ่มฝั่งยุโรปก็เคยเผชิญกับปัญหาการโจมตีทางไซเบอร์ด้วยเช่นเดียวกันจากกลุ่มแฮกเกอร์รัสเซียที่มีชื่อว่า Killnet โดยการโจมตีครั้งนี้เกิดจากการที่ลิทัวเนียได้มีการปิดกั้นการส่งสินค้าบางส่วนไปยังเขตคาลินินกราดของรัสเซีย ซึ่งอยู่ระหว่างพื้นที่ประเทศโปแลนด์และลิทัวเนีย เป็นการบริการด้วยการส่งการเชื่อมต่อหรือคำขอในการเข้าถึงข้อมูลจำนวนมาก ๆ พร้อม ๆ กัน เข้าโจมตีด้วยคำสั่งชุดเดียวกันกับประเทศเอสโตเนียคือ Distributed Denial of Service: DDOS แต่เป็นวิธีการโจมตีบนเว็บไซต์ โดยแฮกเกอร์พุ่งเป้าไปที่ Secure Data Transfer Network หรือเรียกว่า “เครือข่ายการโอนข้อมูล” ซึ่งเป็นเครือข่ายสื่อสารสำหรับเจ้าหน้าที่รัฐบาล และเป็นหน่วยงานที่สร้างขึ้นเพื่อต่อต้านสงครามและวิกฤติอื่นๆของประเทศ (ไทยรัฐออนไลน์, 2565)

สถานการณ์ภัยคุกคามไซเบอร์ในในกลุ่มประเทศอาเซียนอย่างประเทศสิงค์โปร์ ก็เคยได้รับบทเรียนจากการถูกโจมตีทางไซเบอร์ จากกรณีเรื่องที่ “สิงคโปร์ เฮลธ์ เซอร์วิส” ซึ่งเรียกกันสั้นๆ ว่า “สิงค์เฮลธ์” กลุ่มธุรกิจการแพทย์ที่ใหญ่ที่สุดของประเทศ ถูกแฮคเกอร์มือดีเจาะระบบเข้าลักลอบตรวจสอบและอาจก็อปปี้บันทึกข้อมูลของผู้ป่วยไปมากถึง 1.5 ล้าน เมื่อวันที่ 27 มิถุนายน พ.ศ. 2561

โดยคนร้ายให้ความสนใจเป็นพิเศษต่อบันทึกทางการแพทย์ของ ลี เซียนหลุง นายกรัฐมนตรีสิงคโปร์ ถึงขนาดพยายามพุ่งเป้าเข้าไปที่บันทึกข้อมูลชุดนี้ซ้ำแล้วซ้ำอีก ข้อที่น่าสนใจก็คือ แฮคเกอร์ ไม่ได้สนใจข้อมูลส่วนอื่นๆ ไม่ว่าจะเป็นบันทึกการวินิจฉัยโรค หรือบันทึกผลการตรวจสอบโรค หรือคำแนะนำของแพทย์ แต่มุ่งไปที่ข้อมูลส่วนตัวของผู้ป่วยแต่ละรายเท่านั้น ในจำนวนผู้ป่วย 1.5 ล้านรายที่ถูกฉกข้อมูลส่วนตัวไปนี้ ส่วนหนึ่งคือราว 160,000 รายเป็นผู้ป่วยนอกกิจการของ สิงค์เฮลธ์ นั้นมีโรงพยาบาลอยู่ในเครือ 2 โรงพยาบาล มีสถานพยาบาลเฉพาะทางอีก 5 ศูนย์ รองรับผู้ป่วยจากทั่วโลก นับเป็นบันทึกการลักลอบเจาะระบบคอมพิวเตอร์ครั้งใหญ่ที่สุด ร้ายแรงที่สุด เท่าที่สิงคโปร์เคยเผชิญมา (ไพรัตน์ พงศ์พานิชย์, 2561)

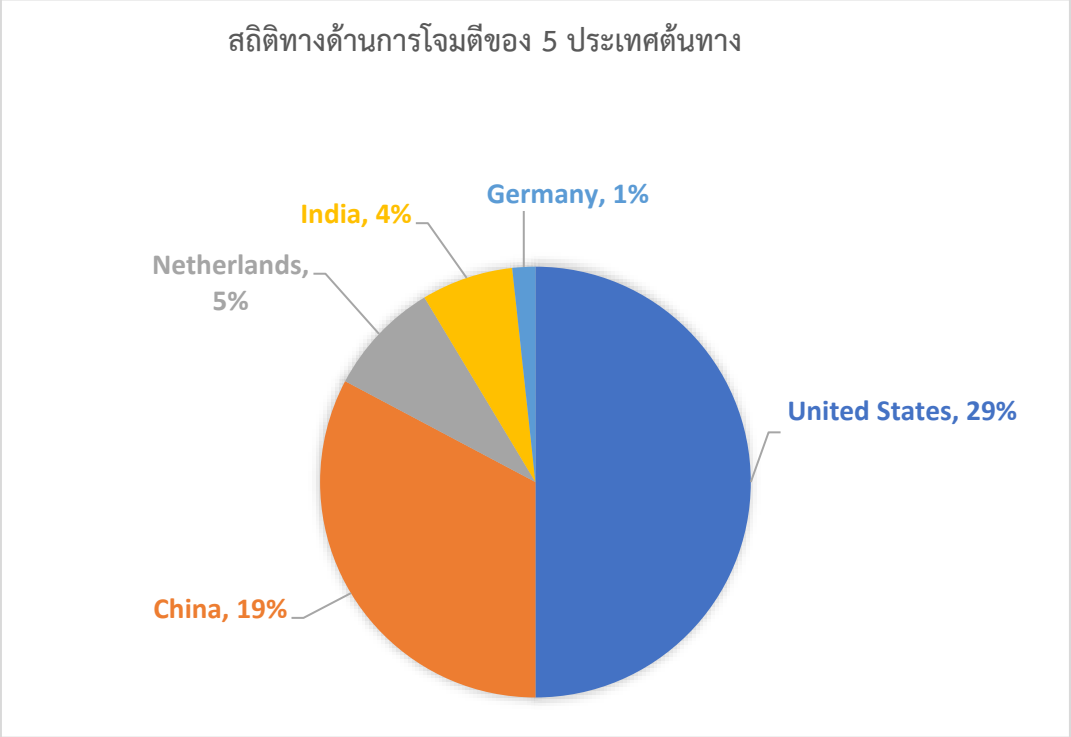
แม้กระทั่งประเทศไทยเอง สถานการณ์ภัยคุกคามทางไซเบอร์ที่เห็นได้ชัดเจนเกิดขึ้นเมื่อเดือนกันยายน ปี พ.ศ. 2563 โรงพยาบาลสระบุรีโดนแฮกข้อมูล ทำให้แพทย์และพยาบาลทำงานล่าช้าลง เนื่องจากไม่สามารถเข้าถึงข้อมูลคนไข้ได้ จากการสอบเบื้องต้นพบว่า มีสาเหตุมาจากระบบคอมพิวเตอร์ของโรงพยาบาลถูกมัลแวร์โจมตีทำให้ไม่สามารถเข้าถึงข้อมูลผู้ป่วยที่อยู่ในเซิร์ฟเวอร์ โดยแฮกเกอร์ใช้มัลแวร์ชนิด Ransomware เข้ารหัสข้อมูลคนไข้ในโรงพยาบาลสระบุรีทั้งหมด และได้เรียกค่าไถ่เป็น Bitcoin จำนวนทั้งหมดถึง 200,000 BTC หรือคิดเป็นเงินจำนวน 63,000 ล้านบาท ข้อมูลที่โดนเข้ารหัสนั้นล้วนเป็นข้อมูลคนไข้ในระบบซึ่งเป็นข้อมูลที่จำเป็นต่อการรักษาและวินิจฉัยโรค และแม้ว่าทางโรงพยาบาลได้มีการกู้คืนข้อมูลบางส่วนไว้บ้างแล้ว แต่ข้อมูลเหล่านั้นกลับเป็นข้อมูลเก่าตั้งแต่ปี พ.ศ. 2558 ทำให้ไม่สามารถนำมาใช้ได้ (เดลินิวส์, 2563) นอกจากนี้ จากข้อมูลข่าวสารในปี พ.ศ. 2564 พบว่า เกิดเหตุการณ์โรงพยาบาลเพชรบูรณ์โดนแฮกข้อมูลคนไข้กว่า 10,000 รายถูกนำไปขายบนเว็บไซต์แห่งหนึ่งในราคา 500 ดอลลาร์ หรือประมาณ 16,400 บาท โดยจากการให้ข้อมูลของรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กล่าวไว้ว่า โรงพยาบาลเพชรบูรณ์ได้พัฒนาเว็บแอปพลิเคชันขึ้นมาใช้เองเป็นการภายใน สำหรับติดตามการเข้าใช้บริการของผู้ป่วยและการทำงานของแพทย์ สาเหตุอาจเกิดจากระบบรักษาความปลอดภัยไม่ได้มาตรฐาน เมื่อเชื่อมต่อกับอินเตอร์เน็ตจึงถูกแฮกเกอร์โจมตี และส่วนใหญ่เป็นข้อมูลเบื้องต้นเกี่ยวกับผู้ป่วยเท่านั้น ได้แก่ ข้อมูลรายชื่อเวชระเบียนผู้ป่วยใน 10,095 ราย ใช้ในการตรวจสอบระบบเวชระเบียน (ไม่มีรายละเอียดการดูแลรักษา) ข้อมูลรายชื่อผู้ป่วยนอกที่นัดรับการรักษา ประมาณ 7,000 ราย ข้อมูลตารางเวรแพทย์ มีเลข 13 หลักของแพทย์ผู้รักษา 39 ราย เพื่อใช้ในการเข้าถึงฐานข้อมูล ข้อมูลรายชื่อผู้ป่วยในการ

คำนวณค่าใช้จ่ายในการผ่าตัด 692 ราย และข้อมูลผู้ป่วยโรงพยาบาลสนาม 795 ราย (ผู้จัดการออนไลน์, 2564) จากสถานการณ์ดังที่กล่าวมา ถือเป็นภัยคุกคามทางไซเบอร์ หรือ อาชญากรรมไซเบอร์ที่เป็นความผิดทางอาญาดำเนินการโดยใช้คอมพิวเตอร์ หรือ อินเทอร์เน็ตเป็นเครื่องมือ ในขณะที่บริษัทใหญ่ หน่วยงานเอกชน หรือ รัฐบาลอาจไม่ใช่เป้าหมายกลุ่มเดียวอีกต่อไป เมื่อประชาชนทั่วไปต่างก็ได้รับผลกระทบของการคุกคามเหล่านี้เช่นเดียวกัน อีกทั้งยังมีเป้าหมายไม่เลือกกลุ่มสร้างความสูญเสียเป็นวงกว้าง

การโจมตีทางไซเบอร์นับวันจะมีการพัฒนารูปแบบในการโจมตีใหม่ๆ ที่ซอฟต์แวร์ด้านความมั่นคงปลอดภัยไซเบอร์ที่มีอยู่อาจไม่สามารถป้องกันได้ จากรายงานของ Crowdstrike เรื่องดัชนีชี้วัดอาชญากรรมไซเบอร์ (eCrime) ในช่วงปลายปี พ.ศ.2563 ถึงกุมภาพันธ์ พ.ศ.2564 พบว่าอัตราความถี่ของอาชญากรรมไซเบอร์จากทั่วโลกเพิ่มขึ้นถึงร้อยละ 123.94 (Crowdstrike, 2021) แสดงให้เห็นว่าแนวโน้มของการก่ออาชญากรรมไซเบอร์กำลังพุ่งสูงขึ้นอย่างต่อเนื่อง ก่อให้เกิดความสูญเสียทั้งส่วนบุคคลและทางธุรกิจจากความเสียหายจากการทำลายข้อมูล การสูญเสียประสิทธิภาพจากการทำงาน การโจรกรรมทรัพย์สินทางปัญญา การขโมยข้อมูลส่วนบุคคล การทุจริต การหยุดชะงักทางธุรกิจภายหลังจากการถูกโจมตี การกู้ข้อมูลและฟื้นฟูระบบ และการคุกคามต่อชื่อเสียงและความไว้วางใจ ดังนั้นการเรียนรู้ ปรับตัว เพื่อรับมือ แก้ไข และป้องกัน จึงถือเป็นส่วนสำคัญที่จะทำให้ธุรกิจองค์กรหรือหน่วยงานภาครัฐปลอดภัยจากการจู่โจมบนโลกไซเบอร์

อย่างไรก็ตาม ภัยคุกคามความมั่นคงปลอดภัยต่าง ๆ ได้เกิดขึ้นมากมายไม่ว่าจะเป็นการโจมตีทางไซเบอร์ ข้อมูลลูกค้าและข้อมูลองค์กรหลุดสู่สาธารณะ (Data Breach) รวมถึงการละเมิดความเป็นส่วนตัว หรือแม้แต่การเจาะระบบฐานข้อมูล การสืบเสาะหาช่องโหว่ Zero Day ที่เกิดขึ้นแทบทุกวัน คงจะปฏิเสธไม่ได้ว่าส่วนหนึ่งนั้นมาจากสถานการณ์โรคระบาดอย่างโรคติดเชื้อไวรัสโคโรนา 2019 (COVID-19) ที่ได้เข้ามาเปลี่ยนแปลงวิถีชีวิต รวมถึงรูปแบบในการปฏิบัติงานหลายองค์กร ทำให้เกิดการทำงานจากระยะไกล (Remote work) เพิ่มมากขึ้น ส่งผลให้ผู้คนใช้เวลาอยู่บนโลกออนไลน์นานขึ้น และอาจรวมไปถึงการปรับตัวตามเทรนด์ (Trend) หรือแนวโน้มทางเทคโนโลยีที่เปลี่ยนไปของเหล่าอาชญากรไซเบอร์ด้วยเช่นเดียวกัน ซึ่งบริษัทโทรคมนาคมแห่งชาติ จำกัด (มหาชน) หรือ National Telecom Public Company Limited : NT ผู้ให้บริการด้านความปลอดภัยระบบเทคโนโลยีสารสนเทศ ได้รวบรวมข้อมูลสถิติภัยคุกคามที่อาจส่งผลกระทบกับระบบ IT จากศูนย์

ปฏิบัติการ Cyber Security Operation Center (CSOC) ของ NT Cyfence ในปี พ.ศ.2564 ที่ผ่านมา โดยแบ่งตามอันดับด้านการโจมตีดังนี้



ภาพที่ 1 สถิติทางด้านการโจมตีของ 5 ประเทศต้นทาง
ที่มา: บริษัทโทรคมนาคมแห่งชาติ จำกัด (มหาชน), 2565

จากภาพที่ 1 พบว่าสถิติทางด้านการโจมตี 5 ประเทศต้นทาง อันดับที่ 1 ในปัจจุบันยังคงมาจากประเทศสหรัฐอเมริกา แต่มีแนวโน้มลดลงจากปีที่ผ่านมาและพบประเทศที่ติดอับดับเข้ามาใหม่คือประเทศอินเดีย เป็นที่น่าสังเกตว่าฐานการโจมตีนั้นเริ่มหลากหลายและขยายตัวกว้างขวางมากยิ่งขึ้น

ต่อมาระบบเศรษฐกิจโลกได้ก้าวเข้าสู่ภาวะเศรษฐกิจดิจิทัล นับเป็นการปฏิวัติทางดิจิทัล (Digital Revolution) ที่ส่งผลให้องค์กรส่วนใหญ่ในโลก ต่างเข้าสู่การเปลี่ยนผ่านให้อยู่ในรูปขององค์กรดิจิทัล (Digital Transformation) หลายประเทศมีการนำเทคโนโลยีปัญญาประดิษฐ์ (AI) และการใช้การเรียนรู้ของเครื่อง (Machine Learning) มาใช้งานด้านความมั่นคงปลอดภัยอย่างเป็นรูปธรรมทั้งหน่วยงานภาครัฐและภาคเอกชน เพื่อระบุภัยคุกคามที่อาจจะเกิดได้เร็วขึ้น นอกจากนี้ AI และ Machine Learning ยังสามารถที่จะระบุภัยคุกคามตามประเภทได้ ในขณะที่การแพร่หลายของ

อุปกรณ์ IoT (Internet of Things) ยังคงเป็นปัญหาใหญ่ เนื่องด้วยยากต่อการบังคับใช้นโยบายด้านความมั่นคงปลอดภัยและด้วยจำนวนอุปกรณ์อันมหาศาล ทำให้แฮกเกอร์ (Hacker) มีช่องทางในการโจมตีเข้าระบบเครือข่ายมากยิ่งขึ้น การเตรียมความพร้อมขององค์กรในการรับมือกับภัยคุกคามทางไซเบอร์นั้น จึงเป็นสิ่งที่องค์กรสามารถดำเนินการได้ ซึ่งควรเริ่มตั้งแต่ระดับนโยบายแล้วถ่ายทอดลงสู่ระดับปฏิบัติการ การที่องค์กรมีทักษะที่ดีในการรับมือ แก้ไข และเยียวยาจากเหตุการณ์ทางไซเบอร์ หรือที่เรียกว่าการคืนสภาพได้ทางไซเบอร์ (Cyber resilience) เป็นสภาวะที่องค์กรมีความทนทานซึ่งประกอบด้วยความคล่องตัว (Agility) และความทนทาน (Robustness) ต่อภัยคุกคามทางไซเบอร์ จะช่วยให้องค์กรสามารถป้องกัน ตรวจจับ และตอบสนองต่อการถูกโจมตีทางไซเบอร์ได้อย่างรวดเร็ว และพบว่าหลายองค์กรเริ่มมีความตระหนักเกี่ยวกับความปลอดภัยของเทคโนโลยีดิจิทัล และเริ่มมีการนำมาตรฐานความปลอดภัยระดับสากลมาใช้เป็นกรอบแนวทางกันมากขึ้น

ปัจจุบันภัยคุกคามทางไซเบอร์ในประเทศไทย มีอิทธิพลต่อความมั่นคงปลอดภัยไซเบอร์ที่เพิ่มจำนวนอย่างต่อเนื่องตามกระแสเทคโนโลยีเปลี่ยนโลก หรือ“ Disruptive Technology” และส่งผลกระทบตั้งแต่ระดับบุคคล ขยายไปยังองค์กร จนถึงระดับความมั่นคงของชาติ ที่สำคัญและน่ากังวลอย่างยิ่งสำหรับประเทศไทย คือ 1) การถูกชี้นำหรือครอบงำทางความคิดโดยไม่รู้ตัวจากเครือข่ายสังคมออนไลน์ และโทรศัพท์สมาร์ทโฟน 2) การถูกละเมิดสิทธิความเป็นส่วนตัว (Privacy) 3) การถูกขโมยข้อมูลไปใช้เพื่อวัตถุประสงค์ต่างๆโดยเฉพาะด้านพาณิชย์ และ 4) การได้รับข่าวสารลวง (Fake Information) โดยพบว่าบริษัทชั้นนำของโลกที่มีมูลค่าตามราคาตลาด (Market Capitalization) อยู่ในลำดับต้นๆ ล้วนเป็นบริษัทที่ให้บริการเครือข่ายสังคมออนไลน์ ข้อมูลข่าวสาร และการให้บริการด้านการประมวลผล จัดเก็บข้อมูล และระบบออนไลน์ต่างๆ แก่ผู้ใช้บริการทางอินเทอร์เน็ต หรือ ระบบ Cloud Services อันได้แก่ เว็บไซต์ที่ให้บริการเครือข่ายสังคมออนไลน์ Facebook YouTube Line Microsoft และ Amazon ตามลำดับ ซึ่งกลายเป็นปัญหาใหญ่ที่กำลังอุบัติขึ้นในทุกประเทศทั่วโลก ได้แก่ ปัญหา “อธิปไตยไซเบอร์” (Cyber Sovereignty) หรือ “ความเป็นเอกราชทางไซเบอร์” ของผู้คนในประเทศตลอดจนไปถึงปัญหาความมั่นคงของชาติ (National Security) ทั้งในระยะสั้นและระยะยาว ซึ่งหลายประเทศ แม้แต่ประเทศไทยเอง หลายคนยังไม่รู้ตัวด้วยซ้ำว่ากำลังถูกละเมิดในเรื่อง “อธิปไตยไซเบอร์” เนื่องจาก ปัญหาดังกล่าวถูกซ่อนอยู่ในการใช้งานสมาร์ทโฟนและอุปกรณ์สื่อสารผ่านไซเบอร์สเปซ ทำให้ผู้ให้บริการ Social Media และ Cloud รายใหญ่ที่สามารถเข้าถึงข้อมูลเชิง

ลึกได้ มีความได้เปรียบในการแข่งขันทางธุรกิจ และสามารถนำข้อมูลมาใช้ในการตลาดได้อย่างมีประสิทธิผลและประสิทธิภาพ (ปริญญา หอมอเนก, 2564)

อนึ่ง แม้ว่าประเทศไทยจะให้ความสำคัญในเรื่องความมั่นคงปลอดภัยไซเบอร์มากขึ้นตามลำดับ และได้มีการดำเนินงานของหน่วยปฏิบัติหลายหน่วยงาน เช่น การทำงานของศูนย์ประสานความมั่นคงปลอดภัยทางไซเบอร์ (The Computer Emergency Response Team) หรือไทยเซิร์ต (ThaiCERT) ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ที่ช่วยในการปกป้องและประสานการทำงานด้านความมั่นคงปลอดภัยไซเบอร์และเริ่มมีการทำงานในรูปแบบ CERT ในองค์กรที่ทำหน้าที่กำกับดูและองค์การภาคเอกชนบ้างแล้วก็ตาม มีการดำเนินงานของกองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีภายใต้สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีภายใต้สำนักงานตำรวจแห่งชาติ สำนักคดีเทคโนโลยีและสารสนเทศภายใต้กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม ส่วนตรวจสอบการกระทำความผิดทางเทคโนโลยี ศูนย์เทคโนโลยีสารสนเทศภายใต้สำนักงานป้องกันและปราบปรามการฟอกเงิน หรือธนาคารแห่งประเทศไทยแล้วก็ตาม แต่รูปแบบการทำงานดังกล่าวก็เป็นการทำงานในเชิงป้องกันและตั้งรับเมื่อมีภัยคุกคามทางไซเบอร์เท่านั้น ต่อมาได้มีแนวนโยบายระดับชาติฉบับแรกของไทยในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ คือ ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560-2564 เพื่อสร้างความเชื่อมั่นและความไว้วางใจในการใช้ไซเบอร์สเปซ (Cyberspace) และเพิ่มบทบาทของไทยในระดับภูมิภาคและระดับโลกในการลดความขัดแย้งทางไซเบอร์ระหว่างรัฐ แต่สถานการณ์ภัยคุกคามทางไซเบอร์ในประเทศไทยยังคงมีจำนวนเพิ่มขึ้นอย่างต่อเนื่อง โดยสถิติภัยคุกคามระหว่างเดือนมกราคม - กันยายน ปี พ.ศ. 2565 มีจำนวนรวมทั้งสิ้น 1,884 ครั้ง มากกว่าสถิติภัยคุกคามในปี พ.ศ. 2564 จำนวน 448 ครั้ง เมื่อเปรียบเทียบในระยะเวลาเดียวกัน (บริษัทโทรคมนาคมแห่งชาติ จำกัด (มหาชน), 2565)

ในขณะเดียวกัน ภัยที่เกิดจากมิจฉาชีพหรือผู้ไม่ประสงค์ดีใช้อินเตอร์เน็ตในการก่ออาชญากรรมและแสวงผลประโยชน์ในรูปแบบต่างๆ ภัยที่จะเกิดต่อระบบควบคุมดูแลการใช้อินเตอร์เน็ตและระบบปฏิบัติการที่เกี่ยวข้องกับโครงสร้างสาธารณูปโภคพื้นฐานที่สำคัญ ซึ่งก่อให้เกิดผลกระทบต่อการใช้ชีวิตของประชาชนและภาคธุรกิจเอกชน ทั้งในยามปกติและยามเกิดเหตุฉุกเฉิน รัฐบาลไทยเองได้เล็งเห็นถึงความสำคัญของการดูแลป้องกันและการเตรียมพร้อมในการรับมือแก้ไข

ปัญหาที่เกิดขึ้นกับระบบเครือข่ายสื่อสารและโครงสร้างพื้นฐานที่สำคัญของประเทศ จึงได้บรรจุประเด็นความมั่นคงไว้ในยุทธศาสตร์ชาติ (พ.ศ. 2561-2580) เพื่อเป็นแนวทางให้ประเทศมีแผนการดำเนินงานในการป้องกันปัญหาที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ และข้อมูลที่ได้จากอุปกรณ์และเครื่องจักรต่างๆ พร้อมกำหนดให้ทุกหน่วยงานที่เกี่ยวข้องในการป้องกันดังกล่าวดำเนินการจัดทำแผนการป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์ ซึ่งเป็นโครงการเร่งด่วน (Flagship) และต่อมาได้มีการออกพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งเป็นกลไกเฝ้าระวัง ป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ที่อาจเกิดกับระบบปฏิบัติการและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) โดยสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มีคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ “กมช.” (National Cyber Security Committee : NCSC) กำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ มีคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ หรือ “กกม.” ทำหน้าที่กำหนดแนวทางปฏิบัติของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและประสานเมื่อเผชิญเหตุได้แก่ ความมั่นคงของรัฐ บริการภาครัฐที่สำคัญ การเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม การขนส่งและโลจิสติกส์ พลังงานและสาธารณูปโภค สาธารณสุข และด้านอื่นๆ ตามที่บอร์ดกำหนดเพิ่มเติม และมีคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.) ดูแลงานด้านกิจการบริหารงานทั่วไปของสำนักงาน แต่เพราะเหตุใด หลายหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศเหล่านี้ยังตกเป็นเหยื่อของภัยคุกคามทางไซเบอร์อยู่บ่อยครั้ง แม้ว่าจะมีโครงสร้างการกำกับดูแล ยุทธศาสตร์ และนโยบายด้านความมั่นคงปลอดภัยไซเบอร์

ด้วยเหตุนี้ ผู้วิจัยจึงศึกษาการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ การประเมินความเสี่ยงในการจัดทำแผนเฝ้าระวังและรับมือภัยคุกคามทางไซเบอร์ การกำหนดกรอบทิศทาง หลักการในการบริหารจัดการเพื่อให้เกิดความมั่นคงปลอดภัยไซเบอร์และแนวปฏิบัติที่ดี (Best Practice) อย่างมีประสิทธิภาพและประสิทธิผลในระดับองค์กร ตลอดจนกระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อทำให้องค์กรปราศจากความเสี่ยง และความเสียหายจากการแฮกข้อมูล โดยเลือกศึกษาหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศด้านสาธารณสุขและสาธารณูปโภคที่มีความเสี่ยงต่อการถูก

โจมตีโดยการแฮกหรือเจาะระบบฐานข้อมูลสารสนเทศ ได้แก่ โรงพยาบาล การไฟฟ้า การประปา เพื่อนำไปวิเคราะห์เตรียมแผนการรับมือและเฝ้าระวังภัยคุกคามทางไซเบอร์ในองค์กร

1.2 โจทย์/คำถามวิจัย

1. สถานการณ์ภัยคุกคามไซเบอร์ที่เป็นการเจาะระบบฐานข้อมูลหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศด้านสาธารณสุขและด้านสาธารณูปโภคเป็นอย่างไร

2. โครงสร้างการกำกับดูแลด้านเทคโนโลยีดิจิทัลขององค์กรมีการขับเคลื่อนการบังคับใช้นโยบายและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ในการบริหารจัดการอย่างไร เพื่อสร้างความตระหนักและเฝ้าระวังภัยคุกคามความมั่นคงปลอดภัยไซเบอร์

3. หน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศด้านสาธารณสุขและด้านสาธารณูปโภคมีแนวทางการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์และการกำกับดูแลการบริหารจัดการที่ดีด้านเทคโนโลยีดิจิทัลในองค์กรอย่างไร เพื่อลดความเสี่ยงและป้องกันภัยคุกคามทางไซเบอร์ในอนาคต

1.3 วัตถุประสงค์ในการวิจัย

1. เพื่อศึกษาสถานการณ์ภัยคุกคามไซเบอร์ที่เป็นการเจาะระบบฐานข้อมูลหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศด้านสาธารณสุขและด้านสาธารณูปโภค

2. เพื่อศึกษาโครงสร้างการกำกับดูแลด้านเทคโนโลยีดิจิทัลขององค์กร การขับเคลื่อนด้วยนโยบายและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ในการบริหารจัดการ เพื่อสร้างความตระหนักและเฝ้าระวังภัยคุกคามความมั่นคงปลอดภัยไซเบอร์

3. เพื่อศึกษาแนวทางการเตรียมแผนการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์และการกำกับดูแลการบริหารจัดการที่ดีด้านเทคโนโลยีดิจิทัลในองค์กร เพื่อลดความเสี่ยงและป้องกันภัยคุกคามทางไซเบอร์ในอนาคต

1.4 ขอบเขตของการวิจัย

1.4.1 ขอบเขตด้านเนื้อหา

ศึกษาการเจาะระบบหรือการแฮก (Hack) จากสถานการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศด้านสาธารณสุขและด้านสาธารณูปโภคในประเทศ ที่ส่งผลกระทบต่อองค์กรและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง อันนำไปสู่ปัญหาอาชญากรรมไซเบอร์ (Cybercrime) ศึกษาโครงสร้างการกำกับดูแล การขับเคลื่อนนโยบายและมาตรการรักษา

ความมั่นคงปลอดภัยไซเบอร์ ตลอดจนแนวทางการแก้ไขปัญหา การป้องกัน และความตระหนักรู้ของบุคลากรหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ หน่วยงานควบคุมและกำกับดูแล และหน่วยงานป้องกันและปราบปราม รวมไปถึงศึกษาข้อเสนอแนะของผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อนำมาวิเคราะห์หาแนวทางการกำกับดูแลการรับมือภัยคุกคามทางไซเบอร์ที่เหมาะสมกับองค์กร และการเฝ้าระวังภัยคุกคามรูปแบบใหม่ที่อาจจะเกิดขึ้นกับองค์กรได้ในอนาคต

1.4.2 ขอบเขตด้านประชากร

ขอบเขตด้านกลุ่มตัวอย่างของการศึกษาวิจัยเชิงคุณภาพ ผู้วิจัยจะทำการศึกษาจากกลุ่มตัวอย่าง 4 กลุ่ม มีประสบการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์หรือไซเบอร์ไม่น้อยกว่า 3 ปี ด้วยวิธีการเฉพาะเจาะจง (Purposive Sampling) ดังนี้

1.4.2.1 กลุ่มบุคลากรระดับบริหารและเจ้าหน้าที่เฝ้าระวังและรับมือภัยคุกคามทางไซเบอร์หน่วยงานโครงสร้างพื้นฐานสารสนเทศด้านสาธารณสุขและสาธารณูปโภค ได้แก่ ผู้แทนจากหน่วยงานด้านสาธารณสุข การไฟฟ้าส่วนภูมิภาค การประปาส่วนภูมิภาค การประปานครหลวง ธนาคารแห่งประเทศไทย ธนาคารออมสิน

1.4.2.2 กลุ่มบุคลากรระดับบริหารกำหนดนโยบายและยุทธศาสตร์ด้านการกำกับดูแลเทคโนโลยีดิจิทัลและความมั่นคงปลอดภัยทางไซเบอร์ ได้แก่ ผู้แทนจากสำนักงานคณะทำกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) สำนักงานสภาความมั่นคงแห่งชาติ กระทรวงมหาดไทย สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

1.4.2.3 กลุ่มบุคลากรระดับบริหารด้านกระบวนการยุติธรรม ได้แก่ ผู้แทนจากกระทรวงยุติธรรม สำนักงานตำรวจแห่งชาติ กองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี

1.4.2.4 กลุ่มผู้เชี่ยวชาญอิสระระดับบริหารด้านการจัดการความมั่นคงปลอดภัยทางไซเบอร์ ได้แก่ อาจารย์มหาวิทยาลัย ที่ปรึกษา ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ คอมพิวเตอร์ และระบบสารสนเทศ

โดยข้อมูลที่ได้มาจากการสัมภาษณ์เชิงลึก จะถูกนำมาวิเคราะห์ข้อมูลด้วยวิธีการวิเคราะห์เชิงเนื้อหา (Content Analysis) เพื่อจัดกลุ่มข้อมูลตรวจสอบความถูกต้อง ความครบถ้วนของข้อมูลที่ถูกรวบรวมมาและคัดแยกประเด็นที่ไม่เกี่ยวข้องกับการวิจัยออกไป เพื่อให้ได้ข้อมูลที่มีเนื้อหาที่ตรงประเด็นกับคำถามวิจัยที่ได้ตั้งไว้

1.4.3 ขอบเขตด้านระยะเวลา

การวิจัยครั้งนี้ มีระยะเวลาดำเนินการวิจัยการวิจัยตั้งแต่เดือนมกราคม พ.ศ.2565 ถึงเดือนมิถุนายน พ.ศ.2566

1.5 นิยามคำศัพท์ในการวิจัย

1.5.1 นิยามศัพท์ทั่วไป

การกำกับดูแลองค์กร (Corporate Governance) หมายถึง การบริหารจัดการองค์กร การกำกับ การติดตาม การควบคุม และการดูแล ผู้ที่ได้รับมอบหมายอำนาจหน้าที่ให้ไปทำหน้าที่ทางการบริหาร เพื่อให้ทรัพยากรขององค์กรได้นำไปใช้อย่างมีประสิทธิภาพ ประสิทธิผล ตรงตามเป้าหมายอย่างคุ้มค่า โปร่งใส ตรวจสอบได้ ทั้งนี้เพื่อให้เกิดประโยชน์สูงสุดแก่ผู้มีส่วนได้ส่วนเสียทุกฝ่ายอย่างเป็นธรรม

ความตระหนักรู้ (Awareness) หมายถึง ขั้นต่ำสุดของภาคอารมณ์และความรู้สึก (Affective Domain) ความตระหนักรู้ไม่จำเป็นต้องเน้นปรากฏการณ์หรือสิ่งใดสิ่งหนึ่งและจะเกิดขึ้นเมื่อมีสิ่งเร้ามาเป็นตัวกระตุ้นให้เกิดความตระหนักรู้

ยุคดิจิทัล (Digital Era) คือ ยุคของอิเล็กโทรนิกส์ที่เกี่ยวข้องกับเทคโนโลยีที่มีความรวดเร็ว ในการสื่อสารการส่งผ่านข้อมูลความรู้ต่าง ๆ ที่มีอยู่ในสังคมไม่ว่าจะเป็นข่าวสาร ภาพหรือวิดีโอที่ทุกคนสามารถเข้าถึงได้อย่างรวดเร็วทุกที่และทุกเวลา

1.5.2 นิยามศัพท์เชิงปฏิบัติการ

ภัยคุกคามไซเบอร์ (Cyber Threats) หมายถึง การกระทำหรือการดำเนินการใดๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นๆที่เกี่ยวข้อง และเป็นภัย

อันตรายที่ใกล้จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง โดยแบ่งออกเป็น 3 ระดับ คือ

(1) ภัยภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง หมายถึง ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศหรือการให้บริการของรัฐด้อยประสิทธิภาพลง

(2) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมุ่งหมายเพื่อโจมตีโครงสร้างพื้นฐานสำคัญของประเทศและการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศ ความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจการสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหาย จนไม่สามารถทำงานหรือให้บริการได้

(3) ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติมีลักษณะ คือ

(ก) เป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ในระดับที่สูงขึ้นกว่าภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยส่งผลกระทบรุนแรงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศในลักษณะที่เป็นวงกว้าง จนทำให้การทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบ จนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือการใช้มาตรการเยียวยาตามปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิตหรือระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ

(ข) เป็นภัยคุกคามทางไซเบอร์อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชนหรือเป็นภัยต่อความมั่นคงของรัฐหรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวล

กฎหมายอาญา การรบหรือการสงคราม ซึ่งจำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขต ผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ส่วนรวม หรือการป้องปัดหรือแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง (พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562)

ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) หมายถึง กระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อให้องค์กรปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบทั้งทางอิเล็กทรอนิกส์และทางกายภาพ ความปลอดภัยของระบบและเครือข่ายที่ใช้ในการเก็บ เข้าถึง ประมวล และกระจายข้อมูล ทั้งนี้รวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม และความผิดพลาดต่างๆ

อาชญากรรมไซเบอร์ (Cyber Crime) หมายถึง อาชญากรรมใดๆ ที่เกี่ยวข้องกับคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ รวมถึงการแสวงหาผลประโยชน์อย่างผิดกฎหมายบนอินเตอร์เน็ต ความผิดที่กระทำขึ้นมีต่อปัจเจกบุคคลหรือกลุ่มของปัจเจกบุคคลด้วยเหตุจูงใจทางอาญาที่เจตนาทำให้เหยื่อเสื่อมเสียชื่อเสียง หรือทำร้ายร่างกายหรือจิตใจของเหยื่อ โดยทางตรงหรือทางอ้อม โดยใช้เครือข่ายโทรคมนาคมสมัยใหม่ อาทิ อินเทอร์เน็ต และโทรศัพท์เคลื่อนที่ สำหรับการศึกษาในครั้งนี้ หมายความรวมถึง อาชญากรรมเช่นนั้นอาจคุกคามความมั่นคงของรัฐด้วย

ศูนย์ปฏิบัติการไซเบอร์ (Cyber Security Operation Center: CSOC) คือ ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ที่ใช้บุคลากรและเทคโนโลยีเพื่อตรวจสอบและปรับปรุงการรักษาความปลอดภัยขององค์กรอย่างต่อเนื่อง พร้อมทั้งทำหน้าที่ตรวจจับ, ป้องกัน, วิเคราะห์และแก้ไขสถานการณ์หากมีเหตุการณ์ด้านความมั่นคงปลอดภัยและทำหน้าที่เหมือนศูนย์บัญชาการกลาง โดยรับข้อมูลจากโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศขององค์กร รวมถึงเครือข่ายอุปกรณ์, เครื่องใช้และการเก็บข้อมูล

การรับมือ (Coping) หมายถึง จัดการ ต้านทาน กำราบ และเป็นการจัดเป็นลำดับขั้นตอนโดยแยกแยะหมวดหมู่มักจะทำแบบเป็นคู่ ๆ เช่น มีปัญหาเป็นศูนย์ หรือมีอารมณ์เป็นศูนย์ สู้หรือหนี โดยการรู้คิดหรือโดยพฤติกรรม

แฮก (Hack) หมายถึง การเจาะระบบ หรือการแทรกซึมเข้าไปในเครื่องคอมพิวเตอร์หรือบัญชีทางคอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์โดยไม่ได้รับอนุญาตเพื่อใช้ประโยชน์ ผู้ที่กระทำการแฮกเรียกว่า แฮกเกอร์ (hacker)

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1.6.1 ได้แนวทางการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมต่อองค์กร

1.6.2 นำผลที่ได้ไปวิเคราะห์และประเมินความเสี่ยงภัยคุกคามทางไซเบอร์ ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยระบบดิจิทัลและสารสนเทศขององค์กร เพื่อคาดการณ์ภัยคุกคามไซเบอร์รูปแบบใหม่ในอนาคตได้

1.6.3 สามารถถ่ายทอดสื่อสารกระบวนการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ เพื่อสร้างความตระหนักรู้ให้แก่ผู้มีส่วนได้ส่วนเสียในการเฝ้าระวังภัยคุกคามไซเบอร์ขององค์กร

1.6.4 ทบทวน ปรับปรุงนโยบายและแนวปฏิบัติที่ดีด้านดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ เพื่อเตรียมแผนการรับมือภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้นได้ในอนาคต

บทที่ 2
แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

การนำพาประเทศไทยก้าวสู่ยุคดิจิทัลโดยการส่งเสริมการใช้วิทยาศาสตร์เทคโนโลยี วิจัยและพัฒนา และนวัตกรรมทั้งในภาคการผลิตและภาคบริการ ย่อมเกี่ยวข้องกับความก้าวหน้าของเทคโนโลยียุคใหม่โดยเฉพาะเทคโนโลยีดิจิทัลซึ่งมีประโยชน์ในการช่วยเพิ่มขีดความสามารถในการแข่งขันของประเทศ แต่ก็นำพาภัยคุกคามรูปแบบใหม่ที่เรียกว่าภัยคุกคามไซเบอร์เข้ามา ซึ่งสามารถสร้างผลกระทบทั้งต่อความมั่นคงและต่อเศรษฐกิจของประเทศ การเฝ้าระวังภัยคุกคามและสร้างความมั่นคงปลอดภัยไซเบอร์จึงเป็นเรื่องจำเป็นอย่างยิ่ง ภาครัฐเองมีการกำหนดเรื่องนี้ไว้ในยุทธศาสตร์ชาติ มีการจัดทำแผนและนโยบายรองรับ ศึกษากรอบการทำงานและมาตรฐานสากลที่เกี่ยวข้องกับการสร้างความมั่นคงปลอดภัยไซเบอร์ รวมทั้งวิจัยและสำรวจการดำเนินการดังกล่าวทั้งในหน่วยงานภาครัฐ และองค์กรภาคธุรกิจที่มีการใช้เทคโนโลยีดิจิทัลและไซเบอร์ เพื่อเป็นข้อมูลในการดำเนินการป้องกันภัยคุกคามดังกล่าวให้เกิดประสิทธิภาพ ประสิทธิผล และไม่เป็นอุปสรรคต่อเป้าหมายในการพัฒนาประเทศ

ในมุมของความมั่นคงของชาติ รัฐบาลจำเป็นต้องตื่นตัวและระวังภัยมากขึ้นในการเร่งกำหนดนโยบายทางไซเบอร์ด้วยเหตุผลและที่มาที่ไปดังกล่าว สร้างความตะหนักถึงผลกระทบทางไซเบอร์ทั้งระยะสั้นและระยะยาวต่อความมั่นคง มั่งคั่ง ยั่งยืน ของประเทศชาติ การวางแผนกลยุทธ์ยุทธศาสตร์ชาติ ให้สอดคล้องกับ ความเป็นไปของโลกในศตวรรต 21 ที่ไซเบอร์กำลังเป็นปัจจัยขับเคลื่อนที่สำคัญของทุกประเทศทั่วโลกในขณะนี้และส่งผลกระทบต่อความมั่นคงของชาติในอนาคต ซึ่งในการศึกษาวิจัยนั้นมีความเป็นสหวิทยาการ (Multidisciplinary) เพื่อประโยชน์ในการวิเคราะห์และคาดการณ์แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์และเฝ้าระวังภัยคุกคามทางออนไลน์ในประเทศไทยต่อไป ดังนั้น ในบทนี้จะนำประเด็นทั้งหมดที่เกี่ยวข้องกับการศึกษาถึงสถานการณ์ภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยขององค์กรที่เป็นหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศด้านสาธารณสุขและด้านสาธารณูปโภค รวมทั้งแนวทางการกำกับดูแลเพื่อป้องกัน รับมือ และเฝ้าระวังภัยคุกคามทางไซเบอร์ให้กับองค์กรในยุคดิจิทัล ซึ่งผู้ศึกษาวิจัยได้รวบรวมข้อมูลแนวคิดทฤษฎีที่เกี่ยวข้องมานำเสนอ ดังนี้

2.1 แนวคิดและทฤษฎีเกี่ยวกับสังคมสมัยใหม่ (Modernization)

2.1.1 สภาวะสังคมสมัยใหม่ (Modernization)

2.1.2 เทคโนโลยีดิจิทัล (Digital Technology)

2.1.3 ความเป็นพลเมืองดิจิทัล (Digital Citizenship)

2.1.4 โลกาภิวัตน์ (Globalization)

2.1.5 เครือข่ายสังคม (Social networks)

2.1.6 ทฤษฎีการเปลี่ยนแปลงทางสังคม (Social Change Theory)

2.1.7 แนวคิดสังคมแห่งความเสี่ยงภัย (Risk Society)

2.2 ภัยคุกคามทางไซเบอร์ (Cyber Threats)

2.2.1 รูปแบบและประเภทของภัยคุกคามทางไซเบอร์

2.2.2 ภัยคุกคามทางไซเบอร์และโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ

2.2.3 สถานการณ์ภัยคุกคามทางไซเบอร์ในต่างประเทศ

2.2.4 สถานการณ์ภัยคุกคามทางไซเบอร์ในประเทศไทย

2.3 ทฤษฎีอาชญาวิทยาและภัยคุกคามทางไซเบอร์

2.3.1 ทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory)

2.3.2 ทฤษฎีการกระทำที่เป็นกิจวัตร (Theory of Routine Activity)

2.3.3 ทฤษฎีการเลือกอย่างเป็นเหตุเป็นผล (Rational Choice Theory)

2.3.4 ทฤษฎีการโจมตีทางไซเบอร์ (Cyber Attack Theory)

2.3.5 ทฤษฎีการป้องกันอาชญากรรมตามสถานการณ์ (Situational Crime Prevention)

2.4 พลวัตของภัยคุกคามความมั่นคงปลอดภัยไซเบอร์

2.4.1 อาชญากรรมคอมพิวเตอร์ (Computer Crime)

2.4.2 อาชญากรรมไซเบอร์ (Cyber Crime)

2.4.3 อาชญาวิทยาไซเบอร์ (Cyber Criminology)

2.5 แนวทางการกำกับดูแลและรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์

2.5.1 การเตรียมองค์กรสอดรับกฎหมายและยุทธศาสตร์ทางไซเบอร์

2.5.2 ความร่วมมือด้านการกำกับดูแลและรับมือภัยคุกคามทางไซเบอร์

2.5.3 การจัดการภัยคุกคามทางไซเบอร์ของประเทศไทย

2.5.4 มาตรฐานและกรอบการดำเนินงานการรักษาความมั่นคงปลอดภัยไซเบอร์

2.5.5 การบริหารความเสี่ยงด้านไซเบอร์ขององค์กร

2.5.6 การสร้างความตระหนักรู้และการเตรียมความพร้อมรับมือภัยคุกคามทางไซเบอร์

2.5.7 การจัดตั้งศูนย์ปฏิบัติการไซเบอร์เฝ้าระวังและตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์

2.6 งานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดและทฤษฎีเกี่ยวกับสังคมสมัยใหม่ (Modernization)

2.1.1 สภาวะสังคมสมัยใหม่ (Modernization)

ในคริสต์ศตวรรษที่ 17 ถือได้ว่าเป็นยุคความคิดใหม่ทันสมัย (Modernism) อันหมายถึงยุคสมัยให้ความสนใจในเรื่องศิลปะ วรรณคดี วิทยาการ สถาบัน เหตุผล การศึกษา เศรษฐกิจ การเมือง เทคโนโลยี วิทยาศาสตร์ รูปแบบของชีวิต ความจริงของชีวิตบนฐานของความเจริญเปลี่ยนแปลงของสังคมโลก กล่าวคือเป็น ช่วงเวลาแห่งความเจริญทางวัตถุ ความมั่นคงทางสังคม และความรู้เข้าใจตนเอง (Material progress, social stability and self-realization) ในยุโรปตะวันตก มีอังกฤษ อเมริกา ฝรั่งเศส อิตาลี เป็นต้น แม้มีปัจจัยต่างๆ มากมายที่ทำให้เกิดสมัยใหม่ ปัจจัยสำคัญเหล่านี้ คือ ความจริง (Truth) เหตุผล (Rationality) วิทยาศาสตร์ (Science) เทคโนโลยี (Technology) ผลของอุตสาหกรรม (Emergence of capitalism) การแผ่อำนาจทางตะวันตก (Western imperialism) การแพร่กระจายความรู้ และอำนาจทางการเมือง (Spread of literature and political power) การขับเคลื่อนทางสังคม (Social mobility) เป็นสาเหตุสำคัญสนับสนุนส่งเสริมการเปลี่ยนแปลงพัฒนาสังคมโลก ที่เรียกกันว่า “สมัยใหม่ความทันสมัย (Modernism)” เพราะผลของความเจริญทางการศึกษาวิทยาศาสตร์ เทคโนโลยี อุตสาหกรรม และการขับเคลื่อนทาง

สังคม ทำให้มนุษย์ต้องการรู้เข้าใจตนเองและสังคมมากยิ่งขึ้นตามลำดับ ทำให้ต้องมาคิดใหม่ทำใหม่ เพื่อความถูกต้องดีงามแบบสากล แสดงความรับผิดชอบต่อสังคมโลกร่วมกัน เพื่อความรู้เข้าใจใหม่ร่วมกัน จึงขอลำดับเหตุการณ์การวิวัฒนาการแนวความคิดใหม่ทันสมัย

ในทรรศนะของแอนโธนี กิดเดนส์ (Anthony Giddens) นักสังคมวิทยาชาวอังกฤษ ได้ตั้งข้อสังเกตว่ามโนทัศน์และจินตภาพที่ถูกสร้างขึ้นมาในสังคมวิทยา เช่น สถานภาพทางสังคม ถูกนำไปใช้อย่างกว้างขวางในสื่อและในการถกเถียงของคนทั่วไปในชีวิตประจำวัน ความรู้ทางสังคมวิทยาได้ถูกกำหนดเป้าหมายให้กลายเป็นเรื่องของ “สิ่งที่ทุกๆคนรู้” เนื่องจากเป็นวิธีหลักที่สมาชิกของสังคมสมัยใหม่ใช้ในการทำความเข้าใจและอธิบายสิ่งต่างๆที่เกิดขึ้นในสังคม ความรู้ทางสังคมวิทยาได้เข้ามาและกลายเป็นส่วนหนึ่งของโลกทางสังคมและมีส่วนช่วยในการเปลี่ยนแปลงโลกทางสังคม โลกที่เปลี่ยนแปลงไปอย่างรวดเร็วจากพัฒนาการของเทคโนโลยีตั้งแต่ศตวรรษที่ 16 จนถึงปัจจุบันส่งผลให้สภาพของสังคมโลกมีความเจริญก้าวหน้าอย่างต่อเนื่อง อันเป็นผลจากการสร้างสังคมที่วางอยู่บนรากฐานของระบบเทคโนโลยี กระตุ้นให้เกิดการเปลี่ยนแปลงแบบค่อยเป็นค่อยไปหรือวิวัฒนาการ (evolution) เป็นการผสานระหว่างของเดิมกับของใหม่ (diffusion Process) ทำให้สังคมดั้งเดิมกลายเป็นสังคมสมัยใหม่ (Giddens, 1996) ในขณะที่มุมมองของจัง จ๊าร์ค รุสโซ(Jean-Jacques Rousseau) นักคิดทางการเมืองที่ได้แสดงทัศนคติต่อวิทยาศาสตร์สมัยใหม่ ที่เฟื่องฟูอยู่ในยุคภูมิปัญญานั้น ว่ามิได้เป็นไปตามกระแสสังคมที่เชื่อว่าตั้งอยู่บนหลักของเหตุและผล แต่กลับมีพื้นฐานที่สำคัญอยู่กับสิ่งที่สังคมสมัยใหม่ (Modern Society) ไม่ได้ให้การยอมรับ เช่น วิชาดาราศาสตร์ (Astronomy) ที่มีพื้นฐานมาจากโหราศาสตร์ (Astrology) ซึ่งก็คือความเชื่อในพลังเหนือธรรมชาติ (Superstition) วิชาคณิตศาสตร์ (Mathematics) จากการก่อหนี้สิ้น (Accounting) อันเป็นผลมาจากความโลภของมนุษย์ กฎหมาย (Law) ก็เป็นผลที่เกิดขึ้นโดยตรงจากความไม่เท่าเทียม (Inequality) และความอยุติธรรม (Injustice) ในสังคมมนุษย์ ขณะเดียวกัน ความก้าวล้ำหน้าในเทคโนโลยีการทำสงคราม ได้เข้ามาแทนที่และบดบังความกล้าหาญของทหาร ที่ร้ายกาจที่สุดคือความก้าวหน้าทางด้านการแพทย์แผนใหม่ ได้ทำลายความสามารถของมนุษย์ที่จะเผชิญหน้ากับความตาย (capacity to face death) (ราม โชติคุต, 2555)

ในปัจจุบันด้วยสภาวะสังคมสมัยใหม่ที่มีความก้าวหน้าด้านวิทยาศาสตร์ เทคโนโลยี และนวัตกรรม ทำให้สังคมโลกแห่งความจริงกลายเป็นสังคมดิจิทัล เกิดเป็นยุคแห่ง Digital

Transformation ที่มนุษย์ได้นำเทคโนโลยีมาปรับใช้ในชีวิตประจำวัน เพราะนอกเหนือจากปัจจัย 4 ที่เป็นพื้นฐานที่จำเป็นต่อการดำรงชีวิตของมนุษย์อย่าง อาหาร ที่อยู่อาศัย เครื่องนุ่งห่ม และยารักษาโรคนั้น เทคโนโลยีที่ปัจจุบันถูกพัฒนาอย่างก้าวกระโดดอย่างโทรศัพท์มือถือ คอมพิวเตอร์โน้ตบุ๊ก แท็บเล็ต จึงปฏิเสธไม่ได้ว่าอุปกรณ์อิเล็กทรอนิกส์เหล่านี้กลายเป็นปัจจัยที่ 5 ที่หลายคนในสังคมต้องการและกล่าวถึงอยู่ในขณะนี้ ผู้วิจัยสนใจสภาวะสังคมสมัยใหม่ (Modernity) น่าจะเป็นปัจจัยที่ทำให้เกิดการอาชญากรรมรูปแบบใหม่ในการก่ออาชญากรรม ส่งผลให้คนไทยในปัจจุบันมีความเสี่ยงอันตรายจากอาชญากรรมที่มากขึ้น อีกทั้งอาชญากรรมที่มีลักษณะรูปแบบใหม่ ๆ เป็นผลจากอาชญากรรมเดิม ๆ จากผลกระทบของระบบการผลิตแบบอุตสาหกรรมในสังคมสมัยใหม่ ความรู้จากกระบวนการทางวิทยาศาสตร์และเทคโนโลยีสมัยใหม่ที่สร้างความก้าวหน้าให้สังคมไทย เช่น อาชญากรรมทางเศรษฐกิจ อาชญากรรมไซเบอร์ อาชญากรรมที่เกิดจากผลกระทบของการแพร่ระบาดของโรคติดเชื้อไวรัสโคโรนา 2019 (COVID-19) เป็นต้น ทำให้ปัญหาอาชญากรรมในปัจจุบันได้แสดงให้เห็นถึงอันตรายและสิ่งต่าง ๆ ที่จะเป็นอันตรายในรูปแบบต่าง ๆ ได้ ไม่จำกัดเวลาและสถานที่ ยิ่งไปกว่านั้น ความล้ำสมัยของเทคโนโลยีในปัจจุบันก็แปรผันไปตามบริบทของสังคมสมัยใหม่ วิกฤตการณ์โลกเป็นตัวเร่งเร้าที่ทำให้เกิดการเปลี่ยนแปลงอย่างรวดเร็วและคาดไม่ถึงในทุกสภาวการณ์อย่างหลักเลี่ยงไม่ได้

2.1.2 เทคโนโลยีดิจิทัล (Digital Technology)

การเข้าสู่ยุค “ประเทศไทย 4.0” ที่มุ่งหวังให้มีการขับเคลื่อนเศรษฐกิจด้วยนวัตกรรมนำเทคโนโลยีที่ทันสมัยมาช่วยการพัฒนาประเทศ ในขณะเดียวกันได้เกิดกระแสของการให้บริการในรูปแบบใหม่ในยุคดิจิทัลเรียกได้ว่าเป็น “เทคโนโลยีก้าวกระโดด” (Disruptive Technology) ที่ได้รับความนิยมอย่างฉับพลันอันเนื่องมาจากความสามารถในตอบสนองต่อความต้องการของผู้บริโภคในวิถีปัจจุบันโดยเฉพาะกรณีของประเทศไทยหลังการจัดสรรคลื่นความถี่โดยคณะกรรมการกระจายเสียง กิจการโทรทัศน์ และ กิจการโทรคมนาคมแห่งชาติ (กสทช.) ที่ให้บริการอินเทอร์เน็ตความเร็วสูงแบบไร้สาย อีกทั้งเมื่อราคาของโทรศัพท์แบบสมาร์ทโฟนในตลาดมีราคาถูกลง คนจำนวนมากเข้าถึงได้มากขึ้น จึงทำให้เกิดการบริการผ่านระบบออนไลน์ที่แพร่หลายอย่างรวดเร็วในสังคมไทย ทั้งนี้การเปลี่ยนแปลงที่ก้าวกระโดดดังกล่าวอยู่ในภาพใหญ่ที่ทางสภาผู้บริหารเศรษฐกิจโลก (World Economic Forum) เรียกว่าเป็นการปฏิบัติอุตสาหกรรมครั้งที่สี่ (The Fourth

Industrial Revolution) ที่ไม่ได้หมายถึงแค่ระบบและจักรกลอัจฉริยะที่เชื่อมโยงกันได้เท่านั้น แต่มีขอบเขตที่กว้างขวางกว่านั้นมาก สิ่งที่เกิดควบคู่กันคือคลื่นแห่งการค้นพบที่ยิ่งใหญ่ล้ำหน้ายิ่งขึ้นในด้านต่างๆ ตั้งแต่การจัดลำดับพันธุกรรมไปถึงนาโนเทคโนโลยี ตั้งแต่พลังงานทดแทนไปถึงคอมพิวเตอร์ระบบควอนตัม การผสมกลมกลืนและปฏิสัมพันธ์ของเทคโนโลยีเหล่านี้ ทั้งในด้านกายภาพ ดิจิทัล และชีวภาพ คือสิ่งที่ทำให้การปฏิวัติอุตสาหกรรมครั้งที่สี่แตกต่างจากการปฏิวัติที่ผ่านมาโดยสิ้นเชิง

การเปลี่ยนแปลงอย่างก้าวกระโดดด้วยพลังของตลาดและการบริโภค หากภาครัฐ ภาคธุรกิจ และภาคสังคมไม่สามารถปรับตัวให้ทันต่อการเปลี่ยนแปลงดังกล่าว ก็จะส่งผลให้ความสำคัญของภารกิจ (Relevance) ลดลงไป ยกตัวอย่างกรณีกิจการสื่อสารมวลชน ซึ่งได้รับผลกระทบจากเทคโนโลยีสารสนเทศแบบใหม่ผ่านสื่อสังคมออนไลน์ (Social Media) เห็นได้จากปรากฏการณ์ของสื่อสิ่งพิมพ์รวมถึงสถานีโทรทัศน์ที่ต้องทยอยปิดกิจการลง เพราะพฤติกรรมของผู้บริโภคที่เปลี่ยนแปลงไป เนื่องจากประชาชนส่วนใหญ่ โดยเฉพาะกลุ่มวัยรุ่นและวัยทำงานที่รับสื่อผ่านโทรศัพท์มือถือมากกว่าดูทีวี หรือ การที่ประชาชนจับจ่ายใช้สอยผ่านแพลทฟอร์มออนไลน์และทำธุรกรรมผ่านโทรศัพท์ไร้สายมากขึ้นอย่างก้าวกระโดด รวมไปถึงการพัฒนานวัตกรรม (Innovation) การใช้สมองกลอัจฉริยะ ปัญญาประดิษฐ์ (Artificial Intelligence) และ เทคโนโลยีภาคพลเมืองมาแก้ปัญหาสังคมมากขึ้น (Civic Technology)

แม้ว่าเทคโนโลยีที่เจริญก้าวหน้าอย่างเทคโนโลยีชั้นสูง (Advanced Technology) รูปแบบต่าง ๆ ในปัจจุบันจะถูกใช้เป็นเครื่องมือในการเผยแพร่แนวคิดหรือส่งเสริมการพัฒนาสังคมและประเทศชาติ แต่ความก้าวหน้าของเทคโนโลยีเหล่านี้ อาจทำให้เกิดปัญหาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) เช่น การใช้เทคโนโลยีเป็นเครื่องมือในการเผยแพร่ข้อมูลในลักษณะที่ทำให้เกิดการครอบงำการตัดสินใจของประชาชน นอกจากนี้ ความเจริญก้าวหน้าทางเทคโนโลยีอาจก่อให้เกิดการละเมิดสิทธิในรูปแบบใหม่รวมไปถึงการก่ออาชญากรรมในรูปแบบใหม่ที่มีความรุนแรงและส่งผลเสียหายเป็นวงกว้างยิ่งกว่าอาชญากรรมอื่นๆ ที่ไม่เกี่ยวข้องกับดิจิทัล ซึ่งหลายประเทศพยายามแก้ไขปัญหาความปลอดภัยทางไซเบอร์ด้วยการให้รัฐบาลเข้าไปควบคุมการใช้สื่อไซเบอร์ของประชาชนในระดับความเข้มข้นที่ต่างกัน จนทำให้หลายประเทศถูกตั้งคำถามเกี่ยวกับความได้สัดส่วนของการจัดการปัญหาความมั่นคงทางไซเบอร์กับการจำกัดสิทธิเสรีภาพของประชาชน ยิ่งกว่านั้น

หลายประเทศได้เริ่มใช้เทคโนโลยีเป็นเครื่องมือในการส่งเสริมประชาธิปไตย การใช้ระบบอินเทอร์เน็ตในการเลือกตั้ง และการแสดงความเห็น อีกทั้งสื่อเหล่านี้ยัง กลายเป็นช่องทางในการเข้าถึงข้อมูลที่สำคัญ ความท้าทายจึงเกิดขึ้นเมื่อพบว่าแท้จริงแล้ว ประชาชนยังคงไม่สามารถเข้าถึงเทคโนโลยีเหล่านี้ได้อย่างเท่าเทียมกัน จนกล่าวได้ว่าความเหลื่อมล้ำในการเข้าถึงเทคโนโลยีซึ่งส่งผลให้เกิดความเหลื่อมล้ำในการเข้าถึงข้อมูลหรือการใช้สิทธิบางประการอีกด้วย ทฤษฎีเทคโนโลยีสมัยใหม่โดย Meadows (2007) อธิบายไว้ว่า เป็นทฤษฎีที่ชี้ให้เห็นถึงความเจริญทางเทคโนโลยีสมัยใหม่มีความเกี่ยวข้องกับการเกิดอาชญากรรม เพราะพัฒนาการทางเทคโนโลยีในเชิงเครื่องมือที่เกิดขึ้นอย่างต่อเนื่อง ทำให้ต้องพึ่งพาเทคโนโลยีที่เป็นการอำนวยความสะดวก การเข้าถึงข้อมูล หรือมีความจำเป็นต้องใช้ย่อมทำให้ผู้คนสามารถนำไปใช้หาประโยชน์ในทางที่ผิด ขณะเดียวกันเทคโนโลยีก็ได้กลายเป็นแหล่งที่ส่งเสริมการตกเป็นเหยื่อได้เหมือนกัน มีบุคคลบางจำพวกที่หาประโยชน์จากเทคโนโลยีโดยการทำให้คนหนุ่มสาวหรือผู้ที่ขาดวุฒิภาวะและผู้ที่ไร้เดียงสาต้องตกเป็นผู้เสียหายอันมีผลมาจากเทคโนโลยีนั้น เกิดจากอาชญากรรมที่เรียกว่า อาชญากรรมทางคอมพิวเตอร์และอินเทอร์เน็ต (Cybercrime) ตัวอย่างเช่น การคุกคามโดยพวกอาชญากร (Criminal threats) การล่อลวง (Cyber stalking) การคุกคามโดยจดหมายอิเล็กทรอนิกส์ (Threatening or Annoying Electronic Mail) การล่อลวง (Luring and Enticement) และการเจาะระบบคอมพิวเตอร์ (Computer Hacking) ซึ่งผู้ตกเป็นผู้เสียหายทางคอมพิวเตอร์ มักจะเป็นเด็กหรือวัยรุ่น ผู้กระทำความผิดจะติดต่อกับเด็กหรือเยาวชนทางอินเทอร์เน็ต (ศรีสมบัติ โชคประจักษ์ชัด, 2561) ในทัศนะของอิลลูล (Jacques Ellul) มองสังคมเทคโนโลยีสมัยใหม่ว่าตกอยู่ภายใต้การกำหนดของเทคโนโลยีด้วยการเสนอหลักการมีอำนาจในตัวเองของเทคโนโลยีอย่างเข้มข้น การมุ่งประเด็นวิเคราะห์ตัวสังคมสมัยใหม่ทำให้ความเข้าใจเทคโนโลยี มีแกนกลางอยู่ที่อำนาจของเทคโนโลยีในสังคมสมัยใหม่ที่เขาเรียกว่า “กรรมวิธีทางเทคนิค” (Technological order หรือ Technique) อิลลูลมองว่าสังคมเทคโนโลยีสมัยใหม่อยู่ในการควบคุมของ “กฎ” คล้าย ๆ กับกฎธรรมชาติ (แรงโน้มถ่วง) หรือกฎทางพันธุศาสตร์ (DNA) กล่าวคือ ทุก ๆ เหตุการณ์หรือการกระทำในสังคมเทคโนโลยีล้วนแล้วแต่อยู่ภายใต้ “กรรมวิธีทางเทคนิค” อันหมายถึง “วิธีการทุกอย่างที่มีเหตุผลเพื่อจะไปให้ถึงและได้ประสิทธิภาพสูงสุดในทุก ๆ พื้นที่ของกิจกรรมมนุษย์” (Ellul, 1964)

เทคโนโลยีดิจิทัลได้สร้างเครื่องมือและทรัพยากรที่น่าทึ่งทำให้ข้อมูลที่เป็นประโยชน์ การปฏิวัติทางเทคโนโลยีทำให้ชีวิตของเราง่ายขึ้น เร็วขึ้น ดีขึ้น ความก้าวหน้าของเทคโนโลยีเปลี่ยนแปลงรูปแบบของการสื่อสารและพฤติกรรมของผู้คนไปอย่างมาก จากเดิมที่ผู้คนส่วนใหญ่เป็นผู้รับสารและรอรับข้อมูลจากผู้ส่งสาร แต่ในปัจจุบันทุกคนสามารถเป็นผู้ส่งสารได้อย่างง่ายดาย เทคโนโลยีที่มีผลด้านบวกต่อสังคมคือส่งผลต่อการเรียนรู้ ทำให้การเรียนรู้มีการโต้ตอบและทำงานร่วมกันมากขึ้นซึ่งจะช่วยให้ผู้คนมีส่วนร่วมกับเนื้อหาที่เรียนรู้และมีปัญหาได้ดีขึ้น เพราะอินเทอร์เน็ตช่วยให้ผู้เรียนสามารถเรียนได้ตลอดเวลา และส่งเสริมการเรียนรู้ตลอดชีวิต นอกจากนี้เทคโนโลยีส่งผลกระทบต่อสังคมคือช่วยให้ผู้คนมีปฏิสัมพันธ์ระหว่างกันได้แม้อยู่คนละมุมโลก อย่างไรก็ตาม เทคโนโลยียังส่งผลกระทบด้านลบต่อผู้คน กล่าวคือ เทคโนโลยีโทรทัศน์มือถือลดการสื่อสารและความสัมพันธ์ระหว่างกัน การบริหารจัดการเวลาส่วนตัวมีน้อยลงเนื่องจากต้องออนไลน์ติดตามผู้อื่นและถูกผู้อื่นติดตามตลอดเวลา จนอาจกล่าวได้ว่าอิทธิพลทางเทคโนโลยีมีส่วนกำหนดและการเป็นส่วนหนึ่งของรูปแบบการกระทำของมนุษย์ในปัจจุบันไป และด้วยความรวดเร็วของเทคโนโลยีที่ได้รับการพัฒนาขึ้นอย่างต่อเนื่อง ทำให้การแข่งขันด้านความรวดเร็วจึงเกิดขึ้นอย่างเลี่ยงไม่ได้ ความถูกต้องของข้อมูลจึงถูกมองข้ามไป ซึ่งสิ่งเหล่านี้ส่งผลกระทบต่อสุขภาวะทั้งทางร่างกายและทางใจของสมาชิกในสังคม จากการได้รับชุดข้อมูลผิดหรือบิดเบือน โดยเฉพาะในช่วงของการแพร่ระบาดของไวรัสโควิด-19 (Coronavirus Disease 19) ซึ่งกลายเป็นปัญหาของโลก ที่สั่นคลอนเสถียรภาพทั้งเศรษฐกิจและสังคม เกิดความรู้สึกไม่มั่นคงและเต็มไปด้วยความหวาดกลัว ทำให้เกิดการแพร่สะพัดของข้อมูลบิดเบือนจำนวนมากผ่านทางสื่อสังคมออนไลน์ นอกจากนี้ยังรวมถึงอาชญากรรมไซเบอร์ที่สร้างผลกระทบต่อชีวิต ทรัพย์สิน และ สิทธิของพลเมืองในยุคดิจิทัล

จากสถานการณ์ทั่วโลกตกอยู่ในภาวะวิกฤติด้านสุขภาพจากโรคระบาดโควิด-19 ที่กระทบรุนแรงและลึกซึ้งต่อระบบสุขภาพ เศรษฐกิจ สังคมการเมือง ส่งผลให้ประชากรทั่วโลกรวมถึงประเทศไทยต้องปรับพฤติกรรมและวิถีชีวิตด้วยการทำงานและใช้ชีวิตอยู่ในบ้านเป็นเวลายาวนาน โดยมีกิจกรรมผ่านบริการโทรคมนาคมและปรับตัวเข้าสู่ยุคดิจิทัลมากขึ้นทั้งการประชุมออนไลน์ การทำงาน การเรียน การจับจ่ายใช้สอยและการทำธุรกรรมในชีวิตประจำวัน บทบาทของเทคโนโลยีมีอิทธิพลต่อพลเมืองและกระตุ้นให้เกิดการการปรับตัวครั้งใหญ่ของทุกภาคส่วน ผลักดันให้พลเมืองเปลี่ยนผ่านสู่ระบบดิจิทัลอย่างเร็วขึ้นอีก จนกลายเป็นสิ่งที่เรียกว่าวิถีปรกติใหม่ (New Normal) อีก

ทั้งมาตรการควบคุมโรคกลายเป็นเหตุจำเป็นให้ภาครัฐต้องมีการเก็บข้อมูลส่วนบุคคลของประชาชนเพื่อติดตามการเคลื่อนไหวของผู้ติดเชื้อด้วยเช่นกัน (Contact tracing) เหตุปัจจัยเหล่านี้ก็ให้เกิดการตั้งคำถามถึงจุดสมดุลระหว่างความมั่นคงปลอดภัยสาธารณะในการใช้ชีวิตเชื่อมต่อโลกออนไลน์ ความเป็นส่วนตัว การคุ้มครองข้อมูลส่วนบุคคล (Data Protection) การเข้าถึงข้อมูลของภาครัฐและเอกชน และการเปิดเผยข้อมูลของภาครัฐให้สาธารณชนได้เข้าถึงและใช้ประโยชน์ (Open Data) เป็นต้น

จะเห็นได้ว่าการที่สังคมไทยพึ่งพาเทคโนโลยีในการอำนวยความสะดวก การเข้าถึงข้อมูล หรือเพราะมีความจำเป็นต้องใช้ น่าจะเป็นปัจจัยที่นำไปสู่การก่ออาชญากรรมไซเบอร์ในสังคมไทย และเกิดความสัมพันธ์กับอาชญากรรมเศรษฐกิจและอาชญากรรมรูปแบบใหม่ในการก่ออาชญากรรม ส่งผลให้ปัญหาอาชญากรรมไซเบอร์เข้ามาอยู่ในการใช้ชีวิตประจำวันของคนในสังคมไทยมากขึ้น จนทำให้ประชาชนตกเป็นผู้เสียหายจากอาชญากรรมไซเบอร์ได้โดยง่าย ตัวอย่างเช่น คดีหลอกรักออนไลน์ (Romance Scam หรือ Love Scam) จากอาชญากรรมดั้งเดิมคือการล่อลวงจะเป็นการพบปะกันซึ่งหน้าและจะเห็นรูปร่างลักษณะของผู้ก่อเหตุ แต่ในปัจจุบันความจำเป็นที่ต้องใช้เทคโนโลยีในชีวิตประจำวันมากขึ้น เช่น โทรศัพท์มือถือ แท็บเล็ต คอมพิวเตอร์ การใช้สื่อสังคมออนไลน์ ส่งผลให้ผู้เสียหายจะไม่รู้ว่าอาชญากรเป็นใคร ติดตามตัวได้ยาก ร้อยเล่ห์เพทุบาย เมื่อเหยื่อตายใจและตกหลุมรัก ก็จะสร้างสถานการณ์ให้น่าสงสารและเห็นใจ เพื่อขอเงิน โดยหลอกว่าจะมาแต่งงานกับเหยื่อที่เมืองไทยโดยจะส่งทรัพย์สิน เช่น เงินสด ทองคำ เครื่องเพชร มาให้เหยื่อที่เมืองไทย ขอข้อมูลส่วนตัว ขอที่อยู่อาศัย สถานที่พักพิง เพราะหลอกว่าจะมาใช้ชีวิตอยู่ที่เมืองไทย หลอกล่อเหยื่อด้วยการถ่ายรูปส่งมาให้ดูเพื่อจูงใจ โดยรูปที่เอามาใช้ส่วนใหญ่จะนำมาจาก Google แปลงโฉมตัวเองโดยสร้างโปรไฟล์ปลอมให้ดูสวย หล่อ มีฐานะดี มีรูปแบบการดำเนินชีวิตที่ดี หรูหรา เพื่อล่อเหยื่อเข้ามาติดกับดัก ซึ่งปัจจุบันความก้าวหน้าทางเทคโนโลยีอย่าง Deepfake เทคโนโลยีใหม่ที่ช่วยให้ปลอมแปลงตัวตนของผู้คน ผ่านภาพ เสียง หรือคลิปวีดีโอได้อย่างแนบเนียนจนยากจะแยกแยะ ถึงขนาดสร้างใบหน้าใหม่ขึ้นมาได้ โดยอาศัยการประมวลผลของปัญญาประดิษฐ์ (Artificial Intelligent: AI)

นอกจากนี้ ยังมีภัยอาชญากรรมจากมิจฉาชีพคอลเซ็นเตอร์ หรือแก๊งคอลเซ็นเตอร์ (Call Center) เป็นอาชญากรรมทางเศรษฐกิจระหว่างประเทศรูปแบบหนึ่งในยุคดิจิทัล ซึ่งนอกจากจะก่อให้เกิดความเสียหายทางเศรษฐกิจต่อเหยื่อจำนวนมากแล้ว ยังก่อให้เกิดความเสียหายต่อเศรษฐกิจในภาพรวมระดับประเทศอีกด้วย ภัยคอลเซ็นเตอร์ถือได้ว่าเป็นอาชญากรรมทางเศรษฐกิจ

ข้ามชาติที่เป็นภัยร้ายแรงและเฝ้าระวังในช่วงปีที่ผ่านมา โดยเฉพาะอย่างยิ่งในยุคปัจจุบันซึ่งเป็นยุคข้อมูลข่าวสารที่การติดต่อในรูปแบบดิจิทัลมีบทบาทมากขึ้นเรื่อย ๆ โดยมีหน้าม้าที่เป็นคนไทยโทรศัพท์มาอ้างกับเหยื่อว่าเป็นเจ้าหน้าที่กรมศุลกากร หลอกเหยื่อว่ามีทรัพย์สินส่งมาจากต่างประเทศจริง ขอให้เหยื่อโอนเงินค่าภาษีมาให้ เป็นต้น จึงเห็นได้ว่าเทคโนโลยีไม่เพียงแต่เปลี่ยนแปลงสังคมแต่ยังรวมถึงเป็นอำนาจเชิงสาเหตุที่พัฒนาการทางเทคโนโลยีมีต่อความเปลี่ยนแปลงของปัญหาอาชญากรรมในสังคมไทยไปด้วย ซึ่งขึ้นอยู่ที่คนที่นำไปใช้ กรรมวิธีทางเทคนิคของเทคโนโลยีเชิงเครื่องมือในการก่ออาชญากรรมในรูปแบบใหม่ มีเหตุผลเพื่อที่จะไปให้ถึงและได้ประสิทธิภาพสูงสุดในทุก ๆ พื้นที่ของการก่ออาชญากรรม รวมทั้งการครอบครองเทคโนโลยียังทำให้เกิดความได้เปรียบในการก่ออาชญากรรมไซเบอร์ ดังนั้นการก่ออาชญากรรมในยุคใหม่จึงไม่อาจเป็นอิสระหรือปราศจากเทคโนโลยีในการก่ออาชญากรรมได้ เช่น การแพร่ระบาดของโรคติดเชื้อไวรัสโคโรนา 2019 (COVID-19) ส่งผลให้เกิดภัยคุกคามและการก่ออาชญากรรมจากการใช้เทคโนโลยีในสังคมไทยเพิ่มปริมาณมากขึ้นจากอาชญากรรมรูปแบบเดิม เช่น การหลอกลวงผ่านระบบอินเตอร์เน็ตในรูปแบบใหม่ ๆ การฉ้อโกง การหลอกลวงให้เสียทรัพย์จากการซื้อของออนไลน์ได้ง่าย ข่าวลวง (Fake NEWS) ปัญหาขบวนการปล่อยกู้เงินนอกระบบที่ผิดกฎหมาย เป็นต้น หรือปัญหาการแพร่ระบาดของโรคติดเชื้อไวรัสโคโรนา 2019 (COVID-19) เป็นปัญหาอาชญากรรมทางชีวภาพเพื่อใช้เป็นเครื่องมือในการสร้างความเสียหายหรือผลกระทบต่อระบบการเมือง เศรษฐกิจ และสังคมไปทั่วทั้งโลกรวมถึงสังคมไทยด้วย

2.1.3 ความเป็นพลเมืองดิจิทัล (Digital Citizenship)

การกล่าวขานถึง พลเมือง (Citizen) หรือ ความเป็นพลเมือง (Citizenship) ในยุคสังคมกรีกและโรมัน ถือเป็นต้นแบบประชาธิปไตยและมีพัฒนาความเป็นเมืองที่เปลี่ยนแปลงอย่างรวดเร็ว ทำให้ประชาชนในรัฐมีความรู้ความเข้าใจสภาพการณ์ทางสังคมกว้างขวางมากขึ้น อันเป็นผลมาจากการติดต่อสื่อสารระหว่างกันทั้งทางสังคม วัฒนธรรม เศรษฐกิจ การเมืองและการปกครอง ดังนั้น สังคมในศตวรรษที่ 21 ยังมีผู้นำในรัฐต่าง ๆ หยิบยกเอา “ความเป็นพลเมือง” เป็นเครื่องมือพัฒนาการอยู่ร่วมกัน และส่งเสริมให้ระบบการเมืองการปกครองจนก้าวไปสู่ความเป็นพลเมืองในสังคมประชาธิปไตยมากเท่าใด ก็ย่อมได้รับการยอมรับและช่วยเหลือเกื้อกูลให้สังคมนั้นก้าวไปสู่การพัฒนาประเทศภายใต้ระเบียบโลกใหม่โดยง่าย ในทำนองเดียวกันประเทศนั้น ๆ ต้องปลูกฝังรากฐานความรู้ความเป็นพลเมืองให้สืบทอดได้อย่างมั่นคงและยั่งยืน สังคมไทยยุคใหม่ ต้องทบทวนความเป็นพลเมืองที่สามารถสร้างความร่มเย็นเป็นสุขระหว่างกันจึงควรส่งเสริมความรู้ความเข้าใจสาระสำคัญ

ของความเป็นพลเมือง โดยใช้หลัก “เข้าใจ เข้าถึง และเข้าพัฒนา” เพราะความรู้และความเข้าใจพลเมือง จะเกิดขึ้นอย่างเป็นธรรมและเสมอภาคได้ จะต้องเกิดจากการมีส่วนร่วมตามพื้นฐานของพลเมืองที่ควรจะเป็นอย่างเหมาะสม และต้องมีหลักคุณธรรมเป็นพื้นฐานแก่คนเป็นสำคัญ

ในยุคสังคมปัจจุบัน การตระหนักถึงการสร้างความเป็นพลเมืองดิจิทัลเกิดขึ้นอย่างจริงจังและได้รับการกล่าวถึงอย่างแพร่หลาย โดย DQ institute (2022) ให้ความหมายของพลเมืองดิจิทัลว่า ความสามารถในการใช้เทคโนโลยีดิจิทัลและสื่ออย่างปลอดภัย มีความรับผิดชอบและมีจริยธรรม ขณะที่ Kusnadi and Hikmawan (2020) กล่าวว่าความเป็นพลเมืองดิจิทัลถูกกำหนดให้เป็นของบทบาทของผู้คนในสังคมที่แวดล้อมด้วยข้อมูลจำนวนมากในยุคดิจิทัล ผ่านการใช้เทคโนโลยีเครื่องมือและแพลตฟอร์มซึ่งกลายเป็นสิ่งจำเป็นสำหรับประชาชนในการดำรงชีวิตและการทำกิจกรรมทางสังคม ส่งผลต่อการขยายขอบเขตของกิจกรรมของพลเมืองมากขึ้นและสามารถสื่อสารข้อมูลของตนเองผ่านสื่อดิจิทัล ดังนั้นจึงเป็นโอกาสในการเสริมพลังพลเมืองและเอื้อต่อการเป็นประชาธิปไตย เปิดโอกาสให้เกิดการมีส่วนร่วมของการเป็นพลเมืองดิจิทัลที่มีปฏิสัมพันธ์กับสภาพแวดล้อมทางสังคมและการเมืองมากขึ้นเรื่อย ๆ

นอกจากนี้ Moonsun (2016) ยังนิยามความเป็นพลเมืองดิจิทัลออกเป็น 3 มิติ คือ (1) มิติด้านความรู้เกี่ยวกับสื่อและสารสนเทศ ซึ่งพลเมืองดิจิทัลต้องมีความรู้และสามารถเข้าถึง ใช้ สร้างสรรค์ ประเมิน สังเคราะห์ และสื่อสารข้อมูลข่าวสารผ่านเครื่องมือดิจิทัล (2) มิติด้านจริยธรรม พลเมืองดิจิทัลจะต้องใช้อินเทอร์เน็ตได้อย่างปลอดภัย มีจริยธรรม ความรับผิดชอบ ต้องตระหนักถึงผลกระทบที่อาจเกิดต่อสังคม เคารพสิทธิและความรับผิดชอบออนไลน์ และ (3) มิติด้านการมีส่วนร่วมทางการเมืองและสังคม พลเมืองดิจิทัลจะสามารถมีส่วนร่วมทางการเมือง เศรษฐกิจและสังคมโดยใช้อินเทอร์เน็ตเป็นเครื่องมือ

จะเห็นได้ว่า พลเมืองในยุคดิจิทัลจะมีทักษะที่เกี่ยวข้องกับเครื่องมือเทคโนโลยีดิจิทัล รวมถึงทักษะในการรู้คิดขั้นสูงและมีวิจารณญาณ และเนื่องจากมีการใช้เทคโนโลยีออนไลน์มากขึ้น ทำให้เกิดการปฏิสัมพันธ์กับผู้คนมากขึ้น การรู้จักสิทธิตนเอง เคารพผู้อื่น และการปกป้องตนเองและชุมชนจากความเสี่ยงออนไลน์ จึงเป็นทักษะที่สำคัญ นอกจากนี้พลเมืองดิจิทัลยังสามารถใช้อินเทอร์เน็ตในการมีส่วนร่วมทางการการเมืองภาคพลเมือง และการแสดงความคิดเห็นได้มากขึ้น ความท้าทายของการเป็นพลเมืองดิจิทัลคือ ผู้คนในยุคปัจจุบันมีความหลากหลาย ที่เรียกกันว่า Generation ซึ่งมีทั้ง Baby Boomer, Gen X, Gen Y, Gen Z และ Gen Alpha โดยที่ผ่านมาความแตกต่างระหว่างผู้คนในแต่ละรุ่นอาจมีไม่มากนัก แต่การเข้ามากระทบของเทคโนโลยีดิจิทัล หรือ Digital Disruption กับวิถีชีวิตอย่างหนักหน่วง ทำให้ผู้คนที่ถูกเรียกว่า Gen Z และ Gen Alpha มีพฤติกรรม ความคิด และความเชื่อแตกต่างอย่างคนรุ่นก่อนหน้าค่อนข้างชัดเจน เนื่องจากเติบโตมาใน

สิ่งแวดล้อมดิจิทัลหรือชาวดิจิทัลดั้งเดิม (Digital Natives) ที่ทะลายกำแพงด้านสถานที่และเวลา ทำให้ได้เห็น ได้เรียนรู้ ได้ทราบเหตุการณ์รอบตัวและรอบโลกอย่างหลากหลายและรวดเร็ว ในขณะที่ Baby Boomer, Gen X, Gen Y ซึ่งมีวิถีชีวิตแบบผู้อพยพเข้าสู่ยุคดิจิทัล (Digital Immigrants) ต้องมีการปรับตัวในการใช้ชีวิตยุคดิจิทัลอย่างมาก โดยความแตกต่างนี้ถูกกระตุ้นให้ชัดเจนและมีการส่งต่อมากขึ้นด้วยสื่อสังคมออนไลน์ ปรากฏการณ์นี้เองอาจก่อให้เกิดความแตกแยก ความเป็นอื่น และความเกลียดชังได้ นอกจากความท้าทายด้านการจัดการความสัมพันธ์ระหว่างพลเมืองดิจิทัลซึ่งเป็นคนต่างรุ่นแล้ว ยังมีความท้าทายด้านอื่นๆ ที่อาจเกิดขึ้นในประเด็นทางสังคมและเศรษฐกิจ ซึ่งเกิดจากการที่เทคโนโลยีเปลี่ยนแปลงรูปแบบการใช้ชีวิตของมนุษย์

อย่างไรก็ตามการส่งเสริมการเรียนรู้ว่าจะใช้ประโยชน์จากเทคโนโลยีดิจิทัลและปกป้องตนเองจากความเสี่ยงต่างๆ รวมทั้งรู้จักเคารพสิทธิของตนเองและมีความรับผิดชอบต่อสังคมในโลกสมัยใหม่ ไปจนถึงเข้าใจผลกระทบของเทคโนโลยีดิจิทัลที่มีต่อสังคมและใช้มันเพื่อสร้างการเปลี่ยนแปลงทางสังคมในเชิงบวกยังคงเป็นสิ่งที่ต้องดำเนินการอย่างต่อเนื่อง เพราะแม้เราอาจจะใช้อินเทอร์เน็ตราวกับมันเป็นส่วนหนึ่งของชีวิตไปแล้ว แต่ดูเหมือนคนจำนวนมากยังขาดทักษะและความรู้ที่จำเป็นต่อการใช้ประโยชน์จากโอกาสดังกล่าว ยังไม่รู้วิธีลดผลกระทบจากความเสี่ยงในโลกออนไลน์ รวมถึงขาดความเข้าใจเรื่องสิทธิและความรับผิดชอบในโลกยุคดิจิทัล สอดคล้องกับการศึกษาล่าสุดของ Next Billion Users ของ Google พบว่าสิ่งจำเป็นในการดำรงชีวิต เช่น การค้าขาย การศึกษา บริการต่างๆ ถูกย้ายไปไว้บนโลกออนไลน์ตามแนววิถีชีวิตรูปแบบใหม่ที่ถูกปรับจากการแพร่ระบาดของโรคติดเชื้อไวรัสโคโรนา 2019 (COVID-19) ทำให้ความรู้และทักษะด้านดิจิทัลมีความจำเป็น ซึ่งประเทศไทยการบริการเทคโนโลยีสื่อโทรคมนาคมและการเงินเป็นหนึ่งในอุตสาหกรรมชั้นนำในการก้าวไปสู่การเปลี่ยนแปลงสู่ดิจิทัลและนโยบายของประเทศให้ความสำคัญกับเรื่องดังกล่าวอย่างจริงจังหลังจากที่รัฐบาลผลักดันนโยบายเศรษฐกิจดิจิทัล (Digital Economy) เพื่อเสริมสร้างความเข้มแข็งให้กับระบบเศรษฐกิจ อีกทั้งในแผนปฏิรูปประเทศด้านสื่อสารมวลชนเทคโนโลยีสารสนเทศ ที่ให้ความสำคัญกับการพัฒนาพลเมืองและการรู้เท่าทันสื่อ ตลอดจนการเสริมสร้างศักยภาพการใช้เทคโนโลยีของประชาชน ยิ่งไปกว่านั้นวิกฤตโรคติดเชื้อไวรัสโคโรนา 2019 (COVID-19) ได้เร่งการเปลี่ยนแปลงสู่ดิจิทัลให้เร็วมากขึ้น ยิ่งเป็นการตอกย้ำว่าการสร้างความคิดแบบดิจิทัลถือเป็นสิ่งสำคัญต่อความสำเร็จในสภาพแวดล้อมนี้

ทว่า ความก้าวหน้าในเทคโนโลยีไม่อาจจะเป็นตัวชี้วัดในความสำเร็จของการรับมือด้านมืดของออนไลน์ได้ นโยบายในการส่งเสริมความก้าวหน้าด้านอุปกรณ์เครื่องใช้ และเศรษฐกิจควรควบคู่ไปกับการส่งเสริมให้ประชาชนได้คิดวิเคราะห์ และเปิดใจรับข้อมูลที่แตกต่าง เพราะพลเมืองในยุคดิจิทัลนี้ นอกจากต้องมีทักษะในการรักษาความปลอดภัย สิทธิและความรับผิดชอบแล้ว ยังต้อง

เผชิญกับโอกาสและความท้าทายแห่งยุคสมัยที่ได้รับข้อมูลออนไลน์ตั้งแต่ลืมตา (รวมถึงข้อมูลการแพร่ระบาดของโรคติดต่อ) การคิดวิเคราะห์ สังเคราะห์ ก่อนการส่งต่อข้อมูลที่ถูกต้องในชุมชนออนไลน์ จึงจำเป็นอย่างยิ่งในการส่งเสริมให้ประชาชนเป็นพลเมืองดิจิทัลที่สมบูรณ์ ตัวอย่างสังคมดิจิทัลได้เกิดขึ้นท่ามกลางการระบาดของโรคโควิดเช่นกรณีในอินโดนีเซียแสดงให้เห็นอีกด้านหนึ่งของปรากฏการณ์ทางสังคมที่สามารถเห็นชุมชนร่วมกันผ่านโซเชียล เกิดการแบ่งปันผ่านสื่อเพื่อเอาชนะพลวัตและความซับซ้อนของปัญหาที่มีอยู่ การบรรเทาและช่วยเหลือในยุคการแพร่ระบาดของโควิด-19 การปรับเปลี่ยนชีวิตให้เป็นดิจิทัล เช่น การต้องทำงานจากบ้านทุกวัน ซึ่งมีผลอย่างมากสำหรับกิจกรรมทางสังคมและเศรษฐกิจของประชาชน นอกจากนี้โลกดิจิทัลได้กลายเป็นสิ่งที่น่าเชื่อถือในช่วงการระบาดของโควิด-19 เพราะเป็นศูนย์รวมกิจกรรมทางสังคมและเศรษฐกิจรูปแบบใหม่กับวิถีชีวิตใหม่ที่เกิดขึ้นจากการระบาดของโรคโควิด-19 อีกด้านหนึ่งกิจกรรมนี้ก็ได้เปลี่ยนเป็นพลเมืองดั้งเดิมกลายเป็นพลเมืองดิจิทัล และกลายเป็นช่องทางในการสร้างความสามัคคีของชุมชนในยุคของการแพร่ระบาดของโควิด-19 (ณภัทร เรืองนภากุล, 2564)

ผู้วิจัยสนใจว่าความเป็นพลเมืองยุคดิจิทัล น่าจะเป็นปัจจัยที่นำไปสู่ช่องว่างในการพัฒนาและความเหลื่อมล้ำยุคดิจิทัลนั้น ตอกย้ำปัญหาความไม่เป็นธรรมจากยุคแอนะล็อกที่ยังมีคนจำนวนไม่น้อยรวมถึงคนชายขอบยังถูกทิ้งไว้ข้างหลัง ในขณะเดียวกันภาครัฐก็มีภารกิจในการส่งเสริมนวัตกรรมด้านเทคโนโลยี แต่ก็ต้องระมัดระวังและรับมือผลกระทบด้านลบรวมทั้งภัยคุกคามที่มากับยุคดิจิทัลด้วยเช่นกัน อาทิ ปัญหาการแพร่ระบาดของข้อมูลข่าวสาร (Infodemic) ทั้งในลักษณะความเข้าใจผิด (Misinformation) และการตั้งใจบิดเบือน (Disinformation) หรือปรากฏการณ์ที่เรียกกันว่าข่าวลวง (Fake News) รวมไปถึงด้านมืดในยุคดิจิทัลและอาชญากรรมไซเบอร์ (Cyber Crime) ที่กลายเป็นเรื่องใกล้ตัวประชาชนมากขึ้น เพราะสามารถเกิดขึ้นจากที่ใดแบบไร้พรมแดนกับใครเมื่อไหร่ก็ได้ที่ประชาชนอาจตกอยู่ในภาวะมีจุดอ่อนเพราะขาดความรู้ความเข้าใจและความตื่นตัวในการป้องกันตนเองที่ดีพอ รวมทั้งระบบการบังคับใช้กฎหมายในประเทศหรือข้ามประเทศนั้นยังมีข้อจำกัดอีกทั้งความสมดุลในการใช้กฎหมายเพื่อปราบปรามอาชญากรรม แต่ไม่ล้ำเส้นสิทธิเสรีภาพขั้นพื้นฐานของประชาชน ซึ่งเป็นประเด็นที่ส่งผลให้เกิดข้อถกเถียงในสังคมไทยตลอดมา ดังนั้นในเชิงนโยบายสาธารณะ (Public Policy) ภาครัฐจึงต้องมีหลักนิติธรรมควบคู่ไปกับการกำกับเทคโนโลยีและนวัตกรรม พร้อมไปกับความรับผิดชอบของภาคเอกชนต่อสังคม สำคัญที่สุดคือการส่งเสริมความเข้มแข็งของพลเมืองในยุคดิจิทัล (Digital Citizenship) อย่างฉลาดรู้เท่าทันมากพอ (Digital Intelligence) โดยมีศักยภาพในการปรับใช้เทคโนโลยีเพื่อยกระดับคุณภาพชีวิตและรับมือด้านมืดยุคดิจิทัลอย่างปลอดภัยและยืดหยุ่นต่อความท้าทายรูปแบบใหม่ด้วยเช่นกัน (Digital Resilience)

2.1.4 โลกาภิวัตน์ (Globalization)

วิวัฒนาการของสังคมมนุษย์มีลักษณะเช่นเดียวกับปรากฏการณ์ธรรมชาติต่าง ๆ คือ มีการเปลี่ยนแปลง บางสังคมเปลี่ยนแปลงช้าขณะที่บางสังคมเปลี่ยนเร็ว จากสภาพสังคมแบบโบราณกลายเป็นสังคมสมัยใหม่ ที่เห็นชัดเจนคือการเปลี่ยนจากสังคมแบบเกษตรกรรมมาเป็นสังคมอุตสาหกรรม จากสังคมแบบชนบทมาเป็นสังคมเมือง เป็นต้น แนวโน้มที่กำลังเป็นไปขณะนี้ คือ การแพร่กระจายเทคโนโลยีและระบบเศรษฐกิจจากสังคมที่ “พัฒนาแล้ว” ไปสู่สังคมที่ “ด้อยพัฒนา” หรือ “กำลังพัฒนา” ทั่วโลก หรือที่เรียกว่า “โลกาภิวัตน์” การเปลี่ยนแปลงในส่วนหนึ่งส่วนใดของสังคมมักส่งผลกระทบถึงส่วนอื่น ซึ่งอาจเป็นผลกระทบในทางบวกหรือทางลบ โดยนักวิชาการจำนวนหนึ่งเรียกยุคปัจจุบันว่า ยุคโลกาภิวัติ เป็นยุคที่มีการเปลี่ยนแปลงไหลเวียนเคลื่อนย้ายในด้านต่าง ๆ อย่างรวดเร็ว ได้แก่ (1) ชาติพันธุ์ (Ethnoscapes) หรือการไหลเวียน เคลื่อนย้ายของผู้คนไปทั่วโลก เช่น นักธุรกิจ นักศึกษา นักวิชาการ นักท่องเที่ยว แรงงานข้ามชาติ ผู้อพยพ ผู้ร้ายข้ามแดน เป็นต้น (2) เทคโนโลยี (Technoscapes) หรือการไหล เวียนเคลื่อนย้ายของเครื่องจักรกล สินค้า บริการ โรงงาน บริษัท เป็นต้น (3) การเงิน (Finanscapes) หรือการไหลเวียน เคลื่อนย้ายอย่างรวดเร็วของเงินตรา ตลาดหุ้น การลงทุน ข้ามชาติ (4) สื่อสารมวลชนและข่าวสารข้อมูล (Mediascapes) หรือการไหลเวียน เคลื่อนย้ายของข่าวสาร ข้อมูล และภาพลักษณ์ต่าง ๆ ไปทั่วโลก (5) อุดมการณ์ (Ideoscapes) หรือการไหล เวียนเคลื่อนย้ายของอุดมการณ์ แนวคิดทฤษฎีจากที่หนึ่ง ไปยังที่หนึ่งของโลกอย่างรวดเร็ว (Appadurai, 1990) ซึ่งการไหลเวียนเคลื่อนย้ายดังกล่าว ไม่ได้ก่อให้เกิดความเหมือนหรือคล้ายคลึงกันในทุกมุมของโลก หากแต่ก่อให้เกิดความหลากหลายและการผสมผสานของสิ่งต่าง ๆ ที่ปรากฏขึ้นในสังคมที่แนวคิดเดิมไม่อาจอธิบายได้

ในปัจจุบัน ทั่วโลกอยู่ในช่วงเปลี่ยนผ่านสู่การเป็นสังคมดิจิทัลอย่างก้าวกระโดด มีการนำเทคโนโลยีดิจิทัลมาปรับใช้ในทุกมิติของการดำรงชีวิตในสังคม ความตระหนักรู้ ความเข้าใจ และการมีภูมิคุ้มกัน ในการใช้เทคโนโลยีดิจิทัลจึงเป็นสิ่งสำคัญต่อการปรับ ตัวให้สอดคล้องกับบริบทของสังคมยุคโลกาภิวัตน์ ซึ่งขณะนี้เทคโนโลยีได้เข้ามามีบทบาทต่อการดำเนินชีวิตประจำวันของประชากรโลก มีบทบาทในด้านการทำงานมากขึ้น ทั้งการใช้ปัญญาประดิษฐ์ (AI) และเทคโนโลยีอินเทอร์เน็ตของสรรพสิ่ง (Internet of Things: IoT) ส่งผลให้รูปแบบธุรกิจและอาชีพเปลี่ยนแปลง ในขณะที่บางอาชีพเลือนหายไปอย่างไม่มีวันหวนกลับเนื่องจากแรงงานคนถูกทดแทนด้วยเทคโนโลยีและเทคโนโลยีทำงานได้ดีกว่า อีกทั้งช่วยลดต้นทุนให้กับธุรกิจอย่างมหาศาล ทำให้แรงงานคนหลากหลายอาชีพกำลังก้าวเข้าสู่สภาวะตกงาน ในขณะเดียวกันอาจทำให้ตำแหน่งงานที่มีอยู่ในปัจจุบันโดยเฉพาะแรงงานรายได้น้อยและแรงงานทักษะต่ำ หายไปถึง 85 ล้านตำแหน่ง สะท้อนให้เห็นได้ชัดเจนว่าถึงแม้บางอาชีพจะยังไม่สามารถเปลี่ยนไปใช้หุ่นยนต์ได้แต่การพัฒนาอย่างต่อเนื่องจะ

ทำให้ระบบอัตโนมัติและหุ่นยนต์สามารถเข้ามาแทนที่ตำแหน่งงานต่าง ๆ ได้มากขึ้น ทั้งนี้ ในปี พ.ศ. 2563 สภาเศรษฐกิจโลก (World Economic Forum) ประเมินไว้ว่า การพัฒนาเครื่องจักรและหุ่นยนต์ให้มีความสามารถที่ซับซ้อนและทำงานในตำแหน่งงานที่ใช้ทักษะของมนุษย์จะเพิ่มมากขึ้น อาทิ การให้คำปรึกษา การตัดสินใจ การใช้เหตุผล การสื่อสาร และการมีปฏิสัมพันธ์ รวมทั้งกลุ่มงานในอุตสาหกรรมสีเขียว ปัญญาประดิษฐ์ วิศวกร Big Data และ Cloud Computing จะเพิ่มขึ้นกว่า 97 ล้านตำแหน่งทั่วโลกภายในปี พ.ศ. 2568 หรืออีก 5 ปีข้างหน้า (สำนักงานสภาพัฒนาเศรษฐกิจและสังคมแห่งชาติ, 2561)

สังคมจึงจำเป็นจะต้องพัฒนาให้เท่าทันกับโลกาภิวัตน์ ประกอบกับการดำเนินตามแผนงาน มาตรการเชิงปฏิบัติและโครงการขับเคลื่อนสำคัญต่าง ๆ ให้บรรลุเป้าหมายในการปฏิรูปประเทศไทยสู่ดิจิทัลไทยแลนด์ (Digital Thailand) โดยเชื่อมโยงทุกองค์ประกอบผ่านกลไกการขับเคลื่อนตามบทบาทและหน้าที่ของหน่วยงานทุกภาคส่วน เพื่อสร้างระบบนิเวศทางดิจิทัล (Digital Ecosystem) ซึ่งจำเป็นต้องอาศัยการยอมรับและการขับเคลื่อนจากหลายภาคส่วน ทั้งหน่วยงานขับเคลื่อนหลัก หน่วยงานขับเคลื่อนสนับสนุน รวมถึงหน่วยงานอื่น ๆ ทั้งในภาครัฐและภาคเอกชน เพื่อให้เกิดการเปลี่ยนแปลงและเกิดความพร้อมในการสร้างความร่วมมืออย่างมีประสิทธิภาพ และใช้ศักยภาพที่มีอยู่อย่างเต็มที่เพื่อผลักดันให้เกิดนวัตกรรมและเทคโนโลยีรูปแบบใหม่ สร้างโอกาสทางธุรกิจใหม่ ๆ อย่างไร้ขีดจำกัดและสร้างความได้เปรียบในเชิงแข่งขันให้กับประเทศไทย โดยมีมาตรฐานและความเป็นหนึ่งเดียวเพื่อยกระดับและขับเคลื่อนการพัฒนาเศรษฐกิจและสังคมดิจิทัลของประเทศไทย

ผู้วิจัยสนใจว่า โลกาภิวัตน์ (Globalization) น่าจะเป็นปัจจัยที่ก่อให้เกิดภัยคุกคามที่มาจากผู้ก่อเหตุใช้เทคโนโลยีดิจิทัลที่ล้ำสมัยเป็นเครื่องมือในการหลอกลวงประชาชนที่เจ้าหน้าที่รัฐไม่สามารถตามจับได้ เนื่องจากเป็นอาชญากรรมที่ไม่มีเชื้อชาติ ไม่มีขอบเขตประเทศ นอกจากนี้ ความเป็นนิรนาม ความปลอดภัย ความเป็นส่วนตัว โลกาภิวัตน์ และสิทธิเสรีภาพของประชาชน อีกทั้งยังเอื้อต่อการก่ออาชญากรรมไซเบอร์ จึงมีความจำเป็นอย่างยิ่งที่รัฐต้องสนับสนุนให้ประชาชน มีความตระหนักรู้ ความเข้าใจ และมีภูมิคุ้มกันในการใช้เทคโนโลยี เพื่อป้องกันภัยที่จะตามมาในอนาคต การส่งเสริมให้ประชาชนมีความพร้อมเข้าสู่สังคมดิจิทัล (Digital Literacy and Resilience) หมายถึง ประชาชนทุกคนมีความตระหนักรู้ ความเข้าใจ และมีทักษะในการใช้เทคโนโลยีดิจิทัลให้เกิดประโยชน์และสามารถเข้าถึงบริการต่าง ๆ ได้อย่างมีภูมิคุ้มกัน มีความรับผิดชอบในการใช้งาน ซึ่งหากประชาชนมีทักษะดังกล่าว จะช่วยยกระดับสังคมให้มีความก้าวหน้าขึ้น ตลอดจนยกระดับคุณภาพชีวิตของประชาชนทั้งประเทศ ไม่ตกเป็นเหยื่อของภัยคุกคามทางดิจิทัล

2.1.5 เครือข่ายสังคม (Social networks)

เครือข่ายสังคม เป็นโครงสร้างทางสังคมที่ สร้างขึ้นจากกลุ่มของผู้กระทำ เช่น ปัจเจกบุคคลหรือองค์การ และความสัมพันธ์ทวิภาคระหว่างผู้กระทำเหล่านี้ ทัศนคติเครือข่ายสังคมช่วยให้สามารถวิเคราะห์โครงสร้างของหน่วยสังคมทั้ง มวลได้อย่างกระจ่างแจ้ง การศึกษาโครงสร้างเหล่านี้ใช้การวิเคราะห์เครือข่ายสังคมเพื่อระบุแบบอย่างท้องถิ่นหรือทั่วโลก ค้นหาหน่วยสังคมที่มีอิทธิพล และตรวจวัดพลวัตของเครือข่าย เครือข่ายสังคมและการวิเคราะห์เป็นสาขาวิชาสหวิทยาการโดยแท้ อันปรากฏขึ้นจากจิตวิทยาสังคม สังคมวิทยา สถิติศาสตร์ และทฤษฎีกราฟ จอร์จ ซิมเมิล (Georg Simmel) ได้แต่งตำราเกี่ยวกับทฤษฎีเชิงโครงสร้างในสังคมวิทยา เพื่อเน้นให้เห็นถึงพลวัตของความสัมพันธ์ไตรภาคและ “ข่ายโยงใยของการเข้าร่วมกลุ่ม” จาค็อบ โมเรโน (Jacob Moreno) ก็มีชื่อเสียงในเรื่องการพัฒนาผังสังคมมิติ (sociogram) ขึ้นเป็นคนแรกในคริสต์ทศวรรษ 1930 เพื่อศึกษาความสัมพันธ์ระหว่างบุคคล แนวการศึกษาเหล่านี้ถูกทำให้เป็นระเบียบแบบแผนเชิงคณิตศาสตร์ในคริสต์ทศวรรษ 1950 จากนั้นทฤษฎีและวิธีการต่าง ๆ ของเครือข่ายสังคมก็เป็นที่แพร่หลายในสังคมศาสตร์และพฤติกรรมศาสตร์ในคริสต์ ทศวรรษ 1980 (Technology News, 2016) ปัจจุบันนี้การวิเคราะห์เครือข่ายสังคมเป็นหนึ่งในกระบวนทัศน์หลักของสังคม วิทยาร่วมสมัย และถูกนำไปใช้ในศาสตร์เชิงสังคมและรูปนัยอื่น ๆ อีกจำนวนหนึ่ง นอกจากนี้เครือข่ายสังคมก่อร่างขึ้นเป็นส่วนหนึ่งของสาขาวิชาวิทยาการเครือข่ายที่เพิ่งเริ่มต้น ควบคู่ไปกับเครือข่ายซับซ้อนอื่น ๆ

แนวโน้มล่าสุดของการใช้อินเทอร์เน็ตคือการใช้อินเทอร์เน็ตเป็นแหล่งพบปะสังสรรค์เพื่อสร้างเครือข่ายสังคม ซึ่งพบว่าปัจจุบันเว็บไซต์ที่เกี่ยวข้องกับกิจกรรมดังกล่าวกำลังได้รับความนิยมอย่างแพร่หลายเช่น เฟซบุ๊ก (Facebook) ทวิตเตอร์ (Twitter) และการใช้เริ่มมีการแพร่ขยายเข้าไปสู่การใช้อินเทอร์เน็ตผ่านโทรศัพท์มือถือ (Mobile Internet) มากขึ้น เนื่องจากเทคโนโลยีปัจจุบันสนับสนุนให้การเข้าถึงเครือข่ายผ่านโทรศัพท์มือถือทำได้ง่ายขึ้นมาก และเมื่อเครือข่ายสังคมเป็นกลุ่มของบุคคลที่มีความสัมพันธ์กัน การวิเคราะห์เครือข่ายสังคมจึงเน้นที่บุคคลที่มีความสัมพันธ์เชื่อมโยงแต่ละบุคคลหรือกลุ่มบุคคลเข้าด้วยกันเป็นจุดสำคัญ การวิเคราะห์เครือข่ายสังคมจึงไม่เพียงเป็นวิธีการวิเคราะห์ แต่เป็นกลุ่มของทฤษฎี โมเดลและการประยุกต์ที่อธิบายแนวคิดของความสัมพันธ์และกระบวนการความสัมพันธ์ที่อธิบายโดยการเชื่อมโยงระหว่างหน่วยของแต่ละบุคคล เช่น ครู นักเรียน เขตพื้นที่ การศึกษา เป็นต้น เรียกว่าเป็นแนวคิดของการวิเคราะห์เครือข่ายทางสังคม นอกเหนือจากการวิเคราะห์ความสัมพันธ์แล้ว การวิเคราะห์เครือข่ายสังคมยังเกี่ยวข้องกับการที่แต่ละบุคคลและการกระทำของแต่ละบุคคลเป็นอิสระ การเชื่อมโยงความสัมพันธ์ระหว่างบุคคลเป็นโอกาสของการแลกเปลี่ยนทรัพยากรระหว่างกัน รูปแบบของความสัมพันธ์ระหว่างบุคคลเป็นโครงสร้างสังคม

ที่เกิดสภาพแวดล้อมที่ให้โอกาสแต่ละบุคคล และรูปแบบเครือข่ายสังคมทำให้เกิดรูปแบบความสัมพันธ์ระหว่างบุคคล

ปัจจุบัน เครือข่ายสังคมไม่ได้เป็นเพียงความสัมพันธ์ที่เกิดขึ้นบนโลกแห่งความเป็นจริงเท่านั้น แต่ยังหมายรวมถึงเครือข่ายที่เกิดจากการมีปฏิสัมพันธ์ด้วยเทคโนโลยีดิจิทัลเป็นรูปแบบของเว็บไซต์ในการสร้างเครือข่ายสำหรับผู้ใช้งานในอินเทอร์เน็ต หรือที่เรียกว่า สังคมออนไลน์ (Social Network) สามารถสร้างสรรค์สังคมใหม่ๆให้กับทุกคน และเชื่อมโยงการสื่อสารภายในองค์กร และภายนอกองค์กรเข้าด้วยกันได้อย่างมีประสิทธิภาพ ซึ่งเป็นสิ่งที่ตอบสนองรูปแบบชีวิตของมนุษย์ยุคปัจจุบันนั่นเอง โดยภาพรวมของ Social Network เป็นสื่อที่มีประสิทธิภาพในการสื่อสารกับองค์กร จากคำพูดของมนุษย์ได้เป็นอย่างดี ผู้บริหารองค์กรขนาดใหญ่จะสามารถสื่อสารกับคนในองค์กรได้อย่างมีประสิทธิภาพ ไม่ต้องประสบปัญหาการบิดเบือนข้อความ หรือการสื่อสารที่ตกหล่นอีกต่อไป ครูอาจารย์สามารถให้แง่คิดหรือสิ่งละอันพันละน้อยแก่ลูกศิษย์ได้โดยไม่จำเป็นต้องรอให้พูดกันทีเดียวคราวละยาวๆ นักวิจัยอาจพบอะไรที่น่าสนใจแล้วสื่อสารให้รู้กันทุกคนในเครือข่ายเดียวกันได้ทันทีเพื่อให้ทีมรับรู้สิ่งน่าสนใจไปพร้อมๆกัน

ผู้วิจัยสนใจว่าเครือข่ายสังคมโดยเฉพาะสังคมออนไลน์ น่าจะเป็นปัจจัยที่กระตุ้นและสร้างโอกาสให้กับผู้ไม่ประสงค์ดีในการริเริ่มก่ออาชญากรรมและภัยคุกคามต่างๆ ได้ง่ายยิ่งขึ้น ทั้งอาชญากรรมแบบดั้งเดิมและอาชญากรรมไซเบอร์ รวมถึงอาชญากรรมอื่นๆ มีความเชื่อมโยงและสัมพันธ์กัน เช่น คดีแก๊งคอลเซ็นเตอร์ การหลอกลวงรักออนไลน์ กลโกงการซื้อขายสินค้าของออนไลน์ เป็นต้น ซึ่งเป็นอาชญากรรมที่มีความสัมพันธ์กับเทคโนโลยี ทำให้เชื่อมโยงถึงกันได้ง่ายผ่านเครือข่ายสังคมระหว่าง มนุษย์ เครื่องมือหรืออุปกรณ์สื่อสาร และสภาพแวดล้อมที่สนับสนุนการสร้างเครือข่ายแบบไร้พรมแดนบนโลกไซเบอร์ ความเป็นเครือข่ายสังคมนี้จึงเป็นส่วนสำคัญที่ก่อให้เกิดภัยคุกคามและอาชญากรรวมกลุ่มเป็นองค์กรในการก่ออาชญากรรมไซเบอร์ และอาชญากรรมรูปแบบใหม่ๆมากขึ้นในอนาคต

2.1.6 ทฤษฎีการเปลี่ยนแปลงทางสังคม (Social Change Theory)

การเปลี่ยนแปลง (Change) คือ การทำให้สิ่งต่างๆ เปลี่ยนไปจากที่เป็นอยู่เดิม ไม่เจาะจงว่าเป็นแบบวิธีใด ไม่เจาะจงทิศทาง หรืออัตราความเร็ว เช่น การแลกเปลี่ยนเงินตรา ลมเปลี่ยนทิศทาง สังคมเปลี่ยน โดยองค์ประกอบของโครงสร้างทางสังคม ได้แก่ ความสัมพันธ์ทางสังคม ค่านิยม ความเชื่อ อัตลักษณ์ และระบบความรู้ เป็นต้น

การเปลี่ยนแปลงทางสังคม (Social Change) หมายถึง การที่ระบบสังคม กระบวนการ แบบอย่าง หรือรูปแบบทางสังคมได้เปลี่ยนแปลงไปไม่ว่าจะเป็นด้านใดก็ตาม การเปลี่ยนแปลงทางสังคมนี้อาจจะเป็นไปในทางก้าวหน้าหรือถดถอย เป็นไปได้อย่างถาวรหรือชั่วคราว โดยการวางแผนให้เป็นไปหรือเป็นไปเอง และที่เป็นประโยชน์หรือให้โทษก็ได้ทั้งสิ้น (ราชบัณฑิตยสถาน, 2524) ปัจจัยที่มีผลต่อการเปลี่ยนแปลงทางสังคม เช่น สภาพแวดล้อมและประชากร การพัฒนาเศรษฐกิจ ความเชื่อของคนในสังคม การเคลื่อนไหวทางสังคม กระบวนการทางวัฒนธรรม การประดิษฐ์คิดค้นสิ่งใหม่ๆ โดยรูปแบบการเปลี่ยนแปลงทางสังคม ได้แก่ การเปลี่ยนแปลงแบบเส้นตรง เป็นการเปลี่ยนแปลงทางสังคมจากอารยธรรมขั้นต่ำไปสู่สังคมที่มีความเจริญของอารยธรรมระดับสูงขึ้นต่อไป และการเปลี่ยนแปลงแบบวัฏจักร เป็นการเปลี่ยนแปลงทางสังคมที่ไม่มีความสม่ำเสมอ ค่อย ๆ เจริญก้าวหน้าไปเรื่อย ๆ จนถึงที่สุดก็จะเสื่อมสลายไป ซึ่งตามแนวคิดทฤษฎีการเปลี่ยนแปลงสังคม (Vago Steven, 2004) ประกอบด้วย

(1) ทฤษฎีวิวัฒนาการ (Evolutionary Theory) เป็นแนวความคิดที่ได้รับอิทธิพลจากทฤษฎีวิวัฒนาการทางชีววิทยาของ ชาร์ลส์ ดาร์วิน (Charles Darwin) ซึ่งกล่าวว่า การเปลี่ยนแปลงของสังคมเป็นกระบวนการที่มีการเปลี่ยนแปลงอย่างเป็นขั้นตอนตามลำดับจากขั้นหนึ่งไปสู่อีกขั้นหนึ่งในลักษณะที่มีการพัฒนาและก้าวหน้ากว่าขั้นที่ผ่านมา มีการเปลี่ยนแปลงจากสังคมที่มีรูปแบบเรียบง่ายไปสู่รูปแบบที่สลับซับซ้อนมากขึ้น และมีความเจริญก้าวหน้าไปเรื่อย ๆ จนเกิดเป็นสังคมที่มีความสมบูรณ์ ในขณะที่ Auguste Comte (1798 – 1857) เสนอว่า สังคมมนุษย์มีพัฒนาการและการเปลี่ยนแปลงด้านความรู้ (Knowledge) ผ่าน 3 ขั้นตอนตามลำดับ คือ จากขั้นเทววิทยา (Theological Stage) ไปสู่ขั้นอภิปรัชญา (Metaphysical Stage) และไปสู่ขั้นวิทยาศาสตร์ (Positivistic Stage) ในทำนองเดียวกัน ทัลคอทท์ พาร์สัน (Talcott Parsons, 1950 - 1951) นักสังคมวิทยาชาวอเมริกัน ได้นำเอาแนวความคิดเรื่องวิวัฒนาการมาประกอบกับแนวความคิดของ เอมิลล์ เดอร์ไคม์ (Emile Durkheim, 1858 - 1917) และ เฮอร์เบิร์ต สเปนเซอร์ (Herbert Spencer, 1820 - 1903) มาผสมกับทฤษฎีการกระทำของตน ทำให้ได้ความจริงเกี่ยวกับวิวัฒนาการ 4 ประการ คือ วิวัฒนาการทำให้เกิดการจำแนกความแตกต่างระหว่างระบบทั้ง 4 ทำให้เกิดการจำแนกความแตกต่างในแต่ละระบบ ทำให้เกิดความเร่งในเรื่องบูรณาการ เกิดหน่วยหรือโครงสร้างด้านบูรณาการใหม่ และวิวัฒนาการทำให้พิสัย สามารถในการดำรงอยู่ของแต่ละระบบมีมากขึ้นรวมทั้งของสังคมมนุษย์ด้วย (ดิเรกฤทธิ์ บุษยธนากรณ์, 2563)

(2) ทฤษฎีความขัดแย้ง (Conflict Theory) เป็นแนวความคิดที่มีข้อสมมุติฐานที่ว่าพฤติกรรมของสังคมสามารถเข้าใจได้จากความขัดแย้งระหว่างกลุ่มต่าง ๆ และบุคคลต่าง ๆ เพราะการแข่งขันในการเป็นเจ้าของทรัพยากรที่มีค่าและหายาก ซึ่ง Karl Marx (1897 - 1958) มีความเชื่อว่าการเปลี่ยนแปลงของทุก ๆ สังคม จะมีขั้นตอนของการพัฒนาทางประวัติศาสตร์ห้าขั้น โดยแต่ละ

ขั้นจะมีวิธีการผลิต (Mode of Production) ที่เกิดจากความสัมพันธ์ของอำนาจของการผลิต (Forces of Production) ซึ่งทำให้เกิดการเปลี่ยนแปลงทางเศรษฐกิจ ที่เป็นโครงสร้างส่วนล่างของสังคม (Substructure) และเมื่อโครงสร้างส่วนล่างมีการเปลี่ยนแปลงจะมีผลทำให้เกิดการผันแปรและเปลี่ยนแปลงต่อโครงสร้างส่วนบนของสังคม (superstructure) ซึ่งเป็นสถาบันทางสังคม เช่น รัฐบาล ครอบครัว การศึกษา ศาสนา รวมถึงค่านิยม ทัศนคติและบรรทัดฐานของสังคม เป็นต้น (ดิเรกฤทธิ์ บุษยธนากรณ์, 2563)

(3) แนวความคิดการเปลี่ยนแปลงทางสังคมของกลุ่มทฤษฎีโครงสร้างหน้าที่ มีลักษณะดังนี้ (1) สังคมทั้งหมดเป็นระบบหนึ่งที่แต่ละส่วนจะมีความสัมพันธ์ระหว่างกัน (2) ความสัมพันธ์ คือ สิ่งที่สนับสนุนซึ่งกันและกันอย่างเป็นเหตุเป็นผล (3) ระบบสังคมเป็นการเคลื่อนไหวเข้าสู่ความสมดุลการปรับความสมดุลของระบบจะทำให้เกิดการเปลี่ยนแปลงภายในระบบตามไปด้วย ความต่อเนื่องของกระบวนการของข่าวสารจากภายในและภายนอก นอกจากนี้ยังมองว่า ความขัดแย้ง ความตึงเครียด และความไม่สงบสุขภายในสังคมก็เป็นสาเหตุหนึ่งของการเปลี่ยนแปลงทางสังคม นักสังคมวิทยากลุ่มทฤษฎีโครงสร้างหน้าที่ เช่น Robert K. Merton (ค.ศ. 1910 - 2003) Emile Durkheim (ค.ศ. 1858 - 1917) และ Talcott Parsons (ค.ศ. 1902 - 1979) เป็นต้น

(4) ทฤษฎีจิตวิทยาสังคม (Social Psychological Theory) ทฤษฎีนี้กล่าวว่า การพัฒนาทางสังคมเกิดจากการทำงานของปัจจัยทางด้านจิตวิทยาที่เป็นแรงขับให้ประชาชนมีการกระทำ มีความกระตือรือร้น มีการประดิษฐ์ มีการค้นพบ มีการสร้างสรรค์ มีการแย่งชิง มีการก่อสร้างและพัฒนาสิ่งต่าง ๆ ภายในสังคม นักสังคมวิทยาที่ใช้ปัจจัยทางด้านจิตวิทยาอธิบายการเปลี่ยนแปลงทางสังคม เช่น Max Webber (ค.ศ. 1864 - 1920) และ Everett E. Hagen (ค.ศ. 1906 - 1993) เป็นต้น

(5) ทฤษฎีเทคโนโลยี (Technology Theory) ทฤษฎีนี้มีฐานคติ (Assumption) อยู่ 3 ประการ คือ ประการแรก การประดิษฐ์สิ่งใหม่ขึ้นมาจะเพิ่มความสลับซับซ้อนของวัฒนธรรม ชีวิตของมนุษย์ก็สับสนขึ้นตามเนื้อหาของวัฒนธรรมนั้น ประการที่ 2 การกระดิษฐ์สิ่งใหม่จะเป็นเหตุให้เกิดการเปลี่ยนแปลงทางเศรษฐกิจ กล่าวคือ เทคนิคใหม่ ๆ จะทำให้การผลิตเพิ่มขึ้น การวิภาคสินค้าและบริการก็กระจายออกไปในสังคมมากขึ้น ประการที่ 3 โครงสร้างทางสังคมจะมีการปรับตัวให้เป็นระบบการผลิต การวิภาค และการบริโภค การเปลี่ยนแปลงทางสังคมเป็นผลจากกระบวนการปรับตัวนี้เอง

จะเห็นได้ว่า การเปลี่ยนแปลงหลายสิ่งหลายอย่างในชีวิตของมนุษย์เป็นผลมาจากการคิดค้นประดิษฐ์สิ่งใหม่ขึ้นมานับตั้งแต่เข็มทิศ วงล้อ เครื่องพิมพ์ เครื่องจักรกลต่าง ๆ ตลอดจนเครื่องมือสื่อสารและสภาพสิ่งต่าง ๆ การประดิษฐ์คิดค้นสิ่งใหม่ ๆ โดยอาศัยความเจริญทางวิทยาศาสตร์และเทคโนโลยี มีส่วนทำให้มนุษย์เปลี่ยนแปลงชีวิตความเป็นอยู่เป็นอันมาก โดยเฉพาะการใช้เครื่องทุ่นแรงในการผลิตสินค้า ซึ่งมีผลให้ประเทศต่าง ๆ เจริญขึ้นอย่างรวดเร็ว กลายจากประเทศเกษตรกรรมเป็นประเทศอุตสาหกรรม ทำให้มนุษย์ซึ่งแต่ก่อนทำการผลิตสินค้าภายใน

ครัวเรือน ต้องกลายเป็นลูกจ้างในโรงงาน อุตสาหกรรมหรือขายแรงงานแก่ผู้อื่น การผลิตสินค้าโดยใช้เครื่องจักร แม้จะได้ผลผลิตทีละมาก ๆ ในระยะเวลาอันสั้น แต่ก็ได้ทำลายงานศิลปะของมนุษย์ไปหมดสิ้น และทำให้โลกสูญสิ้นความสวยงามไปด้วย ประเทศที่เจริญทางอุตสาหกรรม งานศิลปะที่ใช้ฝีมือมนุษย์นับวันจะหมดไป ซึ่งเป็นผลให้จิตใจของมนุษย์แข็งกระด้าง ขาดความประณีต เพราะห่างไกลจากความสวยงามและสิ่งน่าพึงชมต่าง ๆ

2.1.7 แนวคิดสังคมแห่งความเสี่ยงภัย (Risk Society)

สังคมทันสมัยกำลังถึงจุดสิ้นสุด และมนุษยชาติกำลังก้าวเข้าสู่ปรากฏการณ์ที่เรียกว่า “สังคมแห่งความเสี่ยง” (Risk Society) ในขณะที่สังคมไทยกำลังก้าวไปสู่ความทันสมัย ภาวะความอันตรายก็เพิ่มปริมาณและรูปแบบใหม่ ๆ มากขึ้นทุกขณะ ขณะเดียวกันความรู้สึกหวาดระแวงได้แผ่ขยายเพิ่มไปในหลายๆพื้นที่ของสังคม และแม้ว่าจะผู้เชี่ยวชาญจากแวดวงวิชาการมาให้ความมั่นใจว่าปลอดภัยจากภยันตรายเพียงใด ความรู้สึกไม่ไว้เนื้อเชื่อใจยังคงดำรงอยู่ สิ่งเหล่านี้ เกิดขึ้นไม่ใช่เพราะสังคมรู้สึกหวาดระแวงอย่างเกินควรแต่เพียงฝ่ายเดียวไม่ แต่สังคมไทยกำลังกลายเป็นสังคมความเสี่ยงโดยไม่ตระหนักรู้ ย่อมเป็นเรื่องที่เลี่ยงไม่ได้หากประชาชนทั่วไปจะรู้สึกตระหนกต่อความเสี่ยงอันนำมาสู่ความทุกข์ร้อน ภยันตรายไม่ว่าจะใหญ่หรือเล็กล้วนปรากฏอยู่ทุกหนแห่ง องค์ประกอบอันหนึ่งของอันตรายปรากฏให้เห็นในการดำเนินกิจกรรมในทุกๆ เรื่องของมนุษย์และที่แฝงตัวอยู่ในสิ่งแวดล้อม บ่อยครั้งความเสี่ยงต่างๆ ก็มักจะมาจากแดนไกล หรือแม้แต่ไม่อาจรับรู้ที่มาที่ไปของความเสี่ยงนั้นๆได้ (Beck, 1992) ยกตัวอย่างเช่น การที่สังคมโลกกำลังเผชิญหน้ากับผู้ก่อการร้าย (terrorism) ที่กระจายตัวไปทั่ว การเผชิญหน้ากับโรคภัยไข้เจ็บชนิดใหม่ๆ ที่มีแนวโน้มจะระบาดรุนแรงในวงกว้าง อาทิเช่น โรคซาร์สไข้หวัดนก ไข้หวัด 2009 โรควัวบ้า การเผชิญหน้ากับความผันผวนของวิกฤติสิ่งแวดล้อมและสภาพภูมิอากาศโลกที่แปรปรวณขนานใหญ่ ไปจนถึงการเผชิญหน้ากับความเสี่ยงที่แม้จะยังไม่เกิดขึ้นแต่ก็สร้างความกังวลที่กระจายตัวไปทั่ว

“สังคมสมัยใหม่” สู่ “สังคมแห่งความเสี่ยง” การรับรู้ของสังคมต่อเรื่อง “ความเสี่ยง” มีการเปลี่ยนผ่านอย่างเป็นจริงเป็นจังตั้งแต่ราวศตวรรษที่ 20 เป็นต้นมา ส่วนหนึ่งพอจะอนุมานได้ว่า ความสนใจดังกล่าวได้รับอิทธิพลจากกระแสลัทธิหลังสมัยใหม่ (Postmodernism) ที่ทรงพลังในโลกสังคมศาสตร์ในช่วงเวลาเดียวกัน และเป็นกระแสทฤษฎีที่ตั้งคำถามกับปรากฏการณ์ของลัทธิสมัยใหม่ (Modernism) ที่ครอบงำมนุษยชาติมาแล้วหลายศตวรรษ และจากสังคมสมัยใหม่ (Modern Society) ไปสู่สังคมแห่งความเสี่ยง (Risk Society) จากหลายแง่มุมที่นักวิชาการได้พัฒนาแนวความคิดต่อเรื่องความเสี่ยง มีดังนี้

(1) วัฒนธรรมความเสี่ยง เป็นแนวความคิดที่ แมรี่ ดักลาส (Mary Douglas 1921 – 2007) ได้อิทธิพลทางความคิดมาจากนักสังคมวิทยาอย่าง เอมิล เดอร์ไคม์ (Emile Durkheim) ที่ว่า เงื่อนไขทางสังคม เป็นตัวกำหนดการแสดงออกซึ่งความรู้สึกหรือการอธิบายเหตุการณ์ต่าง ๆ รอบตัวเรา โดยเฉพาะอย่างยิ่ง ในยุคที่ความเข้มแข็ง สมานฉันท์ในสังคม (Solidarity) ถูกทำลายลง มนุษย์จะเริ่มรู้สึกว่าตนเองอ่อนแอลงและเข้าสู่สภาวะความเสี่ยงมากขึ้น ต่อมาดักลาสได้พัฒนาความคิดดังกล่าวออกไปสู่การวิเคราะห์การรับรู้ของสังคมต่อเรื่องความเสี่ยงเพิ่มขึ้น และได้อธิบายว่า คนที่อยู่ในสังคมที่แตกต่างกัน มีแนวโน้มที่จะรับรู้หรือสร้างความหมาย (Make Sense) ต่อความเสี่ยงที่แวดล้อมตัวเขาไม่เหมือนกันด้วย เช่น คนที่อยู่ในสังคมแบบตลาดเสรี มักมีแนวโน้มจะเชื่อว่า การแข่งขันในด้านต่าง ๆ นั้น มีเหตุที่มาของความเสี่ยงในชีวิต อาทิ ความเสี่ยงในการแข่งขันทางธุรกิจการตลอด และมักจะทำให้ระบบดั้งเดิมเปลี่ยนแปลง นำไปสู่สภาวะความเสี่ยง เพราะฉะนั้น ผู้คนในระบบราชการจึงมักมีลักษณะอนุรักษ์นิยมและกังวลต่อการเผชิญหน้ากับปัจจัยใหม่ๆที่เข้ามาจากภายนอกระบบ

(2) สังคมแห่งความเสี่ยง แนวคิดนี้เป็นความสัมพันธ์ระหว่าง “ความเสี่ยง” กับ “ความเป็นสมัยใหม่” โดย อูริช เบ็คส์ (Ulrich Beck 1992) ศาสตราจารย์ด้านสังคมวิทยาชาวเยอรมัน ได้วิเคราะห์เส้นทางพัฒนาการของสังคมจากยุคสังคมอุตสาหกรรม (Industrial Society) มาสู่ยุคสังคมหลังอุตสาหกรรม (Post-industrial Society) ว่า ภายใต้สังคมแห่งความเสี่ยงนั้น มนุษย์เรากำลังเผชิญหน้ากับความเสี่ยงนานาชนิด ที่มีแนวโน้มจะเป็น นามธรรมหรือสิ่งที่จับต้องได้ยาก (อาทิ ความเสี่ยงจากผลิตภัณฑ์เกษตรแบบ GMO) คาดทำนายผลลำบาก (อาทิ กรณีความเสี่ยงจากภาวะเรือนกระจกและโลกร้อน) ยากต่อการค้นหาสาเหตุ (อาทิ กรณีผู้ก่อการร้ายข้ามชาติซึ่งยากจะสืบค้นที่มาได้) ควบคุมผลไม่ได้ (อาทิ กรณีการเกิดแผ่นดินไหวและสึนามิ) ขยายผลไปได้เรื่อย ๆ อย่างรวดเร็ว (อาทิ กรณีการระบาดของโรคซาร์ส ไข้หวัดนก และไข้หวัด 2009) และที่สำคัญคือ ความเสี่ยงยุคหลังอุตสาหกรรมยังเป็นกระบวนการที่สังคมสร้างขึ้น (Social Constructs) (อาทิ ปรากฏการณ์วันสิ้นโลกปี 2012 ที่ได้รับการผลิตและเผยแพร่ผ่านสื่อต่าง ๆ อย่างสำนักข่าวข้ามชาติและภาพยนต์ฮอลลีวู้ดส์) (Beck, 1992)

ในการก้าวเข้าสู่สังคมแห่งความเสี่ยงนั้น เบ็คส์ ยังได้เสนอแนวคิดเรื่อง ปฏิกิริยาหรือการตั้งคำถามต่ออารยธรรมทันสมัย (Reflexive Modernization) ว่า คนในยุคสมัยใหม่จะเน้นอยู่ที่การพยายามผลิตและแพร่กระจายความมั่งคั่งให้เข้าถึงทุกคน แต่ในยุค “สังคมแห่งความเสี่ยง” แล้วปัญหาที่ผู้คนเผชิญหน้าอยู่คือ การฝังความเสี่ยงเข้าไปในจิตสำนึกของคน ทำให้คนยุคนี้มีลักษณะมองโลกในแง่ร้าย และพยายามค้นหาวิธีการที่จะทำให้ตนเองอยู่รอดในภาวะความเสี่ยงทั้งหลาย ด้วยเหตุ

นี้ กระบวนการสร้างความทันสมัย (Modernisation) จึงถูกภาวการณ์ที่เกิดขึ้นจริงบีบให้ผู้คนต้องย้อนกลับมาทบทวนตนเองและเริ่มค้นหาคำตอบว่า เราจะเรียนรู้ให้นิยามและจัดการกับภาวะความเสี่ยงต่าง ๆ อย่างไร และเบ็คส์ตั้งข้อสังเกตไว้ว่า ความไม่แน่นอนของการเปลี่ยนแปลงในสภาวะแวดล้อมโลกหรือความผันผวนไม่แน่นอนในการดำเนินชีวิตแบบสมัยใหม่ คงไม่ใช่แค่การสะท้อน (Reflect) “ภาวะความเสี่ยง” แบบตรง ๆ หากแต่ยังเป็นกระบวนการที่เปิดให้มนุษย์ได้มีโอกาสเผชิญหน้ากับตนเอง (Self-confrontation) หรือทำให้กระบวนการของสังคมทันสมัยได้ถูกตรวจสอบและวิพากษ์วิจารณ์ตัวเอง

(3) ความเสี่ยงกับการสร้างอัตลักษณ์ แนวคิดนี้มาจาก แอนโธนี กิดเดนส์ (Anthony Giddens) นักสังคมวิทยาชาวอังกฤษ ซึ่งจุดยืนของกิดเดนส์เชื่อว่า วิทยาศาสตร์และวิทยาการสมัยใหม่ต่าง ๆ มีลักษณะเป็นเหรียญสองด้านคือ ในขณะที่เทคนิควิทยาการช่วยสร้างความมั่งคั่งทางเศรษฐกิจสังคมให้กับมนุษยชาติ แต่อีกด้านหนึ่งคือ วิทยาศาสตร์เป็นกลจักรสำคัญที่นำไปสู่ภาวะความเสี่ยงเช่นกัน ความสัมพันธ์ระหว่างภาวะความเสี่ยงกับอัตลักษณ์ (Identity) กิดเดนส์เชื่อว่าถึงจะอยู่ในยุคสังคมแห่งความเสี่ยงก็มิได้หมายความว่า ภาวะความเสี่ยงของมนุษย์จะเพิ่มมากขึ้นกว่าที่เคยมีมาในอดีต ตรงกันข้าม ภาวะความเสี่ยงนั้นส่งผลต่อการสร้างตัวตน หรืออัตลักษณ์ของปัจเจกบุคคล (Self-identity) มากกว่า เช่น กรณีความเสี่ยงที่เกี่ยวข้องกับสุขภาพของผู้คนในยุคนี้ที่ไม่อาจสืบค้นหาสาเหตุที่แท้จริงได้ อาทิ อาจมาจากสภาพแวดล้อมที่ผันแปน การบริโภคที่ผิดหลักโภชนาการ มลพิษด้านต่าง ๆ หรือความเครียดในชีวิตประจำวัน เพราะฉะนั้น ภาวะความเสี่ยงดังกล่าวจึงนำไปสู่การสร้างอัตลักษณ์และรูปแบบการดำเนินชีวิตของผู้คนยุคใหม่

(4) ความเสี่ยงกับการจัดวินัยทางอำนาจ มาจากแนวคิดของนักปรัชญาสังคมการเมืองแห่งศตวรรษที่ 20 อย่าง มิเชล ฟูโกต์ (Michel Foucault 1926 – 1984) นำเสนอแนวคิดที่เป็นทัศนะคติเกี่ยวกับอำนาจ (Power) ทั้งนี้ ฟูโกต์ปฏิเสธความเชื่อที่ว่าอำนาจมักมีลักษณะรวมศูนย์แต่ตรงกันข้าม อำนาจมีลักษณะเป็นอนุภาคเล็กๆ ที่กระจายตัวไปถ้วนทั่วทั้งสังคม หรือที่ฟูโกต์เรียกว่า จุลฟิสิกส์แห่งอำนาจ (Micro-physics of power) โดยสังคมได้พัฒนากลยุทธ์การปกครอง (Govern) แบบใหม่ที่เข้ามากำกับควบคุมดูแลจิตใจและจิตวิญญาณ (Mentality) จะนำไปสู่การสร้างความรู้ในการชีวิตด้านต่าง ๆ ของมนุษย์ ความเสี่ยงและการจัดวินัยทางอำนาจนั้น ฟูโกต์กล่าวไว้ว่าความเสี่ยงเป็นปฏิบัติการชนิดหนึ่งในอันที่จะปกครองจิตใจและจิตวิญญาณของปัจเจกเอาไว้ ความเสี่ยงเป็นชุดวาทกรรมที่ถูกผลิตขึ้นเพื่อควบคุมวินัยเหนือร่างกาย ความคิด และพฤติกรรมของเราไว้ว่าสำหรับคนยุคนี้ ต้องกังวลหรือกลัวกับความเสี่ยงเรื่องใดบ้าง เรื่องอะไรที่ถือเป็นความเสี่ยงและไม่เสี่ยง

และเราจะจัดการตนเองเพื่อไม่ให้ชีวิตตกอยู่ในสภาวะความเสี่ยงได้อย่างไร (กาญจนา แก้วเทพ และสมสุข หินวิมาน, 2560)

ลักษณะและมุมมองที่คนในยุคปัจจุบันมีต่อภัยอันตรายและความเสี่ยงนั้นแตกต่างจากในอดีต กล่าวคือ ในยุคโบราณก่อนที่ความรู้เหตุผลแบบวิทยาศาสตร์และระบบการผลิตแบบอุตสาหกรรมจะเกิดขึ้น ภัยอันตรายสำคัญของมนุษย์ล้วนแต่เป็นภัยธรรมชาติ ซึ่งผู้คนมองว่ามีสาเหตุจากอำนาจเหนือธรรมชาติไม่ว่าจะเป็นพระเจ้า เทพเจ้า ปีศาจ ซึ่งมนุษย์ไม่สามารถควบคุมจัดการอะไรได้ ต่อมาเมื่อวิทยาการความรู้ทางวิทยาศาสตร์เจริญรุ่งเรืองได้ทำให้การควบคุมจัดการภัยจากธรรมชาติมีประสิทธิภาพมากขึ้น อันตรายที่กลายเป็นความเสี่ยงหลักของมนุษย์กลายเป็นพฤติกรรมเสี่ยงต่อสุขภาพของมนุษย์เองแทน เช่น โรคระบาด การเกิดอุบัติเหตุ อาชญากรรม เป็นต้น ความเสี่ยงกลายเป็นสิ่งที่มนุษย์สร้างขึ้นเอง ดังนั้นวิธีการจัดการความเสี่ยงก็คือการควบคุมไม่ให้มนุษย์เกิดพฤติกรรมเสี่ยงต่าง ๆ นั่นเอง

ผู้วิจัยมีความสนใจความเสี่ยงอันตราย (Risk) น่าจะเป็นปัจจัยที่ก่อให้เกิดภัยคุกคามและอาชญากรรมในสังคมไทย และทำให้เกิดการผสมผสานอาชญากรรมรูปแบบเดิมและอาชญากรรมรูปแบบใหม่ที่มากับยุคแห่งการสื่อสารที่มีความเจริญก้าวหน้าอย่างยุคดิจิทัล ที่ถือว่าเป็นสังคมเสี่ยงอันตราย (Risk Society) ที่อาจแฝงมากับความล้ำสมัยของเทคโนโลยี ทำให้เกิดภัยคุกคามไซเบอร์รูปแบบใหม่ ๆ ขึ้น เช่น การหลอกหลวงออนไลน์ อาชญากรรมจากข่าวปลอมบนโลกออนไลน์ อาชญากรรมไซเบอร์ เป็นต้น ส่งผลกระทบในวงกว้าง ทำให้สูญเสียบุคลากรและงบประมาณจำนวนมากในการป้องกันและแก้ไข อีกทั้งการแพร่ระบาดของโรคอุบัติใหม่ในปัจจุบันที่ไม่เคยเกิดขึ้นมาก่อน ตัวอย่างเช่น การแพร่ระบาดของโรคโควิด-19 ถือเป็นหนึ่งในเหตุการณ์ที่ส่งผลกระทบหนักที่สุดต่อเศรษฐกิจในศตวรรษที่ 21 ส่งผลกระทบอย่างหนักต่อทุกด้านในชีวิตของผู้คน สังคม และเศรษฐกิจของประเทศต่างๆ ทำให้การท่องเที่ยวทั่วโลกและห่วงโซ่อุปทานตกเข้าสู่ภาวะชะงักงัน ถือเป็นสังคมแห่งความเสี่ยงภัยที่ต้องเตรียมพร้อมรับมือและหาแนวทางแก้ไขในทุก ๆ ด้าน

2.2 ภัยคุกคามทางไซเบอร์

จาก พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 3 บัญญัติความหมายภัยคุกคามไซเบอร์ ไว้ว่า

“การกระทำหรือการดำเนินการใดๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์

ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นๆที่เกี่ยวข้อง และเป็นภัยอันตรายที่ใกล้จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง"

หรือกล่าวได้ว่า การกระทำหรือการดำเนินการใด ๆ ผ่านการใช้ระบบสารสนเทศหรือเครือข่ายที่ก่อให้เกิดผลเสียต่อระบบข้อมูลเครือข่าย เพราะคำว่า "ไซเบอร์" หมายความรวมถึง การสื่อสารข้อมูลที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเตอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันและเชื่อมต่อกัน ซึ่งภัยคุกคามทางไซเบอร์ถือเป็นภัยคุกคามใหญ่หลวงต่อผลประโยชน์ทางเศรษฐกิจ ตลอดจนความมั่นคงของประเทศ การโจมตีทางไซเบอร์มีหลายรูปแบบ เช่น การเจาะระบบคอมพิวเตอร์ (Hacking) การสอดแนมข้อมูลคอมพิวเตอร์ โดยสปายแวร์การดักรับข้อมูลคอมพิวเตอร์ (Sniffing) การโจมตีโดยชุดคำสั่งไม่พึงประสงค์ (Malicious Software : Malware) หรือการรุมสอบถามข้อมูลจนระบบล่ม (Denial of Service Attack : DOS) เป็นต้น การโจมตีแต่ละครั้งล้วนสร้างความเสียหายอย่างมหาศาล ทั้งต่อความมั่นคง ความปลอดภัยของระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ ตลอดจนระบบเศรษฐกิจและความมั่นคงของประเทศ

ข้อมูลจาก Cybersecurity Venture ระบุว่ามูลค่าความเสียหายที่เกิดจากการโจมตีทางไซเบอร์ภายในปี พ.ศ.2564 จะมีมูลค่าสูงถึง 6 ล้านล้านดอลลาร์สหรัฐ และยังคาดการณ์ว่าในช่วง 5 ปีข้างหน้าจะมีมูลค่าความเสียหายจากอาชญากรรมทางไซเบอร์ทั่วโลกขยายตัวเพิ่มขึ้นร้อยละ 15 ต่อปี ซึ่งหมายความว่าในปี พ.ศ. 2568 คาดว่าจะมีมูลค่าความเสียหายสูงถึง 10.5 ล้านล้านดอลลาร์สหรัฐ ซึ่งสูงกว่าความเสียหายจากภัยพิบัติทางธรรมชาติ โดยข้อมูลอาชญากรรมไซเบอร์ที่มีการกระทำกับองค์กรขนาดใหญ่ในปี พ.ศ.2564 เช่น กรณีบริษัท Brenntag ซึ่งเป็นผู้จัดจำหน่ายสารเคมีของสหพันธ์สาธารณรัฐเยอรมนี ถูกโจมตีด้วยมัลแวร์เรียกค่าไถ่โดยกลุ่ม Darkside ในช่วงเวลาเดียวกันกับการโจมตีบริษัท Colonial Pipeline ของสหรัฐอเมริกา ซึ่งกลุ่มอาชญากรไซเบอร์มีการเรียกค่าไถ่สูงถึง 7.5 ล้านดอลลาร์สหรัฐ หลังจากนั้นมีการเจรจาต่อรองลดลงเหลือ 4.4 ล้านดอลลาร์สหรัฐ เพื่อแลกกับข้อมูลที่ถูกขโมยไป 150 กิกะไบต์ (สำนักข่าวอินโฟเควสท์, 2564)

นอกจากนี้ Belani (2020) ได้รายงานผลการศึกษาของ Threat Horizon ถึงภัยคุกคามทางไซเบอร์ที่องค์กรต่างๆ กำลังจะต้องเผชิญ ซึ่งประกอบด้วย 3 ประเด็นหลัก ได้แก่ 1) การ

หยุดชะงัก (Disruption) ทำให้อินเทอร์เน็ตหยุดทำงานซึ่งส่งผลกระทบต่อการดำเนินธุรกิจ 2) การบิดเบือน (Distortion) เป็นการแพร่กระจายของข้อมูลที่ผิดโดยบอต (Bots) และการบิดเบือนแหล่งข้อมูลทำให้ความน่าเชื่อถือของข้อมูลลดลงโดยอัตโนมัติ 3) การเสื่อมสภาพ (Deterioration) ความก้าวหน้าอย่างรวดเร็วของเทคโนโลยีขัดแย้งกับความต้องการในการพัฒนาความมั่นคงของชาติ ส่งผลเสียต่อความสามารถขององค์กรในการควบคุมข้อมูลและความปลอดภัยของระบบ

2.2.1 รูปแบบและประเภทของภัยคุกคามทางไซเบอร์

โดยทั่วไปภัยคุกคามทางไซเบอร์สามารถแบ่งออกเป็นกลุ่มต่าง ๆ ได้ดังนี้

(1) ภัยคุกคามที่เกิดจากการใช้โปรแกรมประยุกต์ที่ถูกดาวน์โหลดมาเพื่อติดตั้งบนคอมพิวเตอร์หรืออุปกรณ์โทรศัพท์เคลื่อนที่ และแฝงมาด้วยโปรแกรมที่เป็นภัยคุกคามที่เรียกว่ามัลแวร์ (Malware) ซึ่งถูกออกแบบมาเพื่อทำอันตรายต่อข้อมูลในคอมพิวเตอร์หรืออุปกรณ์โทรศัพท์เคลื่อนที่ที่ทำ ให้เกิดการขัดข้อง เสียหายกับระบบปฏิบัติการ (CISA, 2019) นอกจากนี้สามารถส่งข้อความไม่พึงประสงค์ออกไปยังที่อื่น ขโมยข้อมูลสำคัญออกไป ตัวอย่างของโปรแกรมเหล่านี้ ได้แก่

Virus มักจะแฝงตัวอยู่ในโปรแกรมคอมพิวเตอร์หรือไฟล์ และสามารถแพร่กระจายไปยังเครื่องอื่นๆ ได้โดยแนบตัวเองไปกับโปรแกรมหรือไฟล์ดังกล่าว แต่ไวรัสจะทำงานก็ต่อเมื่อมีการรันโปรแกรมหรือเปิดไฟล์เท่านั้น

Trojan เป็นโปรแกรมที่ระบุวัตถุประสงค์ให้ผู้ใช้งานเข้าใจว่าเป็นโปรแกรมสำหรับใช้งานตามที่กล่าวอ้างและปลอดภัย แต่แท้จริงแล้วได้แอบแฝงคำสั่งอันตราย เช่น คำสั่งลบไฟล์ข้อมูล เขียนทับข้อมูลใน Hard-drive หรือสร้างการเข้าถึงระยะไกล (Remote Access) บนเครื่องแม่ข่ายกลับไปยัง Hacker เป็นต้น

Worm สามารถแพร่กระจายัวเองไปยังคอมพิวเตอร์และอุปกรณ์เครื่องอื่นๆ ผ่านทางระบบเครือข่าย เช่น email หรือระบบแชร์ไฟล์ โดยไม่ต้องอาศัยการเรียกใช้งานโปรแกรมจากผู้ใช้งาน

Spyware เป็นโปรแกรมที่ใช้ในการติดตาม แอบดูพฤติกรรมและบันทึกการใช้งานของผู้ใช้ และอาจขโมยข้อมูลส่วนตัว เช่น บัญชีชื่อผู้ใช้งาน รหัสผ่าน หรือข้อมูลทางการเงิน เป็นต้น พร้อมทั้งส่งข้อมูลดังกล่าวไปในเครื่องปลายทางที่ระบุเอาไว้อีกด้วย และมักจะถูกติดตั้งโดยที่ผู้ใช้งานไม่ทันได้สังเกต หรือไม่มีการขอความยินยอมจากผู้ใช้งาน

Rootkit เป็นมัลแวร์ที่เปิดช่องทางให้ผู้อื่นเข้ามาติดตั้งโปรแกรมเพิ่มเติม เพื่อควบคุมเครื่อง พร้อมได้สิทธิของผู้ดูแลระบบ (Root)

Bot คือ ซอฟต์แวร์ที่สร้างขึ้นมาเพื่อทำงานใดงานหนึ่งแบบอัตโนมัติ โดยรับคำสั่งและควบคุมจากเครื่องของ Hacker (command and control center) เช่น Botnets หรือเครื่องที่ถูก Hacker ควบคุม ใช้เพื่อมาโจมตีแบบ DDoS หรือ Spambot เพื่อใช้สำหรับการส่ง Spam เป็นต้น โดยเครื่องที่ตกเป็นเหยื่อมักจะถูกเรียกว่า Drones หรือ Zombies

Ransomware คือ มัลแวร์ที่มุ่งหวังจะทำการเข้ารหัสไฟล์ข้อมูลของเหยื่อเพื่อเรียกค่าไถ่ ซึ่งจะส่งผลให้เหยื่อหรือเจ้าของข้อมูลไม่สามารถเข้าถึงไฟล์ข้อมูลของตนเองได้ โดยเหยื่อจะต้องจ่ายเงินให้กับ Hacker เพื่อทำการถอดรหัสไฟล์ข้อมูลดังกล่าว โดยไม่สามารถรับรองได้ว่า Hacker จะทำการถอดรหัสไฟล์ให้เหยื่อหรือไม่ หลังได้รับค่าไถ่แล้ว ทั้งนี้ Hacker มักจะให้ผู้เสียหายจ่ายค่าไถ่ผ่านสกุลเงินดิจิทัล เช่น Bitcoin เนื่องจากเป็นช่องทางที่ยากต่อการตรวจสอบ

Hoaxes เป็นรูปแบบหนึ่งของการก่อกวน โดยไวรัสหลอกลวงพวกนี้จะมาในรูปแบบของ email การส่งข้อความต่อๆ กันไปผ่านทางโปรแกรมรับส่งข้อความ หรือห้องสนทนาซึ่งสามารถสร้างความวุ่นวาย โดยการใช้จิตวิทยาของผู้สร้างข่าวขึ้นมาทำให้ผู้ได้รับข้อความเกิดความกลัว ความลังเล สงสัย และเมื่อผู้รับ ส่งต่อไปยังผู้อื่น ก็ยิ่งสร้างความเชื่อมั่นมากขึ้น จากนั้นผู้รับก็จะทำตัวเป็นผู้ส่งต่อไปอีกหลายๆ ทอด ซึ่งเป็นลักษณะเด่นของไวรัสนี้

Phishing เทคนิคการหลวงลวงโดยใช้ email หรือหน้าเว็บไซต์ปลอม เพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลต่าง ๆ เช่น ชื่อผู้ใช้ รหัสผ่าน วันเดือนปีเกิด เป็นต้น และใช้ข้อมูลดังกล่าวในการเข้าระบบโดยไม่ได้รับอนุญาต รวมถึงหลอกล่อให้เหยื่อกดลิงค์ เพื่อแอบติดตั้งมัลแวร์ลงคอมพิวเตอร์ โดยประเภทของ Phishing ที่พบเห็นโดยส่วนใหญ่มี 2 ประเภท ได้แก่ Email Phishing และ Web Phishing เป็นต้น

(2) ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์หลอกที่ถูกออกแบบมาให้เหมือนของจริง หลอกให้ผู้ใช้งานล็อกอินเข้าอีเมล์เฟซบุ๊ก หรือเว็บไซต์ทางการเงิน แล้วดักจับรหัสของผู้ใช้งาน ทำให้ข้อมูลหรือบัญชีนั้น ๆ มีความเสี่ยงไม่ปลอดภัย

(3) ภัยคุกคามจากการใช้เครือข่ายไร้สาย ปัจจุบันมีผู้ให้บริการเครือข่ายไร้สายเป็นจำนวนมาก มีทั้งที่น่าเชื่อถือและไม่น่าเชื่อถือ รวมถึงผู้ที่แอบแฝงเพื่อวัตถุประสงค์อื่น ดังนั้น ผู้ใช้คอมพิวเตอร์หรืออุปกรณ์เคลื่อนที่เชื่อมต่อระบบเครือข่ายไร้สายต่าง ๆ อาจได้รับผลกระทบโดยตรง รวมถึงยังสามารถเป็นต้นตอของผลกระทบไปยังอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์เคลื่อนที่ของผู้อื่นด้วยเช่นกันโดยผู้ใช้เครือข่ายไร้สายอาจถูกโจมตีด้วยมัลแวร์ผ่านข้อบกพร่องของระบบปฏิบัติการ และถูกเปลี่ยนสถานะมาเป็นผู้โจมตีโดยการส่งต่อหรือแพร่กระจายมัลแวร์เหล่านี้ไปยังอุปกรณ์อื่นผ่านเครือข่ายไร้สายหรือบลูทูธ นอกจากนี้การใช้เครือข่ายไร้สายยังเปิดโอกาสให้ผู้ไม่ประสงค์ดีดักจับข้อมูลสำคัญหรือรหัสผ่านบนเครือข่ายไร้สายได้อีกด้วย

(4) ภัยคุกคามที่เกิดจากการโจมตีแบบเจาะจงเป้าหมาย (Targeted Attack) ที่มาจากหลายประเทศมีมากขึ้น ผู้โจมตีหรือแฮกเกอร์ในประเทศต่าง ๆ จะใช้การโจมตีแบบเจาะจงเป้าหมายอย่างต่อเนื่อง สร้างความเสียหายให้แก่โครงสร้างพื้นฐาน วิกฤตสถาบันการเงิน และองค์กรอื่น ๆ ของภาครัฐและภาคเอกชนในหลายประเทศอาชญากรไซเบอร์เหล่านี้จะใช้มาตรการที่รวดเร็วและรุนแรงในการโจรกรรมข้อมูล ภัยคุกคามประเภทนี้จัดว่าเป็นภัยคุกคามที่กระทบต่อความมั่นคงของประเทศเป็นอย่างยิ่ง

(5) ภัยคุกคามในรูปแบบใหม่ (Non-Traditional threats) มีการอธิบายกันอย่างกว้างขวางในกลุ่มนักวิชาการ ภายใต้บริบทและมุมมองที่แตกต่างกัน แต่ที่โดดเด่นที่สุด คือ กลุ่มของคริสต์ แอบบอต, พอล โรเจอร์ส และจอห์น สโลโบดา (ChristAbbott, Paul Rogers and John Sloboda) ซึ่งได้แบ่งประเภทของภัยคุกคามรูปแบบใหม่ออกเป็น 4 ประเภท คือ 1) ภัยจากการเปลี่ยนแปลงภูมิอากาศ (Climate Change) 2) ภัยจากการแข่งขันแย่งชิงทรัพยากร (Competition over Resources) 3) ภัยจากการเกิดขึ้นใหม่ของชนกลุ่มน้อยในสังคมใหญ่ (Marginalization of the Majority World) และ 4) ภัยจากการแพร่ขยายอิทธิพลทางทหาร (Global MilitariZation) นอกจากนี้ ยังมีการให้คำนิยามและแบ่งประเภทของภัยคุกคามรูปแบบใหม่ ในลักษณะแยกย่อยลงไป

เช่น ภัยคุกคามจากโรคระบาด (Epidemiology) ภัยคุกคามทางสารสนเทศ (Information) ภัยจากอาชญากรรมข้ามชาติ (Transnational crime) ภัยคุกคามต่อความมั่นคงของมนุษย์(Human Security) และภัยคุกคามทางด้านภูมิรัฐศาสตร์ (Geopolitics) ประเทศไทยต้องเผชิญกับภัยคุกคามรูปแบบใหม่ที่ส่งผลกระทบต่อความมั่นคงของประเทศโดยตรง ทั้งทางด้านเศรษฐกิจ สังคมจิตวิทยา และการทหาร ในลักษณะที่ภัยคุกคามได้ทวีความรุนแรงเพิ่มขึ้นตามลำดับ จากปัจจัยบวกของกระแสโลกาภิวัตน์ที่มีการเปิดเสรีการค้าการเงิน การลงทุน ความก้าวหน้าทางการสื่อสารและเทคโนโลยีสารสนเทศ ตลอดจนผู้คนมีการย้ายถิ่นฐานระหว่างประเทศมากยิ่งขึ้น ทั้งนี้ประเทศไทยยังไม่มีหน่วยงานหรือองค์กรใดๆ ที่ได้ให้คำนิยามและแบ่งประเภทของภัยคุกคามรูปแบบใหม่ที่ชัดเจน

ลักษณะของภัยคุกคามไซเบอร์

ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 60 มีการกำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็น 3 ระดับ ดังนี้

ไม่ร้ายแรง

- ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศหรือการให้บริการของรัฐ**ด้อยประสิทธิภาพ**

ร้ายแรง

- ภัยคุกคามทางไซเบอร์ที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ ถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชน**เสียหาย จนไม่สามารถทำงานหรือให้บริการได้**

วิกฤต

- (ก) ภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยส่งผลกระทบรุนแรงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานที่สำคัญอื่นๆ **อาจทำให้บุคคลจำนวนมากเสียชีวิต หรือระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ**
- (ข) ภัยคุกคามทางไซเบอร์ที่กระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับ **การก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือสงคราม ซึ่งจำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย**

ภัยคุกคามที่เกิดขึ้นกับข้อมูลหรือสารสนเทศ หรือการใช้ทรัพยากรของระบบ เช่น การแอบลักลอบใช้ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตการขัดขวางไม่ให้คอมพิวเตอร์ทำงานได้ตามปกติ การปรับเปลี่ยนข้อมูลหรือสารสนเทศโดยไม่ได้รับอนุญาต อาทิเช่น การแอบเข้าใช้งานระบบคอมพิวเตอร์ของหน่วยงานหรือองค์กรอื่น โดยมิได้รับอนุญาต แต่ไม่มีประสงค์ร้าย หรือไม่มีเจตนาที่จะสร้างความเสียหายหรือสร้างความเดือดร้อนให้แก่ใครทั้งสิ้น แต่เหตุผลที่ทำเช่นนั้นอาจ

เป็นเพราะต้องการทดสอบความรู้ความสามารถของตนเองก็เป็นไปได้ ซึ่งเรียกกลุ่มคนรูปแบบนี้ว่า แฮคเกอร์ (hacker) นอกจากนี้ยังมีการแอบเข้าใช้งานระบบคอมพิวเตอร์ของหน่วยงานหรือองค์กรอื่น โดยมีเจตนาร้ายอาจจะเข้าไปทำลายระบบ หรือสร้างความเสียหายให้กับระบบเครือข่าย (Network) ขององค์กรอื่น หรือขโมยข้อมูลที่เป็นความลับทางธุรกิจ ซึ่งเรียกบุคคลกลุ่มนี้ว่า แคร็กเกอร์ (Cracker) ความแตกต่างระหว่าง Hacker กับ Cracker คือ Hacker มีเป้าหมายเพื่อทดสอบความสามารถหรือต้องการท้าท้าย โดยการเจาะระบบให้สำเร็จ ส่วน Cracker มีจุดประสงค์คือต้องการทำลายระบบความมั่นคง ปลอดภัยของระบบคอมพิวเตอร์หรือระบบสารสนเทศ

สถานการณ์ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง

ผู้ใช้งานคอมพิวเตอร์จำนวนไม่น้อยถูกหลอกลวงโดย Banner หรือ Popup ที่โผล่ขึ้นมาเมื่อเปิดเว็บไซต์ แล้วหลงเชื่อและติดตั้งโปรแกรมแอนตี้ไวรัสปลอม (Rogue Antivirus) ซึ่งจะมีลักษณะเหมือนกับโปรแกรมแอนตี้ไวรัสธรรมดาทั่วไป แต่มีจุดประสงค์เพื่อหลอกลวงและไม่สามารถกำจัดไวรัสได้จริง เมื่อผู้ใช้เผลอติดตั้งและเรียกใช้งานโปรแกรมแอนตี้ไวรัสปลอม โปรแกรมนั้นจะปรากฏหน้าจอที่ดูเหมือนกับกำลังทำการสแกนไฟล์ในระบบ แล้วจะแจ้งผลการสแกนขึ้นมาแจ้งว่ามีโปรแกรมอันตรายอยู่ในระบบอยู่เป็นจำนวนมาก แต่ผู้ใช้จะยังไม่สามารถกำจัดโปรแกรมอันตรายเหล่านั้นออกได้ จนกว่าจะจ่ายเงินให้กับผู้พัฒนาโปรแกรมแอนตี้ไวรัสปลอมนี้ก่อน แอนตี้ไวรัสปลอมหลายตัว นอกจากจะไม่สามารถกำจัดไวรัสได้แล้ว ยังดาวน์โหลดโปรแกรมอันตรายอื่นๆ มาติดตั้งเพิ่มเติมในเครื่องของผู้ใช้ด้วย โปรแกรมที่ทำงานในลักษณะแบบนี้มีชื่อเรียกว่า Rogueware หรือ Scareware ซึ่งมีความหมายโดยรวมหมายถึงโปรแกรมที่หลอกลวงผู้ใช้ให้ทำการจ่ายเงิน โดยทั่วไป Rogueware มักจะมาในรูปแบบของโปรแกรมรักษาความมั่นคงปลอดภัย เนื่องจากง่ายต่อการล่อลวงให้ผู้ใช้ดาวน์โหลดโปรแกรมไปทำการติดตั้ง เช่น อาจจะทำ Banner หรือ Popup ที่ปรากฏขึ้นเมื่อผู้ใช้เข้าสู่เว็บไซต์ (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2565) โดยเนื้อหาของข้อความข้างในนั้นจะเป็นการแจ้งเตือนว่าตรวจพบโปรแกรมอันตราย อยู่ในเครื่องคอมพิวเตอร์ของผู้ใช้ ต้องรีบดาวน์โหลดโปรแกรมแอนตี้ไวรัสไปทำการตรวจสอบโดยด่วน กรณีนี้อาจส่งผลให้เครื่องคอมพิวเตอร์ทำงานช้าลงหรือผิดเพี้ยนไป

สถานการณ์ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง

มัลแวร์รูปแบบหนึ่งที่ถูกระบุใช้เป็นเครื่องมือโจมตีโรงพยาบาลสระบุรีเมื่อเดือนกันยายนปี พ.ศ.2563 คือ มัลแวร์สเปด (Spade) เป็นหนึ่งในรูปแบบการติดเชื้อของคอมพิวเตอร์ที่จะสร้างกลไกลล็อคการเข้าถึงข้อมูล มัลแวร์เรียกค่าไถ่นี้ถูกจัดให้อยู่กับกลุ่มของมัลแวร์ทั่วไปที่ชื่อวอยด์คริปท์ (VoidCrypt) (Cyber Security Plan, 2020) โดยที่การโจมตีด้วยสเปดมีการตรวจพบครั้งแรกราวเดือนเมษายน พ.ศ.2563 จุดผิดสังเกตที่ทำให้ได้ชัดเจนอย่างหนึ่งคือไฟล์แปลกปลอมที่ลงท้ายด้วย .Void หรือ .Spade โดยจะมาพร้อมกับอีเมลหลอกลวง เนื้อหาอีเมล์อาจไม่ปรากฏชัดแจ้งให้เห็นสิ่งแปลกปลอม เนื่องจากมีการเข้ารหัสอีเมล์ป้องกันเอาไว้ชั้นหนึ่ง รูปแบบการเข้ารหัสใช้สถาปัตยกรรมการเข้ารหัสเป็นบล็อกแบบสมมาตรหรือแบบเออีเอส (Advance Encryption Standard :AES) ผสมผสานกับอัลกอริทึมการเข้ารหัสแบบอาร์เอสเอ (Rivest-Shamir-Adleman cryptosystem: RSA) นอกจากเข้ารหัสไฟล์ไว้แล้วตัวมัลแวร์ยังคงทิ้งข้อความให้ผู้ใช้รู้ถึงวิธีการถอดรหัส (Read-For-Decrypt) ด้วยไฟล์ข้อความชนิด .HTA (HTML Application) (Wall, 2020) คำขู่จะให้ชำระเงินเป็นบิตคอยน์หรือสกุลเงินดิจิทัลอื่นซึ่งจะได้รับเครื่องมือสำหรับถอดรหัสกลับมา บัญชีอีเมลที่มักจะพบมาพร้อมกับมัลแวร์ ได้แก่ rsaencrypt@tutanota.com,rsaencrypt@protonmail.ch,VoidDeceryptor@tutanota.com,Void Deceryptor@protonmail.com (อัศว์ณุต แสงทองดี และญาณพล ยั่งยืน, 2563) ทำให้ระบบการจัดการและรักษาพยาบาล รวมถึงข้อมูลระบบสนับสนุนบริการทั้งหมดได้รับความเสียหาย และโรงพยาบาลไม่สามารถเข้าถึงข้อมูลได้ และข้อมูลการรักษาพยาบาลเดิมไม่สามารถใช้งานได้ในระยะหนึ่ง

สถานการณ์ภัยคุกคามทางไซเบอร์ในระดับวิกฤต

ในประเทศไทยนั้นยังไม่เคยมีสถานการณ์ภัยคุกคามทางไซเบอร์ในระดับวิกฤตหรือการก่อการร้ายทางไซเบอร์ แต่เหตุการณ์ภัยคุกคามทางไซเบอร์ในต่างประเทศ อย่างกรณีสงครามไซเบอร์ที่เกิดขึ้นโดยการใช้ Botnet ในการโจมตีหน่วยงานโครงสร้างพื้นฐานสำคัญทั้งหมดของประเทศเอสโตเนีย วิเคราะห์ได้ว่า เข้าข่ายภัยคุกคามทางไซเบอร์ขั้นวิกฤต ซึ่งประเทศนี้เป็นประเทศที่ระบบส่วนใหญ่พึ่งพิงกับอินเทอร์เน็ตและเทคโนโลยี การโจมตีทำให้ทั้งประเทศเอสโตเนียไม่สามารถใช้งานด้านสาธารณูโภคทางการติดต่อสื่อสาร ไฟฟ้า ประปา หรือการเดินทางต่างๆ ได้เลย ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ หรือ CERT ของประเทศเอสโตเนีย

ไม่สามารถที่จะควบคุมสถานการณ์ได้ในวันแรก ต่อมา CERT ได้ขอความช่วยเหลือจาก CEO ของ Netnod เป็นบริษัทจำกัดเอกชนที่ตั้งอยู่ในสตอกโฮล์ม ประเทศสวีเดน ให้การช่วยเหลือ ลดความรุนแรงของการโจมตี ภายในสองอาทิตย์การจู่โจมก็ได้สงบลงและสามารถสืบทราบได้ว่าเป็นเพราะรัฐบาลรัสเซียที่พยายามจู่โจม แต่ก็ไม่สามารถหาความจริงหรือวัตุประสงค์ที่แท้จริงได้ การเกิดเหตุการณ์ครั้งนี้ทำให้ องค์กร NATO เคลื่อนไหวในการสร้างความมั่นคงปลอดภัยทางไซแบอร์ให้มีความเข้มแข็งมากกว่าเดิม (Karatzogianni, 2009)

รูปแบบและประเภทภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อองค์กร

ภัยคุกคามทางไซเบอร์เป็นสิ่งที่เกิดขึ้นเพื่อสร้างความเสียหายให้กับระบบคอมพิวเตอร์ โดยมีวัตถุประสงค์ในการโจมตีใน 3 ลักษณะ ได้แก่ การนำความลับไปเปิดเผย (Data confidentiality) การเปลี่ยนแปลงข้อมูล (Data integrity) และการทำให้ระบบหยุดบริการ หรือไม่สามารถใช้งานได้ (System Availability) ซึ่งการจะเข้าดำเนินการกับระบบคอมพิวเตอร์นั้นมีกลยุทธ์การโจมตี (Tactics) องค์กรตามกรอบการโจมตีของ MITRE (MITRE Attack Framework) (Mitre, n.d.) ได้แก่

(1) การลาดตระเวน (Reconnaissance) เป็นการรวบรวมข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศขององค์กร เช่น ข้อมูลองค์กร โครงสร้างพื้นฐาน เจ้าหน้าที่/บุคลากร เป็นต้น เพื่อกำหนดขอบเขตและจัดลำดับความสำคัญของวัตถุประสงค์ในการโจมตี

(2) การพัฒนาทรัพยากร (Resource development) เป็นการสร้างทรัพยากรสำหรับการโจมตีทางไซเบอร์ เช่น การขโมยทรัพยากรหรือโค้ดต่างๆ สำหรับการปฏิบัติการ หรือการขโมยอีเมลสำหรับการทำฟิชชิง (Phishing) ซึ่งเป็นเทคนิคการหลอกลวงโดยใช้จิตวิทยาผ่านระบบคอมพิวเตอร์ มักเป็นในรูปแบบอีเมลหรือเว็บไซต์เพื่อหลอกลวงให้เหยื่อเผยข้อมูลความลับต่างๆ เช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต รวมถึงการหลอกลวงให้กดลิงก์เพื่อแอบติดตั้งมัลแวร์ลงในคอมพิวเตอร์ของเหยื่อ

(3) การเข้าถึงเป้าหมาย (Initial access) เป็นการเข้าถึงเครือข่ายสารสนเทศขององค์กร ได้แก่ การเจาะระบบผ่านช่องโหว่ของแอปพลิเคชัน เช่น ช่องโหว่การอัพโหลดไฟล์ขึ้นบนเว็บไซต์ ช่องโหว่ของโปรแกรมบริหารจัดการบนเว็บไซต์ หรือช่องโหว่ของโปรแกรมเครือข่ายส่วนตัวเสมือน มีการเดารหัสผ่านของบัญชีผู้ใช้หากระบบไม่ได้ถูกตั้งค่าการป้องกัน (Brute Force Attack)

รวมถึง Spearphishing เป็นการโจมตีที่พุ่งเป้าไปยังเป้าหมายรายบุคคล โดยอาชญากรไซเบอร์จะค้นหาข้อมูลเบื้องต้นของพนักงานในองค์กรที่เป็นเป้าหมายจาก ช่องทางต่างๆ เช่น เครือข่ายสังคมออนไลน์ (Social network) จากนั้นอาชญากรไซเบอร์จะสร้างอีเมลฟิชชิง ที่ระบุเนื้อหาสอดคล้องกับเป้าหมายเพื่อให้ เป้าหมายเชื่อใจกดลิงก์ที่แนบมากับอีเมลที่เป็นเป้าหมาย

(4) การดำเนินการ (Execution) เป็นขั้นตอนการเรียกโปรแกรมหรือคำสั่งอันตราย (Malicious code) ในระบบภายใน หรือการเรียกใช้ผ่านการเข้าถึงระยะไกล (Remote access) ขึ้นมา ประมวลผล เช่น เรียกใช้งานโปรแกรมผ่าน Command line หรือ PowerShell คือ แอปพลิเคชันสำหรับรับคำสั่งและภาษาสคริปต์ที่สร้างขึ้นบน .NET ซึ่ง PowerShell ช่วยให้ผู้ดูแลระบบและผู้ใช้งานสามารถสั่งให้กระบวนการ ต่างๆ ทำงานโดยอัตโนมัติบนระบบปฏิบัติการ (Linux, macOS และ Windows) ทำการเข้าถึงระบบจากระยะไกล

(5) ความพยายามที่จะรักษาจุดที่ยึดครองไว้ได้ (Persistence) เป็นการทำให้มัลแวร์ยังคงทำงานอยู่ ในระบบถึงแม้อุปกรณ์จะถูกปิดหรือเปลี่ยนแปลงการตั้งค่า เช่น การกำหนดค่าการเข้าถึง (Configuration) ต่างๆ ใหม่

(6) ความพยายามในการยกระดับสิทธิการเข้าถึง (Privilege escalation) ของระบบด้วยการใช้ประโยชน์ จากจุดอ่อนของระบบ เพื่อเข้าถึงข้อมูลที่จำเป็นต้องมีสิทธิเข้าถึงระดับสูง เช่น ข้อมูล ผู้บริหาร หรือข้อมูลผู้ดูแลระบบ เป็นต้น

(7) การพยายามหลบหลีกการตรวจจับ (Defense Evasion) เป็นเทคนิคที่ใช้หลบเลี่ยงการตรวจจับ หรือการสังเกตความผิดปกติของระบบ เช่น การปิดซอฟต์แวร์ความปลอดภัย การซ่อนหรือ ปลอมแปลงมัลแวร์ไม่ให้ปรากฏเมื่อเรียกดูข้อมูลด้วยวิธีปกติ การลบไฟล์ log ของระบบ เป็นต้น

(8) การเข้าถึงข้อมูลประจำตัว (Credential access) เป็นการพยายามขโมยบัญชีและรหัสผ่าน สำหรับเข้าสู่ระบบ

(9) การค้นพบ (Discovery) เป็นการค้นพบสภาพแวดล้อมทางเครือข่ายและระบบเครือข่ายภายใน โดยมีจุดประสงค์เพื่อปรับแนวทางการโจมตี หรือตรวจหาข้อมูลสำคัญว่าอยู่ที่ใด และจะใช้ เพื่อประโยชน์การใด

(10) การทำ Lateral movement เป็นการรวบรวมข้อมูลเครือข่ายเพื่อทำการเจาะไปยังอุปกรณ์ เครื่องอื่น ๆ ต่อไป เช่น เชื่อมต่อไปยังคอมพิวเตอร์เครื่องอื่นผ่านช่องทาง Secure

shell (SSH) หรือ Remote Desktop (RDP) ด้วยการโจมตีผ่าน SMB โดยอาศัยฟีเจอร์ (Feature) Windows Admin Share เพื่อขโมยข้อมูลสั่งดำเนินการ (Run) โปรแกรมปลายทาง หรือ อาจเพิ่มมัลแวร์ลงในโฟลเดอร์ที่มีการแชร์ผ่านเครือข่าย โดยตั้งชื่อไฟล์ให้ดูเหมือนว่า เป็นไฟล์ทั่วไป เพื่อผู้ใช้คนอื่นในระบบหลงเชื่อและเปิดไฟล์ดังกล่าว

(11) การรวบรวม (Collection) เป็นการรวบรวมข้อมูลจากแหล่งเก็บข้อมูลต่างๆ ขององค์กร เพื่อส่งออกไปยังภายนอก

(12) การใช้เทคนิค Command and control จากภายนอกเพื่อส่งข้อมูลออกจากระบบไปยัง ภายนอกโดยหลีกเลี่ยงการตรวจจับ

(13) การกรองข้อมูล (Exfiltration) คือ การขโมยข้อมูลออกไปด้วยวิธีการทำเป็นแพ็กเกจ (Package) บีบอัด และเข้ารหัส รวมถึงจำกัดขนาดในการส่งข้อมูล เพื่อหลีกเลี่ยงการถูกตรวจจับขณะ นำข้อมูลออกจากระบบ

(14) การสร้างผลกระทบ (Impact) เป็นความพยายามในการจัดการ ควบคุม ขัดขวาง หรือทำลาย ระบบขององค์กร ซึ่งรวมความพยายามในการทำลายและเปลี่ยนแปลงแก้ไขข้อมูลขององค์กร

อนึ่ง Belani (2020) เสนอรูปแบบของภัยคุกคามในอนาคตอันใกล้ที่องค์กรต้องเผชิญ โดยมีรูปแบบภัยคุกคามใหม่ๆ ได้แก่

(1) AI-Enhanced Cyber threats เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) ถูกอาชญากรไซเบอร์ใช้ประโยชน์ในการเปิดการโจมตีทางไซเบอร์ที่ซับซ้อน โดยการใช้มัลแวร์ ที่ถูกควบคุมโดยปัญญาประดิษฐ์ทำให้สามารถสร้างสแปม (Spam) ที่มีความน่าเชื่อถือ ซึ่งสามารถหลีกเลี่ยงการตรวจจับความปลอดภัยและปรับให้เข้ากับแต่ละเป้าหมายได้ดีขึ้น ทั้งยังมีการใช้ปัญญาประดิษฐ์ ในการสแกนสื่อสังคมออนไลน์เพื่อค้นหาบุคคลที่เหมาะสม ในการกำหนดเป็นเป้าหมายสำหรับการทำฟิชชิง แล้วสามารถสร้างสแปมที่ปรับแต่งให้เหมาะกับเหยื่อ

(2) AI Fuzzing เป็นเทคนิคการค้นหาช่องโหว่ในแอปพลิเคชัน หรือในระบบที่ได้รับความนิยม มากที่สุด ด้วยการใช้ประโยชน์จากเทคโนโลยีการเรียนรู้ของเครื่อง (Machine learning) ทำให้อาชญากรไซเบอร์ยังสามารถใช้เทคนิคนี้เพื่อเริ่มการโจมตีได้อย่างอัตโนมัติ และ ย่นระยะเวลาของการโจมตีแบบ Zero-day

(3) Cloud vulnerability หรือ ช่องโหว่บนคลาวด์ เนื่องจากองค์กรต่าง ๆ ใช้ประโยชน์จาก แอปพลิเคชันและจัดเก็บข้อมูลละเอียดอ่อนที่เกี่ยวข้องกับพนักงานและธุรกิจบนระบบคลาวด์ โดย Forbes คาดการณ์ว่าร้อยละ 83 ของปริมาณงานทั้งหมดขององค์กรจะถูกนำขึ้นมา อยู่บนระบบคลาวด์ภายในปี พ.ศ.2563 ซึ่งการละเมิดข้อมูล การกำหนดค่าอินเตอร์เฟส (Interface) และ API (Application Programing Interface) ที่ไม่ถูกต้องปลอดภัย การลักลอบ ใช้บัญชีภัยคุกคามภายในที่เป็นอันตรายและการโจมตี DDoS (Distributed Denial of Service) เป็นการพยายามที่จะทำให้บริการออนไลน์ไม่พร้อมใช้งาน สำหรับผู้ใช้งานมักจะเป็นการทำให้ระบบหยุดชะงัก หรือ ระงับการบริการของเซิร์ฟเวอร์โฮสต์ (Hosting server) ชั่วคราว ถือเป็นภัยคุกคามด้านความปลอดภัยอันดับต้น ๆ ของแพลตฟอร์มคลาวด์

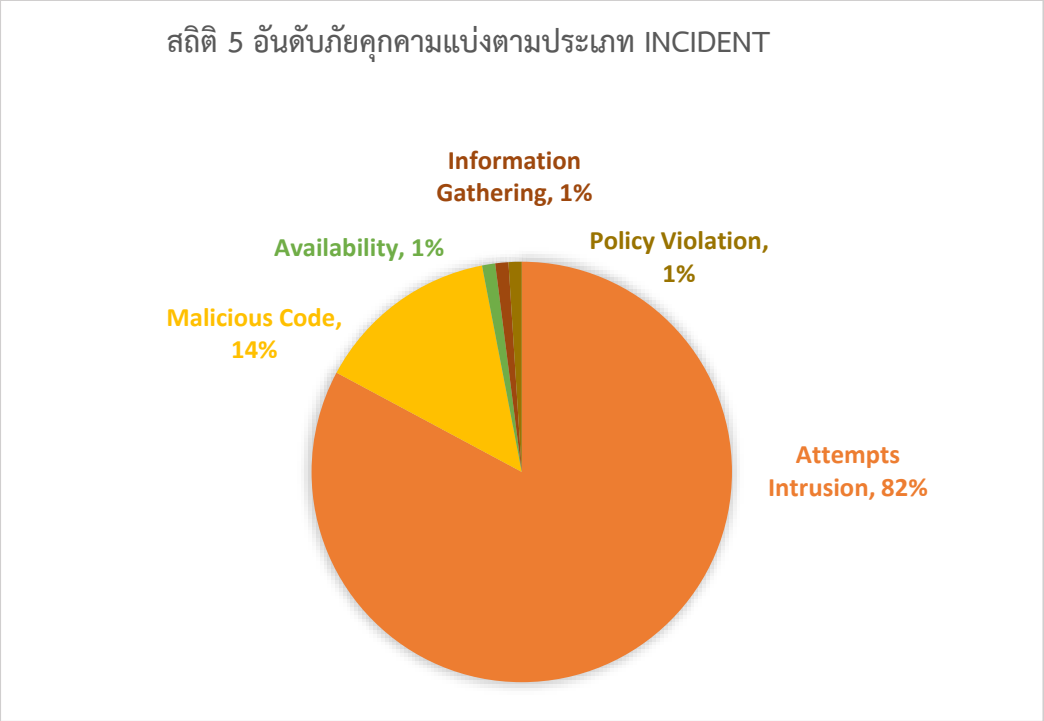
(4) Deepfake เป็นอีกรูปแบบหนึ่งของการปลอมแปลงเนื้อหาตั้งแต่ข้อความ ภาพ เสียง วิดีโอ หรือแม้กระทั่งบทความ คือ การปลอมแปลงอัตลักษณ์ของบุคคลด้วยปัญญาประดิษฐ์ ซึ่งในระยะเวลาอันใกล้นี้ Deepfake จะพัฒนาไปสู่วิธีการปลอมแปลงที่ซับซ้อนและดูน่าเชื่อถือมากขึ้น

(5) Machine Learning Poisoning อาชญากรไซเบอร์ใช้ประโยชน์จากข้อมูลที่ผู้ใช้สร้างขึ้น เช่น การให้คะแนนความพึงพอใจ ประวัติการซื้อ หรือการเข้าชมเว็บ เพื่อใช้หลอกลวง มีการฝังสคริปต์ (Script) ที่เป็นอันตราย หรือโทรจัน (Trojan) เพื่อใช้ทำลายระบบ

(6) Smart Contract Hacking เป็นการโจมตีสัญญาดิจิทัลอัจฉริยะ (Smart contract) บนแพลตฟอร์มบล็อกเชน (Blockchain) เช่น Ethereum ซึ่งทำงานด้วยเทคโนโลยีบล็อกเชน และมีการใช้เหรียญดิจิทัล คือ Ether (ETH) ในการขับเคลื่อนการทำงานของระบบ โดย Ethereum ถูกสร้างขึ้นมาเป็นแพลตฟอร์มแบบเปิด (Open Source) เพื่อให้นักพัฒนา นำเอาจุดเด่นด้านการทำ Smart Contract ไปพัฒนาและประยุกต์ใช้งานได้หลากหลาย แต่ก็เป็นการเปิดช่องโหว่ที่ให้เกิดการโจมตี Smart Contract ของ Ethereum ได้

(7) Social Engineering Attacks เช่น ฟิชชิง (Phishing) มักถูกใช้โดยอาชญากรไซเบอร์เพื่อหลอกลวง เอาข้อมูลส่วนบุคคลจากเหยื่อ เช่น ชื่อบัญชีและรหัสผ่านในการเข้าสู่ระบบเครือข่ายขององค์กร หรือการหลอกล่อข้อมูลบัตรเครดิตและข้อมูลสำหรับการทำธุรกรรมทางการเงิน โดยการฟิชชิง สามารถทำได้หลายวิธี ได้แก่ อีเมลฟิชชิง ที่เป็นการล่อลวงเหยื่อผ่านทางอีเมล หรือ SMiShing ซึ่งเป็นการล่อลวงเหยื่อผ่านระบบข้อความ SMS (SMS Phishing) บนโทรศัพท์เคลื่อนที่

นอกจากนี้ ยังสามารถจำแนกประเภทภัยคุกคามแบ่งตามประเภทอุบัติการณ์ (Incident) คือ เหตุการณ์ที่เกิดขึ้นโดยไม่ได้คาดคิดหรือคาดการณ์ไว้ล่วงหน้า มีดังนี้



ภาพที่ 2 สถิติ 5 อันดับภัยคุกคามแบ่งตามประเภท Incident

ที่มา: บริษัทโทรคมนาคมแห่งชาติ จำกัด (มหาชน), 2565

จากภาพที่ 2 พบว่า 5 อันดับภัยคุกคามแบ่งตามประเภท Incident (ประเภทภัยคุกคามอ้างอิงตามเอกสาร ECSIRT.net project on cooperation and common statics.) ได้แก่

ความพยายามจะบุกรุก/เข้าเจาะระบบ (Intrusion Attempts) ที่สามารถแบ่งย่อยได้เป็น 2 ประเภทคือ 1) Exploit Vulnerability เป็นพฤติกรรมที่มีการพยายามใช้ช่องทางต่าง ๆ โจมตีมายังเป้าหมาย อาจเป็นช่องโหว่ของระบบปฏิบัติการ แอปพลิเคชันต่าง ๆ ที่เพิ่งมีการค้นพบ หรือเป็นช่องโหว่เดิมที่มีอยู่ในระบบ หากเป้าหมายไม่ได้ทำการปิดช่องโหว่หรือแก้ไขก็อาจตกเป็นเหยื่อได้ รวมถึงการพยายามเข้าถึงเครือข่ายจาก IP ต้องสงสัย การเปิด Known Port โดยไม่จำกัดการเข้าใช้งาน เมื่อมีข้อมูลเหล่านี้แล้ว Hacker จะทดลองเจาะเข้ามายังเครือข่าย 2) Login Attempt สาเหตุหลักยังคงมาจาก Human Error หรือเกิดจากตัวผู้ใช้งาน อาทิ การลืมรหัสผ่าน การจดจำ User และ Password ไว้ในระบบแล้วไม่ได้ Update เมื่อทำการเปลี่ยนรหัสผ่าน ฯลฯ ภัยคุกคามชนิดนี้จะยังไม่มีอันตรายแต่

อาจทำให้เกิดความน่ารำคาญใจแก่ผู้ใช้งานหรือเจ้าของระบบเท่านั้น อย่างไรก็ตาม จากข้อมูลสถิติยังมีการตรวจพบความพยายาม Login และเข้าจากภายนอกผ่านช่องทาง Internet Access มายังระบบที่ต้องเปิดให้ผู้ใช้งาน หรือผู้ใช้บริการเข้าถึง ดังนั้น ทุกหน่วยงาน บริษัท หรือองค์กรต่าง ๆ ควรปฏิบัติตามนโยบายความมั่นคงปลอดภัยเกี่ยวกับ Password หรือรหัสผ่านอย่างเคร่งครัด รวมถึงหมั่นตรวจสอบว่าเป็นการพยายามเข้าถึงระบบจากภายนอกที่ผิดปกติหรือไม่ อีกทั้ง ควรมีแผนรับมือและจัดการกับเหตุการณ์ที่เกิดขึ้น เพื่อป้องกันผลกระทบและความเสียหายที่อาจเกิดขึ้นในอนาคต

การโจมตีด้วยโปรแกรมไม่พึงประสงค์ (Malicious Code) สาเหตุหลักมาจากพนักงานขององค์กรเองที่ขาดความรู้ความเข้าใจ และความตระหนักทางด้าน Cybersecurity รวมถึงการควบคุม Policy ที่ไม่รัดกุม ส่งผลให้มีมัลแวร์หลุดรอดเข้ามายังระบบจนส่งผลให้เกิดความเสียหายหนักตามมา ไม่ว่าจะเป็นการโดนโจมตีจาก Ransomware ไวรัส และโทรจัน ที่ยังมีให้พบได้อยู่เสมอ

ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering) ยังคงเป็นพฤติกรรมพื้นฐานของการเจาะระบบที่ Hacker หรือผู้ไม่หวังดีจะกระทำเพื่อหาข้อมูลเบื้องต้น การเก็บข้อมูลของเป้าหมายไม่ว่าจะเป็นจากการใช้เครื่องมือเฉพาะเจาะจงเพื่อค้นหา หรือแม้แต่ข้อมูลการประกาศรับสมัครงานขององค์กรเอง สิ่งเล็ก ๆ น้อย ๆ เหล่านี้ ล้วนเป็นช่องทางในการต่อยอดให้เหล่า Hacker เข้าถึงระบบของเราได้

การละเมิดนโยบายขององค์กร (Policy Violation) อาจจะด้วยความไม่ตั้งใจของพนักงาน เช่น การพยายามใช้งาน USB ซึ่งมักจะเป็นหนึ่งในช่องทางการแพร่มัลแวร์ การเข้าเว็บไซต์ต้องห้าม การแอบติดตั้งโปรแกรม หรือมาจากการโจมตีของผู้ไม่หวังดี เช่น การพยายามเข้าใช้งานระบบนอกเวลางานซึ่งเข้าถึงจากต่างประเทศ เป็นต้น

ดังนั้น ภัยคุกคามทางไซเบอร์อาจเกิดได้จากหลายอุบัติการณ์ที่คอยกระตุ้นจากพฤติกรรมของมนุษย์ตามบริบทของสังคมและทิศทางการเปลี่ยนแปลงด้านเทคโนโลยีทั่วโลก รวมทั้งจากการผสมผสานระหว่างภัยคุกคามรูปแบบเดิมและภัยคุกคามรูปแบบใหม่โดยมีเทคโนโลยีเป็นตัวขับเคลื่อนเหตุการณ์ที่เกิดขึ้นโดยไม่ได้คาดคิดหรือคาดการณ์ไว้ล่วงหน้า ซึ่งปัญหาสำคัญจากการโจมตีทางไซเบอร์ที่เกี่ยวข้องกับองค์กร มีตัวอย่างที่สามารถนำมาอธิบายได้ดังนี้

2.2.2 ภัยคุกคามไซเบอร์และโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ

พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ฉบับนี้มีวัตถุประสงค์เพื่อยกระดับการรักษาความมั่นคงปลอดภัยของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ให้มีประสิทธิภาพยิ่งขึ้น พร้อมทั้งมีมาตรการในการป้องกัน รับมือ และลดความเสี่ยงจากการบุกรุกโจมตีไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงของรัฐ เศรษฐกิจ และความสงบเรียบร้อยภายในประเทศ ซึ่ง CII หรือ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ที่หน่วยงานของรัฐหรือเอกชนใช้ในการดำเนินงาน เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ สาธารณะ และเศรษฐกิจของประเทศ รวมถึงโครงสร้างพื้นฐานที่เกิดประโยชน์แก่สาธารณะ หากระบบถูกรบกวนจะทำให้ไม่สามารถดำเนินงานหรือให้บริการได้ กำหนดโดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (MDES.) นอกจากนี้ เครื่องมือ อุปกรณ์ ระบบเครือข่าย ข้อมูลสารสนเทศ ฯลฯ ที่เป็นทรัพย์สินของหน่วยงาน และมีการใช้โครงสร้างพื้นฐานสำคัญทางสารสนเทศในการจัดการ จะต้องได้รับความปลอดภัยจากการถูกคุกคามทางไซเบอร์ เพื่อไม่ให้ทรัพย์สินทางสารสนเทศของหน่วยงานเสียหายหรือถูกทำลาย ซึ่งหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ประกอบด้วย 8 ด้าน ได้แก่

(1) หน่วยงานด้านความมั่นคงของรัฐ
(2) หน่วยงานด้านบริการภาครัฐที่สำคัญ
(3) หน่วยงานด้านการเงินการธนาคาร
(4) หน่วยงานด้านเทคโนโลยารสนเทศและโทรคมนาคม
(5) หน่วยงานด้านการขนส่งและโลจิสติกส์
(6) หน่วยงานด้านพลังงานและสาธารณูปโภค
(7) หน่วยงานด้านสาธารณสุข
(8) หน่วยงานด้านอื่น ตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม

แม้ว่าภาครัฐจะให้ความสำคัญในการรักษาความมั่นคงปลอดภัยให้กับโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศเพียงใด การใช้ข้อมูลและระบบข้อมูลที่เชื่อมต่อกันก็ยังนำมาซึ่งภัยคุกคามความมั่นคงปลอดภัย นับวันมีแต่จะเพิ่มขึ้น ไม่ว่าจะเป็นโค้ดอันตราย (Malicious Code) มัลแวร์ และซอฟต์แวร์ที่ไม่พึงประสงค์ เช่น ไวรัส โทรจัน โปรแกรมดักการพิมพ์ (Keystroke-Capturing) และสปายแวร์ ที่พบในซอฟต์แวร์ที่มีลิขสิทธิ์ไม่ถูกต้อง เว็บไซต์ หรือเครือข่ายแบบเพียร์ทูเพียร์ (peer-to-peer) ซึ่งสำหรับคนส่วนใหญ่ ผลจากการติดมัลแวร์หรือถูกบุกรุก มักจะทำให้คอมพิวเตอร์ทำงานช้าลง มีโฆษณาที่ก่อกวนใจโผล่ขึ้นมาให้เห็นบ่อยครั้ง และอาจโดนขโมยข้อมูลส่วนตัว แต่สำหรับภาครัฐและภาคเอกชน ผลที่ตามมานั้นร้ายแรงกว่ามาก การใช้ซอฟต์แวร์ที่มี

ลิขสิทธิ์ไม่ถูกต้อง ทำให้หน่อยงานของรัฐตกอยู่ในความเสี่ยงที่จะถูกเจาะระบบ จารกรรมข้อมูล หรือตกเป็นเป้าหมายของการก่อการร้ายทางเทคโนโลยีสารสนเทศ เพราะแฮกเกอร์สามารถใช้มัลแวร์เพื่อควบคุมโครงสร้างพื้นฐานที่สำคัญและข้อมูลที่สำคัญได้

การโจมตีระบบเทคโนโลยีสารสนเทศโดยมุ่งหวังสร้างความเสียหายต่อโครงสร้างพื้นฐานที่สำคัญ เช่น ระบบป้องกันภัยการบิน ระบบไฟฟ้า ระบบสาธารณูปโภค หรือภาคพลังงาน เช่น โรงไฟฟ้านิวเคลียร์ โรงกลั่นน้ำมันและแก๊ส ฯลฯ นอกจากนี้ยังรวมถึงภัยคุกคามของการโจมตีระบบเทคโนโลยีสารสนเทศที่พุ่งเป้าไปที่ประชาชนส่วนใหญ่ เพื่อสร้างความตื่นตระหนกในวงกว้าง สร้างความสูญเสียทางการเงิน หรือทำลายระบบการรักษาความมั่นคงปลอดภัย ภาครัฐส่วนใหญ่กำลังเตรียมความพร้อมรับมือการโจมตีครั้งต่อไปที่จะส่งผลกระทบมากขึ้น เนื่องจากซอฟต์แวร์และมัลแวร์ที่ถูกนำมาใช้ในการสร้างภัยคุกคามและการก่อการร้ายเริ่มซับซ้อนขึ้นเรื่อย ๆ ตัวอย่างเช่น ผู้ให้บริการน้ำประปาในแคลิฟอร์เนียพบว่า กลุ่มแฮกเกอร์สามารถควบคุมระบบน้ำประปาและสามารถสั่งเพิ่มสารเคมีเพื่อบำบัดน้ำ ในสถานการณ์ทำนองเดียวกันนี้ โปรแกรม Stuxnet ได้รับการออกแบบมาเพื่อโจมตีการทำงานของอุปกรณ์อิเล็กทรอนิกส์ (Electromechanical) ถูกมองว่าเป็นจุดพลิกผันของการโจมตีทางระบบเทคโนโลยีสารสนเทศ โปรแกรมตัวนี้ได้รับการค้นพบเมื่อปี พ.ศ. 2553 ซึ่งมีรายงานว่า Stuxnet ทำให้เครื่องแยกยูเรเนียม หนึ่งในห้าของประเทศอิหร่านสูญเสียการควบคุม (ทีมมายด์อินไซต์, 2564)

นอกจากนี้ การโจมตีแบบ Denial of Service (DoS) ต่อโครงสร้างพื้นฐานที่สำคัญของรัฐ ทำให้บริการหรือเซิร์ฟเวอร์ไม่สามารถเข้าถึงได้ การขโมยข้อมูลเพื่อใช้เข้าสู่ระบบคอมพิวเตอร์ต่าง ๆ หรือการเจาะระบบเครือข่ายนั้น เป็นขั้นแรกของการโจมตีแบบ DoS จากนั้นก็ใช้คอมพิวเตอร์ที่เข้าถึงแล้วเป็นฐานในการโจมตีเว็บไซต์เป้าหมาย โดยทำการร้องขอเข้าเว็บไซต์เป็นจำนวนมากจนกระทั่งระบบล่มหรือทำให้ผู้ใช้คนอื่นไม่สามารถเข้าเว็บไซต์นั้นได้ วิธีนี้สามารถทำเป็นแบบอัตโนมัติและขยายไปสู่การโจมตีแบบกระจายกำลัง (Distributed DoS หรือ DDoS) โดยใช้ซอฟต์แวร์ที่เรียกว่า “Botnets” เพื่อควบคุมคอมพิวเตอร์จำนวนมากในคราวเดียว ซึ่งการควบคุมคอมพิวเตอร์จำนวนมากเหล่านี้ Botnets ไม่จำเป็นต้องอาศัยทักษะขั้นสูงทางเทคโนโลยีสารสนเทศ โดยสามารถหาซื้อได้ในราคา 100 ถึง 200 เหรียญสหรัฐต่อคอมพิวเตอร์ที่ถูกควบคุมโดย Botnets 1,000 เครื่อง การโจมตีแบบ DoS ได้รับความนิยมสูง โดยมีระบบเทคโนโลยีสารสนเทศของรัฐบาลและสถาบันการเงินเป็นเป้าหมายยอดนิยม ซึ่งการโจมตีเหล่านี้เป็นโฉมหน้าใหม่ของการจู่โจมที่เปิดฉากขึ้นที่ประเทศเอสโตเนีย ในปี พ.ศ. 2550 และที่ประเทศจอร์เจีย ในปี พ.ศ. 2551 การโจมตีเอสโตเนียทำให้เว็บไซต์ของรัฐสภาล่ม บริการของรัฐและธนาคารหยุดชะงัก เครือข่ายต้องออฟไลน์ การทำงานของรัฐบาลและสื่อมวลชนถูกขัดขวางเพราะการโจมตีแบบ DoS หลายระลอก สำหรับประเทศซึ่งธุรกรรมทางการเงิน 90% ทำผ่านอินเตอร์เน็ต และการยื่นภาษี 70% ทำด้วยระบบอิเล็กทรอนิกส์นั้น

ผลกระทบที่เกิดขึ้นทำให้ประเทศอยู่ในสภาพง่อยเปลี้ย อีกตัวอย่างหนึ่งคือ การโจมตีกลับแบบ DoS ซึ่งทำให้เกิดความตึงเครียดระหว่างประเทศฟิลิปปินส์และไต้หวัน เมื่อต้นปี พ.ศ. 2556 จากเหตุการณ์ยิงชาวประมงไต้หวัน ทำให้ “นักเคลื่อนไหวแฮกเกอร์” ชาวไต้หวัน ระดมโจมตีแบบ DoS บนเว็บไซต์ของรัฐบาลฟิลิปปินส์และสร้างความเสียหายทางเศรษฐกิจโดยตรง

ท่ามกลางการขยายตัวของภัยคุกคามทางไซเบอร์จากการโจมตีแบบ DoS นั้น แอปพลิเคชันที่ใช้เทคโนโลยีอัจฉริยะมีความก้าวหน้าไปมาก และการถือกำเนิดของ “Internet of Thing” ทำให้อุปกรณ์อัจฉริยะต่าง ๆ ที่มี IP เพิ่มมากขึ้น ซึ่งอาจกลายเป็น Botnets หรือเป็นแพลตฟอร์ม (Platform) ใหม่สำหรับการระดมกำลังโจมตี ภัยคุกคามใหม่นี้ คือการหาช่องทางการโจมตีเพื่อเข้าควบคุมระบบประมวลผลของอุปกรณ์เหล่านี้ได้ด้วยตนเอง ซึ่งปัจจุบัน ระบบที่น่าเป็นห่วงอย่างยิ่งในการถูกโจมตี คือ ระบบ SCADA (Super-visory Control and Data Acquisition) ซึ่งรัฐนิยมใช้ควบคุมอุปกรณ์ของหน่วยงานด้านสาธารณูปโภคและโครงสร้างพื้นฐาน ตัวอย่างเช่น ระบบ SCADA ในควีนสแลนด์ ประเทศออสเตรเลีย ถูกเจาะระบบ ส่งผลให้เกิดน้ำเสียจากท่อไหลท่วมสวนสาธารณะและไหลลงคลองกั้นน้ำ มากไปกว่านั้นในปี พ.ศ. 2565 ประเทศออสเตรเลียถูกแฮกเกอร์ลักลอบเข้าถึงข้อมูลส่วนตัวทางด้านสุขภาพนับล้านรายการภายในบริษัทเมดิแบงก์ หนึ่งในเอกชนทำธุรกิจด้านการประกันสุขภาพที่ใหญ่ที่สุดในประเทศ คาดว่าข้อมูลส่วนบุคคลรั่วไหลไปถึง 3.9 ล้านคน ส่งผลให้รัฐบาลออกมายอมรับว่าบรรดาเอกชนยังมีระบบการรักษาความปลอดภัยที่ไม่เพียงพอ (ข่าวสดออนไลน์, 2565)

อีกหนึ่งภัยคุกคามประเภทใหม่ต่อโครงสร้างพื้นฐานสารสนเทศที่มักมุ่งเน้นการโจรกรรมทรัพย์สินทางปัญญา คือ Advanced Persistent Threats (APT) ซึ่งมีเป้าหมายแน่ชัด มีความต่อเนื่อง และรู้จักหลบซ่อนโดยใช้เทคนิคชั้นสูง จากการสำรวจโดย ISACA ซึ่งเป็นองค์กรเอ็นจีโอด้านการกำกับดูแลเทคโนโลยีสารสนเทศพบว่า 67.6% ของผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยคุ้นเคยว่า APT คืออะไรและมองว่าเป็นภัยคุกคามร้ายแรงต่อความมั่นคงของชาติและเศรษฐกิจ แต่อีก 53.4% ของผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยที่ตอบแบบสอบถาม เชื่อว่า APT ไม่ต่างอะไรจากภัยคุกคามเดิม ๆ อย่างโปรแกรมสอดแนมตระกูล NetTraveler ที่เป็นอันตรายได้เริ่มทำงานตั้งแต่ปี พ.ศ. 2547 แต่ไม่ค่อยแสดงพฤติกรรมไม่พึงประสงค์ จนกระทั่งปี พ.ศ. 2553-2556 NetTraveler ถูกใช้โดยแฮกเกอร์ เพื่อเจาะระบบคอมพิวเตอร์สำคัญ ๆ กว่า 350 เครื่องใน 40 ประเทศ ในปี พ.ศ. 2553 Google รายงานว่า ทางบริษัทเองรวมทั้งบริษัทอื่น ๆ หลายสิบแห่ง ตกเป็นเหยื่อของการโจมตีแบบ APT ซึ่งมีที่มาจากประเทศจีน และนำไปสู่การจารกรรมทรัพย์สินทางปัญญาจาก Google

อนึ่ง วัตถุประสงค์ของการโจมตีทางเทคโนโลยีสารสนเทศส่วนใหญ่ ก็เพื่อล้วงข้อมูลลับ ขโมยความลับทางการค้า หรือหาทางชิงความได้เปรียบเหนือบริษัทคู่แข่ง องค์กร หรือรัฐบาลอื่น โดยหลายปีที่ผ่านมา มีเหตุการณ์การจารกรรมข้อมูลเพิ่มขึ้นอย่างมาก ซึ่งมีองค์กรจำนวนน้อยที่

สามารถป้องกันตัวได้แบบครอบคลุม ตัวอย่างเช่น จากคดีดังในช่วงปี พ.ศ. 2554 – 2557 การถูกเจาะระบบโดยแฮกเกอร์แผ่วงกว้างและขยายตัวอย่างรวดเร็ว เหยื่อมีทั้งร้านค้าปลีก Zappos ของ Amazon บริษัทการตลาด Epsilon ธนาคาร Citigroup หน่วยงานภาครัฐต่าง ๆ เช่น กระทรวงกลาโหมของสหรัฐอเมริกาและรัฐบาลแคนาดา ผู้รับเหมาของกองทัพ Lockheed Martin เว็บไซต์เครือข่ายสังคม RockYou ผู้ให้บริการ Cloud อย่าง Gmail ของ Google และแม้กระทั่งด้านความมั่นคงปลอดภัย RSA ของ Symantec โดยการโจมตี eBay ซึ่งเป็นบริษัทยักษ์ใหญ่ด้านพาณิชย์อิเล็กทรอนิกส์ ในปี พ.ศ. 2557 ส่งผลให้ข้อมูล เช่น ที่อยู่อีเมล รหัสผ่านที่เข้ารหัสไว้ วันเกิด และที่อยู่ทางไปรษณีย์ ถูกขโมย จนทางบริษัท eBay ต้องขอให้ผู้ใช้ 145 ล้านรายของตนเปลี่ยนรหัสผ่านหลังถูกโจมตี (TRPC, 2015)

ปัจจุบันสถานการณ์ภัยคุกคามที่น่าจับตามองคือ การโจมตีโครงสร้างพื้นฐานที่สำคัญของประเทศ ในสถานการณ์ความขัดแย้งระหว่างยูเครนและรัสเซีย อันถือได้ว่าเป็นรูปแบบใหม่ของการทำสงคราม (Hybrid warfare) การบุกรุกทางทหารของรัสเซียในยูเครนเมื่อ 24 กุมภาพันธ์ ค.ศ. 2022 นำหน้ามาด้วยการโจมตีทางไซเบอร์ครั้งใหญ่และตามมาด้วยการยิงขีปนาวุธเพื่อถล่มเป้าหมายทางทหาร ประธานาธิบดี ปูติน ได้เตือนประเทศต่างๆ ที่ช่วยเหลือยูเครนว่า จะต้องเผชิญกับผลที่ตามมาอย่างไม่เคยเจอมาก่อน อย่างไรก็ตามประเทศสหรัฐฯ และพันธมิตรในยุโรปยังคงยืนหยัดด้วยการคว่ำบาตรต่อระบบการเงินของรัสเซีย โดยที่ปัจจุบันประธานาธิบดี ปูตินและกองทัพรัสเซียเริ่มรู้สึกถึงผลกระทบที่มาจากการคว่ำบาตร ซึ่งรัสเซียอาจขยายการโจมตีทางไซเบอร์ ด้วยการกำหนดเป้าหมายไปยังประเทศสหรัฐอเมริกาและในยุโรป ที่สำคัญบริษัทเอกชนในสหรัฐอเมริกานั้นมีแนวโน้มต้องเผชิญกับการถูกโจมตีฯ ที่สูงขึ้น เมื่อมีมาตรการในการคว่ำบาตรที่เพิ่มขึ้น ประกอบกับการสร้างความยืดหยุ่น คล่องตัวต่อภัยคุกคามทางไซเบอร์ (Resilience) ซึ่งเป็นความพยายามในการป้องกันที่ต้องร่วมมือกันระหว่างรัฐบาลสหรัฐฯและบริษัทเอกชน เป็นสิ่งที่ต้องเกิดขึ้น ถือเป็นสิ่งที่น่าศึกษาควรค่าแก่การเรียนรู้

ซึ่งปีที่ผ่านมาแฮกเกอร์ชาวรัสเซียได้ทำการปิดท่อส่งเชื้อเพลิง ครึ่งหนึ่งของแหล่งเชื้อเพลิงทางฝั่งตะวันออกของสหรัฐอเมริกา และปิดบริษัทที่ดำเนินงานเกี่ยวกับผลิตภัณฑ์จากเนื้อสัตว์ในสหรัฐอเมริกาจำนวน 20 เปอร์เซ็นต์ รัฐบาลสหรัฐฯ เตือนว่า รัสเซียได้พุ่งเป้าไปที่โครงสร้างพื้นฐานที่สำคัญของสหรัฐฯ อย่างต่อเนื่องในช่วงทศวรรษที่ผ่านมา ดังนั้นจึงมีเหตุผลที่เพียงพอจะคาดได้ว่า ภัยคุกคามไซเบอร์ประเภทต่างๆ ไม่ว่าจะเป็น มัลแวร์หรือรูปแบบอื่นใด มีโอกาสจะฝังตัวอยู่ในระบบสาธารณูปโภค ประปา พลังงาน การบิน และระบบการผลิตที่สำคัญของสหรัฐฯ ซึ่ง มาร์ค มอนโกเมอรี่ ผู้อำนวยการอาวุโสของศูนย์นวัตกรรมทางไซเบอร์และเทคโนโลยี (Center on Cyber and Technology Innovation: CCTI) แห่ง มูลนิธิปกป้องประชาธิปไตย (Foundation for Defense of Democracies: FDD) เป็นสถาบันวิจัยที่ไม่ฝักใฝ่ฝ่ายใดในวอชิงตันดีซี มุ่งเน้นที่ความ

มั่นคงของชาติและนโยบายต่างประเทศ ได้กล่าวว่า “ถ้ารัฐบาลเครมลินเปิดโอกาสในการโจมตีทางไซเบอร์ให้แก่อาชญากรไซเบอร์ของรัสเซีย สิ่งที่ตามมาคือ บริษัทเอกชนในสหรัฐอเมริการวมทั้งบริษัทในชาติตะวันตกอื่นๆ มีแนวโน้มที่จะเผชิญกับการโจมตีฯ ที่เพิ่มสูงขึ้น ถึงแม้จะมีข้อยกเว้นในบางประการ แต่ภาคเอกชนนั้นคงไม่พร้อมหรอกสำหรับสงครามไซเบอร์”

ในขณะที่สถาบันการเงินที่ใหญ่สุด มีความสามารถในการป้องกันทางไซเบอร์อันดับต้นๆ ของโลก ก็ไม่สามารถทำงานได้เป็นระยะเวลานานหากไฟฟ้าดับ ซึ่งแฮกเกอร์เข้าใจดีว่า การผลิตไฟฟ้านั้นขึ้นอยู่กับท่อส่งก๊าซธรรมชาติ ถ่านหินที่ขนส่งมาทางราง และแหล่งน้ำที่ถูกใช้เป็นตัวกลางในการทำความเย็น ทั้งหมดล้วนตกเป็นเป้าหมายในการโจมตีทางไซเบอร์ การสร้างความยืดหยุ่นคล่องตัวต่อภัยคุกคามทางไซเบอร์ (Resilience) นั้น ถือเป็นสิ่งที่สำคัญกล่าวได้คือ ต้องทำให้คอมพิวเตอร์และเครือข่ายที่มีอยู่นั้น สามารถทำงานได้อย่างต่อเนื่องภายใต้การโจมตี ที่เกิดขึ้น อันประกอบด้วย 3 ขั้นตอน คือ **ขั้นแรก** การลงทุนที่เพียงพอจากเจ้าของบริษัทและผู้ดำเนินการโครงสร้างพื้นฐานที่สำคัญเพื่อการป้องกันตนเอง **ขั้นที่สอง** ความพยายามในการป้องกันที่ร่วมกันระหว่างภาครัฐและภาคเอกชน และ **ขั้นที่สาม** ต้องเสริมการป้องปรามภัยคุกคามรวมทั้งบทลงโทษต่อผู้โจมตีด้วยวิธีทางไซเบอร์และการคว่ำบาตรทางเศรษฐกิจ ข้อมูลจากหัวข้อข่าวที่เกี่ยวกับการโจมตีทางไซเบอร์และแรนซัมแวร์ ที่ประสบความสำเร็จในบริษัทต่างๆ ของประเทศสหรัฐฯ นั้นถ้าคิดเป็นคะแนนก็ยืนยันได้ว่า หลายบริษัทยังทำได้ไม่ดีพอหรือยังอยู่ในระดับพอใช้เท่านั้น มีหลายบริษัทจำเป็นที่จะต้องดำเนินการมากกว่านี้ เพื่อการป้องกันบริษัทของตัวเอง โดยธรรมชาติของผู้ถูกโจมตีบนโลกไซเบอร์ คงไม่ต้องสงสัยถ้าเป็นผู้ปฏิบัติงานในรัฐบาลสหรัฐฯ ก็จะตอบโต้กลับด้วยการโจมตีโครงสร้างพื้นฐานของรัสเซีย แม้ว่าระบบของรัสเซียนั้นจะมีการบูรณาการที่น้อยกว่า ดังนั้นผลกระทบที่ได้จากการโจมตีโครงสร้างพื้นฐานของรัสเซียนั้น คงมีน้อยกว่าระบบของสหรัฐฯ (สรรสิริ สิริสันตคุปต์, 2565)

วลาดีมีร์ ปูติน ผู้นำรัสเซีย อาศัยประสบการณ์ที่มีอย่างมากพอของประชาชนในประเทศรัสเซีย เกี่ยวกับความล้มเหลวของโครงสร้างพื้นฐานที่สำคัญของรัสเซีย เช่น ระบบไฟฟ้า เพื่อจำกัดผลกระทบทางจิตใจที่มีต่อการโจมตีทางไซเบอร์บนโครงสร้างพื้นฐานของรัสเซีย ซึ่งถ้าหากประชาชนรัสเซียคุ้นเคยกับไฟฟ้าดับจากระบบที่มีการบำรุงรักษาที่ไม่ดีนั้น ไฟฟ้าดับจากการโจมตีทางไซเบอร์บนโครงสร้างพื้นฐานของรัสเซียดังกล่าว อาจมีความหมายหรือผลกระทบที่น้อยกว่า หมายถึงชาวรัสเซียได้รับผลกระทบจากการคว่ำบาตรทางเศรษฐกิจมากกว่า ในโลกแห่งความจริง สิ่งที่จะโค่นล้มการสร้างความยืดหยุ่นต่อภัยคุกคามทางไซเบอร์ (Resilience) ของโครงสร้างพื้นฐานได้อย่างแท้จริงคือ การขาดการป้องกันที่ร่วมกัน ฝ่ายบริหารของประธานาธิบดี โจ ไบเดน ได้พยายามปรับปรุงความร่วมมือระหว่างภาครัฐและเอกชน ผ่านการแต่งตั้งผู้อำนวยการไซเบอร์แห่งชาติคนแรก และได้สร้างความร่วมมือด้านการป้องกันทางไซเบอร์ร่วมกับบริษัทด้านความปลอดภัยทางไซเบอร์และบริษัทไอทีชั้นนำ ซึ่งความพร้อมบนโลกไซเบอร์ยังคงมีอยู่น้อยมาก เมื่อพูดถึงความยืดหยุ่นต่อภัยคุกคามทาง

ไซเบอร์ของโครงสร้างพื้นฐานนั้น มีความต้องการให้รัฐบาลสหรัฐฯ จัดเตรียมถึงลักษณะหรือรูปแบบภัยคุกคาม สัญญาณเตือนในแบบเรียลไทม์แก่บริษัทเอกชนและผู้ดำเนินการโครงสร้างพื้นฐานที่สำคัญของสหรัฐฯ ซึ่งเรียกร้องให้มีการจัดตั้งและทดสอบกลไกในการป้องกันทางไซเบอร์โดยรวม อาจจำเป็นต้องใช้ความสามารถจากบุคลากรและเครื่องมือด้านไซเบอร์ที่มีประสิทธิภาพมากสุดของรัฐบาลกลางสหรัฐฯ อาทิ ระบบอัตโนมัติ (Automation) ที่ใช้ความสามารถของ AI และ ML สำหรับการตรวจสอบในแบบเรียลไทม์ที่สามารถช่วยลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์ ทั้งหมดเพื่อการป้องกันเหล่าโครงสร้างพื้นฐานที่สำคัญของภาคเอกชนอย่างโรงงานไฟฟ้าจากการโจมตีที่อาจเกิดขึ้น (สรรสิริ สิริสันตคุปต์, 2565)

ดังนั้น การโจมตีโครงสร้างพื้นฐานที่สำคัญของประเทศกลายเป็นวาระสำคัญของประเทศมหาอำนาจ ที่ต้องเร่งหามาตรการรับมือ เพื่อสร้างความพร้อมที่มีความยืดหยุ่นและการรับมือได้อย่างรวดเร็ว ก่อนที่ภัยคุกคามไซเบอร์จะเข้าสร้างความเสียหายกับระบบสาธารณูปโภค ประปา พลังงาน การบิน และระบบการผลิตที่สำคัญ

2.2.3 สถานการณ์ภัยคุกคามทางไซเบอร์ในต่างประเทศ

2.2.3.1 การโจมตีไซเบอร์ทางไซเบอร์ต่อประเทศเอสโตเนีย

ในช่วงปลายเดือนเมษายนถึงพฤษภาคม ปี ค.ศ. 2007 ประเทศเอสโตเนียเผชิญกับการโจมตีทางไซเบอร์ต่อเนื่องนาน 3 สัปดาห์ เหตุการณ์ดังกล่าวเกิดขึ้นในช่วงที่เอสโตเนียตัดสินใจย้ายรูปปั้นทหารโซเวียตนิรนามออกไปจากที่ตั้งเดิมซึ่งอยู่ใจกลางกรุงทาล์ลินน์ เมืองหลวงของประเทศเอสโตเนีย รูปปั้นนี้เป็นอนุสรณ์สงครามโลกครั้งที่สองที่รำลึกถึงทหารโซเวียต การย้ายรูปปั้นนี้นำมาซึ่งความโกรธเคืองในหมู่ประชากรเชื้อสายรัสเซียที่อาศัยอยู่ในเอสโตเนีย พวกเขาทำการประท้วงที่กรุงทาล์ลินน์ จนเกิดเป็นจราจล ต่อมาเหตุการณ์นี้ถูกเรียกว่า “คืนบรอนซ์” เนื่องจากรูปปั้นดังกล่าวมีชื่อเรียกอย่างไม่เป็นทางการว่ารูปปั้นทหารบรอนซ์ นอกจากนี้การย้ายรูปปั้นทหารบรอนซ์ยังทำให้รัสเซียไม่พอใจ ในช่วงเวลาเดียวกันนี้เองที่เกิดการโจมตีไซเบอร์ต่อเอสโตเนีย เว็บไซต์ของหน่วยงานภาครัฐ, ธนาคารและพรรคการเมืองบางพรรคถูกโจมตี การให้บริการภาครัฐของเอสโตเนียซึ่งพึ่งพาการทำงานบนพื้นที่ไซเบอร์มากก็เกิดติดขัดชะงักงันอยู่พักหนึ่ง ความเสียหายทางธุรกิจก็เกิดขึ้นเนื่องจากต้องระงับการทำธุรกรรมทางการเงิน รูปแบบการโจมตีไซเบอร์เป็นลักษณะการโจมตีโดยปฏิเสธการให้บริการแบบกระจายด้วยคำสั่ง Distribute Denial of Service (DDoS) ทำให้ประเทศตกอยู่ท่ามกลางความชะงักงันของระบบทุกอย่างหยุดนิ่ง ระบบทุกระบบทางไซเบอร์ของเอสโตเนียถูกทำลายดั่งกับการชัทดาวน์คอมพิวเตอร์ รวมทั้งมีความพยายามในการเจาะระบบด้วย SQL Injection (การโจมตีที่ต้องการ

เจาะระบบการพิสูจน์ตัวตน) การโจมตีไซเบอร์ดำเนินควบคู่ไปกับการปล่อยข่าวที่บิดเบือน (Disinformation) ในพื้นที่ออนไลน์เหตุการณ์นี้ถือเป็นครั้งแรกที่ “เกิดการโจมตีไซเบอร์ต่อประเทศทั้งประเทศ” แม้ว่ารัสเซียจะปฏิเสธว่าเป็นผู้อยู่เบื้องหลังการโจมตีทางไซเบอร์ในครั้งนั้น แต่เอสโตเนียเชื่อว่ารัสเซียมีความเกี่ยวข้องกับการโจมตี

สำหรับการรับมือ กล่าวได้ว่าหน่วยงานภาครัฐฝ่ายความมั่นคงและกองทัพของเอสโตเนียสามารถรับมือได้ทันท่วงที อีกทั้งผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศจากองค์การสนธิสัญญาแอตแลนติกเหนือ (North Atlantic Treaty Organization) หรือ นาโต้ (NATO) ก็มาร่วมจัดการกับการโจมตีไซเบอร์ในฐานะที่เอสโตเนียเป็นสมาชิก แม้ว่ามาตรา 5 ของสนธิสัญญาป้องกันแอตแลนติกเหนือ จะไม่ถูกใช้ แต่ก็ได้มีการจัดตั้งศูนย์ความเป็นเลิศนาโต้ด้านความร่วมมือในการป้องกันไซเบอร์ (NATO Cooperative CyberDefence Centre of Excellence) พันธมิตรทางทหารที่ยิ่งใหญ่ที่สุดในโลก การท้าทายโดยการจู่โจมในครั้งนี้เปรียบได้เหมือนการทดสอบศักยภาพทางทหารขององค์กร NATO ในการรับมือภับคุกคามไซเบอร์ เวลาต่อมาที่กรุงทาล์ลินน์ในปัจจุบันนอกจากศูนย์บัญชาการไซเบอร์ (Cyber command) กระทรวงกลาโหมของเอสโตเนียหน่วยงานพลเรือนที่มีภารกิจเกี่ยวกับความมั่นคงไซเบอร์คือองค์การระบบสารสนเทศภาครัฐ (Katri Lindau, 2012) นอกจากนี้ที่น่าสนใจคือเอสโตเนียมีหน่วยไซเบอร์ในองค์การอาสาสมัครป้องกันประเทศ ซึ่งประกอบด้วยอาสาสมัครไซเบอร์ที่เข้ามามีส่วนร่วมในการป้องกันพื้นที่ไซเบอร์ของเอสโตเนีย อาจเรียกได้ว่าเป็นกองกำลังรบอาสาสมัครกึ่งทหาร (All-vol-unteer paramilitary force)

กล่าวได้ว่า การโจมตีไซทางเบอร์ในเอสโตเนียครั้งนี้อยู่ในระดับรุนแรงอีกทั้งยังเป็นภัยคุกคามทางไซเบอร์ที่ไม่เคยเกิดขึ้นมาก่อน ไม่มีการเตรียมความพร้อมในเชิงยุทธศาสตร์และกลยุทธ์ทางเทคนิค ซึ่งเป็นความท้าทายต่อองค์กร NATO เพราะเครือข่ายไซเบอร์ของเอสโตเนียถือเป็นส่วนหนึ่งของเครือข่าย NATO โดยจากเหตุการณ์ดังกล่าวทำให้องค์กร NATO ก่อตั้งหน่วยงานขึ้นเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในเมืองหลวงของประเทศเอสโตเนีย (นัทธมน เพชรกล้า, 2564)

2.2.3.2 การโจมตีไซเบอร์ทางไซเบอร์ต่อประเทศจอร์เจีย

เมื่อปี พ.ศ. 2551 เว็บไซต์ของสำนักข่าว OSInform และ OSRadio ถูกแฮ็ก เว็บไซต์ OSinform ที่ osinform.ru ซึ่งเนื้อหาถูกแทนที่ด้วยเนื้อหาของเว็บไซต์ Alania TV Alania TV รัฐบาลจอร์เจียสนับสนุนสถานีโทรทัศน์ที่มุ่งเป้าไปที่ผู้ชมในเซาท์ออสซีเชีย ปฏิเสธว่าไม่มีส่วนเกี่ยวข้องใดๆ ในการแฮ็กเว็บไซต์สำนักข่าวคู่แข่ง ดมิตรีเมโดเยฟ เหตุการณ์การโจมตีต่อมา ท่อส่งก๊าซ Baku–Tbilisi–Ceyhan ถูกโจมตีโดยผู้ก่อการร้ายใกล้กับ Refahiye ในตุรกีซึ่งเดิมทีเป็นความ

รับผิดชอบของพรรคแรงงานเคอร์ดิสถาน (PKK) แต่มีหลักฐานตามสถานการณ์ว่าแทนที่จะเป็นการโจมตีทางคอมพิวเตอร์ที่ซับซ้อน ระบบควบคุมและความปลอดภัยที่นำไปสู่การเพิ่มแรงดันและการระเบิด

จาร์ต อาร์มิน นักวิจัย กล่าวว่าเซิร์ฟเวอร์อินเทอร์เน็ตของจอร์เจียหลายแห่งอยู่ภายใต้การควบคุมจากภายนอกตั้งแต่วันที่ 7 สิงหาคม พ.ศ. 2551 การโจมตี DDoS ถึงจุดสุดยอดและเริ่มมีการโจมตีใน ส่วนสำคัญของการรับส่งข้อมูลทางอินเทอร์เน็ตของจอร์เจีย ซึ่งมีรายงานว่าเปลี่ยนเส้นทางผ่านเซิร์ฟเวอร์ในรัสเซียและตุรกี ซึ่งการรับส่งข้อมูลถูกบล็อกหรือเปลี่ยนเส้นทางเซิร์ฟเวอร์ รัสเซียและตุรกีถูกกล่าวหาว่า การโจมตีดังกล่าวถูกควบคุมโดยแฮกเกอร์ชาวรัสเซีย ต่อมาผู้ดูแลระบบเครือข่ายในเยอรมนีสามารถกำหนดเส้นทางการรับส่งข้อมูลทางอินเทอร์เน็ตของจอร์เจียชั่วคราวไปยังเซิร์ฟเวอร์ที่ดำเนินการโดย Deutsche Telekom AG ได้โดยตรง อย่างไรก็ตาม ภายในไม่กี่ชั่วโมง การรับส่งข้อมูลถูกเปลี่ยนเส้นทางไปยังเซิร์ฟเวอร์ในมอสโกอีกครั้ง โดยส่งผลให้เว็บไซต์ของสำนักข่าว RIA Novosti ถูกปิดใช้งานเป็นเวลาหลายชั่วโมงจากการโจมตีหลายครั้ง Maxim Kuznetsov หัวหน้าแผนกไอทีของหน่วยงานกล่าวว่า: "เซิร์ฟเวอร์ DNS และไซต์เองกำลังถูกโจมตีอย่างรุนแรง" และมีข่าวแจ้งเตือนว่าไซต์ในจอร์เจียที่ออนไลน์อาจเป็นของปลอม “โปรดใช้ความระมัดระวังกับเว็บไซต์ใดๆ ก็ตามที่มาจากแหล่งข้อมูลทางการของจอร์เจีย เนื่องจากเว็บไซต์เหล่านี้อาจเป็นการฉ้อโกง”

ต่อมาเว็บไซต์ของประธานาธิบดีจอร์เจียได้ถูกลบล้างและมีการโพสต์ภาพที่เปรียบเทียบประธานาธิบดีซาคัชวิลีกับอดอล์ฟ ฮิตเลอร์ นี่เป็นตัวอย่างของสงครามไซเบอร์ร่วมกับ PSYOP เว็บไซต์ของรัฐสภาจอร์เจียและบางเว็บไซต์เชิงพาณิชย์ของจอร์เจียก็เป็นเป้าหมายในการโจมตีเช่นกัน จอร์เจียกล่าวหาว่ารัสเซียทำสงครามไซเบอร์บนเว็บไซต์ของรัฐบาลจอร์เจียพร้อม ๆ กับการโจมตีทางทหาร กระทรวงการต่างประเทศจอร์เจียกล่าวในแถลงการณ์ว่า "การรณรงค์สงครามไซเบอร์โดยรัสเซียกำลังรบกวนเว็บไซต์ของจอร์เจียจำนวนมาก รวมถึงเว็บไซต์ของกระทรวงการต่างประเทศด้วย" โฆษกเครมลิน ปฏิเสธข้อกล่าวหาและกล่าวว่า ในทางกลับกัน เว็บไซต์อินเทอร์เน็ตจำนวนหนึ่งที่เป็นของสื่อรัสเซียและองค์กรทางการได้ตกเป็นเหยื่อของการโจมตีของแฮกเกอร์ร่วมกัน กระทรวงการต่างประเทศได้จัดทำบล็อกบนบริการ Blogger ของ Google เป็นเว็บไซต์ชั่วคราวของประธานาธิบดีจอร์เจียถูกย้ายไปยังเซิร์ฟเวอร์ของสหรัฐอเมริกา และเว็บไซต์ของธนาคารแห่งชาติของจอร์เจียถูกทำให้เสียหายและภาพของเผด็จการในศตวรรษที่ 20 และภาพของประธานาธิบดี Saakashvili แห่งจอร์เจียที่ถูกวางไว้เว็บไซต์รัฐสภาจอร์เจียถูกทำลายโดย "กลุ่มแฮ็คเซาท์ออสซีเชีย" และเนื้อหาถูกแทนที่ด้วยรูปภาพที่เปรียบเทียบประธานาธิบดีซาคัชวิลีกับฮิตเลอร์

เอสโตเนียให้บริการโฮสติ้งสำหรับเว็บไซต์ของรัฐบาลจอร์เจียและที่ปรึกษาการป้องกันทางไซเบอร์ อย่างไรก็ตาม โฆษกจากศูนย์พัฒนาระบบข้อมูลของรัฐเอสโตเนียกล่าวว่า

จอร์เจียไม่ได้ขอความช่วยเหลือ “เรื่องนี้จะถูกตัดสินโดยรัฐบาล” โดยมีรายงานว่าชาวรัสเซียวางระเบิดโครงสร้างพื้นฐานด้านโทรคมนาคมของจอร์เจีย รวมทั้งเสาสัญญาณ บริษัทเอกชนในสหรัฐอเมริกายังช่วยเหลือรัฐบาลจอร์เจียในการปกป้องข้อมูลที่ไม่ใช่การทำสงคราม เช่น เงินเดือนของรัฐบาลในระหว่างความขัดแย้ง อีกทั้ง แฮกเกอร์ชาวรัสเซียยังโจมตีเซิร์ฟเวอร์ของสำนักข่าว Azerbaijani Day.Az เหตุผลก็คือตำแหน่งของ Day.Az ในการปกปิดความขัดแย้งรัสเซีย-จอร์เจีย โดย ANS.az หนึ่งในเว็บไซต์ข่าวชั้นนำในอาเซอร์ไบจานก็ถูกโจมตีเช่นกัน หน่วยข่าวกรองของรัสเซียได้ปิดการใช้งานเว็บไซต์ข้อมูลของจอร์เจียในช่วงสงคราม เว็บไซต์ข่าวของจอร์เจีย Civil Georgia ได้เปลี่ยนการดำเนินงานเป็นโดเมน Blogspot ของ Google แม้จะมีการโจมตีทางไซเบอร์ นักข่าวชาวจอร์เจียก็สามารถรายงานเกี่ยวกับสงครามได้

บารัค โอบามาผู้สมัครชิงตำแหน่งประธานาธิบดีสหรัฐฯ เรียกร้องให้รัสเซียหยุดการโจมตีทางอินเทอร์เน็ตและปฏิบัติตามข้อตกลงหยุดยิง ประธานาธิบดีแห่งโปแลนด์ Lech Kaczynski กล่าวว่ารัสเซียกำลังปิดกั้น "พอร์ทัลอินเทอร์เน็ต" ของจอร์เจียเพื่อเสริมการรุกรานทางทหาร เขาเสนอเว็บไซต์ของตัวเองให้กับจอร์เจียเพื่อช่วยในการเผยแพร่ข้อมูล ผู้สื่อข่าวไร้พรมแดนประณามการละเมิดเสรีภาพของข้อมูลออนไลน์ตั้งแต่การปะทุของสงครามระหว่างจอร์เจียและรัสเซีย “อินเทอร์เน็ตกลายเป็นสมรภูมิที่ข้อมูลเป็นเหยื่อรายแรก” (Nichol & Georgia, 2009)

เหตุการณ์ต่อมาในปี พ.ศ. 2562 ที่ถูกเผยแพร่โดยเว็บไซต์ Emerging-Europe.com ในปี พ.ศ. 2563 อธิบายไว้ว่า สหราชอาณาจักรและจอร์เจียเชื่อว่ารัสเซียเกี่ยวข้องกับการโจมตีทางไซเบอร์ครั้งใหญ่ต่อจอร์เจียเมื่อ 28 ตุลาคม พ.ศ. 2562 ส่งผลให้เว็บไซต์หลายพันแห่งของจอร์เจียต้องปิดการให้บริการ และสถานีโทรทัศน์แห่งชาติของจอร์เจีย 2 แห่งต้องระงับการออกอากาศเป็นเวลาหลายชั่วโมง ทั้งนี้ ผลการสืบสวนระหว่างศูนย์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติของสหราชอาณาจักร (National Cyber Security Centre - NCSC) ร่วมกับจอร์เจียพบหลักฐานบ่งชี้ว่า หน่วยข่าวกรองทหารรัสเซีย (Main Intelligence Administration-GRU) เป็นผู้ดำเนินการโจมตีดังกล่าว เนื่องจากพบว่ากลุ่มแฮกเกอร์ Sandworm team, BlackEnergy Group, Telebots และ VoodooBear เกี่ยวข้องกับการโจมตีดังกล่าวเป็นกลุ่มที่ดำเนินงานโดย GRU's Main Centre of Special Technologies หรือ GTsST หรือภายใต้รหัส 74455 สังกัด GRU ทั้งนี้ นาย Dominic Raab รมว.กต.สหราชอาณาจักร แถลงว่า การโจมตีทางไซเบอร์ที่ไร้ความรับผิดชอบของ GRU ถือเป็นการละเมิดอธิปไตยของจอร์เจียซึ่งเป็นสิ่งที่ไม่สามารถยอมรับได้ และเรียกร้องให้รัสเซียเคารพกฎหมายระหว่างประเทศ

สรุปได้ว่า การโจมตีไซทางเบอร์ในจอร์เจียครั้งนี้ เป็นภัยคุกคามในระดับวิกฤติ กระทบต่อความสงบเรียบร้อยของประชาชน เป็นภัยต่อความมั่นคงของรัฐ ทำให้ประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้าย การรบหรือสงคราม เนื่องด้วย

สถานการณ์ในจอร์เจียเป็นความขัดแย้งสืบเนื่องที่ก่อตัวมาจากการทำสงครามทางทหารระหว่างรัสเซียและจอร์เจีย โดยมีประเทศอื่น ๆ เข้ามามีส่วนเกี่ยวข้อง การไม่เคารพต่อกฎหมายสร้างความวุ่นวาย ถือเป็นจุดอ่อนของการพัฒนาและบริหารประเทศ รวมถึงยุทธศาสตร์การต่อต้านภัยคุกคามและการก่อการร้ายทางไซเบอร์ที่ยังไม่แข็งแรงมากพอ

2.2.3.3 การโจมตีทางไซเบอร์ของประเทศรัสเซีย

รัสเซียเป็นอีกประเทศหนึ่งที่ถูกกล่าวหาบ่อยครั้งว่าเป็นผู้ใช้ไซเบอร์ในการรุกรานชาติอื่นก่อน โดยเฉพาะการโจมตีที่จะต้องอาศัยผู้เชี่ยวชาญระบบคอมพิวเตอร์โดยเฉพาะการเจาะระบบแบบ DoS ใช้เทคนิคโฆษณาชวนเชื่อในสมัยสงครามเย็น เป็นการแพร่กระจายข่าวลวงผ่านระบบอินเตอร์เน็ต สนับสนุนกลุ่มตน มีการใช้เทคโนโลยีที่ชื่อว่า “SORM” ซึ่งเป็นการก่อกวนกลุ่มผู้ที่ไม่เห็นด้วยกับรัฐบาลด้านไซเบอร์ สำหรับรัสเซียนั้นรัฐบาลมีศักยภาพมากในการควบคุมเทคโนโลยีไซเบอร์ เพราะฉะนั้นหากมีการก่อกวนจากกลุ่มชน รัฐบาลจะเป็นผู้แสดงและตรวจจับผู้ที่ปลุกปั่น การดำเนินการดังกล่าวเป็นของหน่วยงานข่าวกรองสัญชาติรัสเซีย เป็นหน่วยงานด้านความมั่นคงของมีชื่อเรียกว่า Federal Security Service: FSB ซึ่งในอดีตเคยเป็นส่วนหนึ่งของแผนกที่ 16 ของหน่วยเคจีบี (KGB) ในขณะที่หน่วยงานอื่น ๆ อยู่ภายใต้การควบคุมของกระทรวงมหาดไทยและกิจการทางทหารของรัสเซีย (นัทธมน เพชรกล้า, 2565)

รัสเซียเป็นประเทศสหพันธรัฐการเกิดความร่วมมือกับประเทศเพื่อนบ้านซึ่งเคยเป็นหนึ่งในประเทศโซเวียต จึงเป็นเรื่องง่ายที่รัสเซียจะพัฒนาความก้าวหน้าทางไซเบอร์ ยกตัวอย่างการเกิดการก่อการร้ายในรูปแบบไซเบอร์ของประเทศลัตเวีย โดยในการก่อการร้ายนั้นไม่ได้เป็นการก่อการร้ายแบบองค์กรอาชญากรรมแต่เป็นการก่อการร้ายในระดับบุคคลที่มีความร่วมมือและเต็มใจที่จะช่วยรัสเซีย การก่อการร้ายครั้งนี้มุ่งโจมตีประเทศจอร์เจีย โดยประเทศอเมริกาได้ให้ข้อสังเกตว่าการจู่โจมมาจากคอมพิวเตอร์ส่วนบุคคล ไม่มีส่วนเกี่ยวข้องใด ๆ กับภาครัฐของรัสเซียที่ถูกกล่าวหา นอกจากนี้ยูเครนและลัตเวียยังร่วมมือให้การช่วยเหลือรัสเซียในสงคราม South Ossetia War ในปี 2008 การโจมตีจะใช้กองทัพซอมบี้ (Zombie Army) โดยอาศัยนักเจาะระบบคอมพิวเตอร์ที่จะถูกควบคุมโดยหน่วยงานลับหลายหน่วยงาน เช่น ในเหตุการณ์จับตัวประกันในโรงหนังกลางกรุงมอสโคว์ ในปี 2002 โดยรัสเซียได้ใช้อาวุธไซเบอร์ที่เรียกว่า “Snake” จะทำให้เกิดความเสียหายต่อระบบเครือข่ายของรัฐ Hacker ชาวรัสเซียจะแสวงหาประโยชน์จากข้อบกพร่อง (Bug) ในโปรแกรม Microsoft Windows และโปรแกรมอื่น ๆ เพื่อหาความลับที่รัฐบาลเก็บไว้ สิ่งเหล่านี้เกิดขึ้นกับองค์การ นาโต้ (NATO) สหภาพยุโรป (European Union) และบริษัทต่าง ๆ ที่อยู่ในสายพลังงานและโทรคมนาคม ด้วยเหตุนี้ทำให้เชื่อได้ว่าเหตุการณ์ไฟฟ้าดับในยูเครนเกิดจากการโจมตีด้านไซเบอร์

ของรัสเซีย มีรัฐบาลรัสเซียอยู่เบื้องหลัง การกระทำครั้งนี้ใช้การโจมตีแบบ Malware เข้าทำลายเครือข่ายระบบไฟฟ้าของยูเครนในเดือนธันวาคม ปี 2005 (กรมพัฒนาสังคมและสวัสดิการ, 2563)

ไมโครซอฟท์ เปิดเผยรายงานล่าสุดผ่านเว็บบล็อกอย่างเป็นทางการในหัวข้อที่มีชื่อว่า Defending Ukraine: Early Lessons from the Cyber War เขียนโดยแบรด สมิธ ประธานของไมโครซอฟท์ และเป็นผู้บริหารสูงสุดฝ่ายกฎหมายของบริษัท ระบุว่า แฮกเกอร์ชาวรัสเซียที่มีรัฐบาลเป็นผู้หนุนหลังได้มีความพยายามสอดแนมชาติพันธมิตรของยูเครน นับตั้งแต่รัฐบาลมอสโกตัดสินใจบุกยูเครนในเดือนกุมภาพันธ์ที่ผ่าน รายงานดังกล่าวบอกอีกด้วยว่า องค์กรจำนวนกว่า 128 องค์กร และอีก 42 ประเทศ ซึ่งเป็นพันธมิตรของยูเครน ตกเป็นเป้าในการสอดแนม โดยประเทศที่เป็นเป้าหมายในการสอดแนมมากที่สุด นั่นคือ สหรัฐอเมริกา ตามด้วยชาติพันธมิตรในองค์การสนธิสัญญาแอตแลนติกเหนือ (NATO) เช่นเดียวกับองค์กรต่างๆ ที่อยู่ในประเทศเดนมาร์ก, ลัตเวีย, ลิทัวเนีย, นอร์เวย์, โปแลนด์ ตลอดจนถึงฟินแลนด์ และสวีเดน เป้าหมายของแฮกเกอร์รัสเซียเน้นไปที่หน่วยงานของรัฐบาล มีอยู่บ้างที่จะไปสอดแนมหน่วยงานสถาบันวิจัยเพื่อการพัฒนาประเทศ, กลุ่มที่เป็นถังความคิด (Think Tank), องค์กรด้านสิทธิมนุษยชน และโครงสร้างพื้นฐานสำคัญในด้านความสำเร็จของการแฮก อัตราการแฮกสำเร็จอยู่ที่ 29% และบางกรณีก็นำไปสู่การโจรกรรมข้อมูลอีกด้วย (ไทยรัฐออนไลน์, 2565)

ผู้วิจัยสนใจว่า การโจมตีทางไซเบอร์ของรัสเซียนั้น ถือเป็นภัยคุกคามทางไซเบอร์ระดับวิกฤติต่อประเทศที่ตกเป็นเหยื่อในการทำสงครามไซเบอร์ เพราะความต้องการของแฮกเกอร์รัสเซีย ไม่ได้มุ่งหมายเพียงเพื่อก่อความวุ่นวาย หรือทำให้เกิดการหยุดชะงักของระบบคอมพิวเตอร์เท่านั้น หากแต่จ้องทำลายระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากและขยายเป็นวงกว้างในระดับประเทศ โดยส่งผลกระทบรุนแรงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานที่สำคัญอื่นๆ ก่อตัวกลายเป็นสงครามไซเบอร์ (Cyber War)

2.2.3.4 การโจมตีทางไซเบอร์ของประเทศอิหร่าน

การแลกเปลี่ยนคริปโตเคอร์เรนซี โครงสร้างพื้นฐานทางการเงิน และห่วงโซ่อุปทานของบริษัทซาอุดิอาระเบียและบริษัทอเมริกันล้วนเป็นเป้าใหญ่ที่พร้อมจะถูกโจมตีจากเหล่าแฮกเกอร์ที่อิหร่านให้การสนับสนุนได้ทุกเมื่อ เพื่อตอบโต้การที่ประเทศสหรัฐอเมริกาใช้มาตรการคว่ำบาตรทางเศรษฐกิจและต้องการสร้างความปั่นป่วนแก่ภาคธุรกิจตลอดจนเครือข่ายการทำงานของรัฐบาล อิหร่านแสดงให้เห็นมาตั้งแต่ปี พ.ศ. 2555 แล้วว่าสามารถโจมตีทางไซเบอร์เพื่อสร้างความปั่นป่วนและสร้างความเสียหายทางธุรกิจและเศรษฐกิจของสหรัฐได้ตลอดเวลา ที่จริงทุกวันนี้ก็มีการเผชิญหน้ากันอยู่แล้วในโลกไซเบอร์ระหว่างสหรัฐและอิหร่าน แต่นับจากนี้ไป การเผชิญหน้ากันจะรุนแรงมากขึ้น นายพลกาเซ็ม โซไลมานี ถือเป็นสถาปนิกคนสำคัญผู้ออกแบบอิทธิพลของอิหร่านใน

ภูมิภาคตะวันออกกลาง นำทัพต่อกรกับกองกำลังญิฮัด ขยายบทบาททางการทูตของอิหร่านในอิรัก ซีเรีย และอื่น ๆ ที่สำคัญดูแลหน่วยงานข่าวกรองและเป็นผู้บัญชาการกองกำลังนักรบคุดส์ ซึ่งเป็นหน่วยรบพิเศษในต่างประเทศของกองกำลังพิทักษ์การปฏิวัติอิหร่าน (ไออาร์จีซี) ขึ้นตรงกับอยาตอลเลาะห์ อาลี คาเมเนอี ผู้นำสูงสุดของอิหร่าน มีอิทธิพลต่อภูมิภาคตะวันออกกลางมาตั้งแต่ปี พ.ศ. 2561

ไออาร์จีซี เป็นหน่วยงานที่พัฒนาขีดความสามารถด้านการโจมตีทางไซเบอร์ บ่มเพาะเหล่าแฮกเกอร์อิสระทั้งหลายให้มีฝีไม้ลายมือในการแฮกข้อมูลขั้นเทพ เน้นล้วงความลับหน่วยงานรัฐบาลต่างประเทศ บริษัทข้ามชาติและโจมตีโครงสร้างพื้นฐานของประเทศที่เป็นปฏิปักษ์ และตลอด 10 ปีที่ผ่านมา เหล่าแฮกเกอร์อิหร่านปฏิบัติการโจมตีเป้าหมายที่เป็นบริษัทเอกชนและหน่วยงานรัฐบาลประเทศต่างๆมานับไม่ถ้วน โดยในปี พ.ศ. 2555 แฮกเกอร์ ซึ่งเรียกตัวเองว่า "Cutting Sword of Justice" อ้างความรับผิดชอบเหตุโจมตีทางไซเบอร์บริษัทซาอุดี อารามโค บริษัทน้ำมันแห่งชาติของซาอุดีอาระเบีย จนทำให้คอมพิวเตอร์ประมาณ 30,000 เครื่องใช้งานไม่ได้ และพนักงานของบริษัทต้องใช้เครื่องพิมพ์ดีดและเครื่องโทรสารทำงานแทนกินเวลานานเกือบสัปดาห์ ส่งผลให้บริษัทน้ำมันรายใหญ่ของซาอุฯเปลี่ยนคอมพิวเตอร์ใหม่ทั้งหมด

ในปีถัดมา มีการโจมตีระบบคอมพิวเตอร์ในลาสเวกัส แซนด์ ของ “เชลดอน อเดลสัน” มหาเศรษฐีอเมริกัน ที่ได้รับการหนุนหลังจากอิสราเอลด้วยมัลแวร์ จนทำให้เซิร์ฟเวอร์ของกาสิโนเสียไปประมาณ 2 ใน 3 คิดเป็นมูลค่าความเสียหายต่อธุรกิจหลายสิบล้านดอลลาร์ ซึ่งสหรัฐกล่าวหาว่าเป็นฝีมือของแฮกเกอร์อิหร่าน “จิม เราส์” รองประธานบริหารฝ่ายปฏิบัติการไซเบอร์ของโฮรางอี บริษัทด้านการรักษาความปลอดภัยบนโลกไซเบอร์ ในสิงคโปร์ กล่าวว่า การโจมตีโดยตรงต่อหน่วยงานราชการสหรัฐ เป็นเรื่องที่ทำได้ยากขึ้น ทำให้แฮกเกอร์เลือกที่จะเล่นงานบริษัทที่ได้รับมอบฉันทะ ซัพพลายเชน และผู้ค้าฝ่ายที่ 3 แทน บรรดาเจ้าหน้าที่สืบสวน และผู้เชี่ยวชาญ ยังชี้ถึงจุดอ่อนที่อาจตกเป็นเป้าการโจมตีจากกลุ่มแฮคเกอร์อิหร่านว่า รวมถึง แหล่งเอาท์ซอร์สของบริษัทต่างๆ และบริษัทสนับสนุนเทคโนโลยีทางไกล ที่สามารถเข้าถึงผู้ดำเนินธุรกิจต่างๆ โลจิสติกส์ขนาดใหญ่ และผู้จัดหาบริการต่างๆ ให้กับฐานทัพสหรัฐในเอเชีย หรือแม้กระทั่งห่วงโซ่อุปทานของบริษัทเทคโนโลยีอเมริกันเอง (กรุงเทพธุรกิจ, 2563)

ผู้วิจัยสนใจว่า บริษัทข้ามชาติมีความเสี่ยงสูงที่จะได้รับความเสียหายในการทำสงครามไซเบอร์ระหว่างสหรัฐกับอิหร่าน หลังจากการที่สหรัฐสังหารนายพลกาเซ็ม โซไลมานีของอิหร่าน ไม่ได้จุดชนวนไปสู่การเปิดศึกระหว่างสหรัฐกับอิหร่านอย่างเต็มรูปแบบ ซึ่งการโจมตีทางไซเบอร์ในครั้งนี้ แม้ว่าจะเริ่มต้นด้วยลักษณะของภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง แต่สถานการณ์การโจมตีทวีความรุนแรงจนสร้างความเสียหายต่อระบบเซิร์ฟเวอร์และกระทบต่อโครงสร้างพื้นฐานของประเทศ จนกระทั่งเข้าขั้นวิกฤติที่อาจจะก่อให้เกิดสงครามทางไซเบอร์ได้ในอนาคต

2.2.3.5 การโจมตีไซเบอร์ในประเทศสิงค์โปร์

บทเรียนที่สำคัญของสิงค์โปร์ในปี พ.ศ. 2561 คือเรื่อง “สิงคโปร์ เฮลธ์เซอร์วิส” ซึ่งเรียกกันสั้นๆ ว่า “สิงค์เฮลธ์” กลุ่มธุรกิจการแพทย์ที่ใหญ่ที่สุดของประเทศ ถูกแฮคเกอร์มือดีเจาะระบบเข้าลักลอบตรวจสอบและอาจก็อปปี้บันทึกข้อมูลของผู้ป่วยไปมากถึง 1.5 ล้านบันทึก นี่คือการลักลอบเจาะระบบคอมพิวเตอร์ครั้งใหญ่ที่สุด ร้ายแรงที่สุด เท่าที่สิงคโปร์เคยเผชิญมา เอส. อิสวารัน รัฐมนตรีข้อมูลข่าวสารและโทรคมนาคมของสิงคโปร์ ได้กล่าวถึงเรื่องนี้ไว้น่าสนใจว่า การเจาะระบบดังกล่าวที่ผ่านมา ผู้ร้ายให้ความสนใจเป็นพิเศษ ต่อบันทึกทางการแพทย์ของ ลี เซียนหลุง นายกรัฐมนตรีสิงคโปร์ ถึงขนาดพยายามพุ่งเป้าเข้าไปที่บันทึกข้อมูลชุดนี้ซ้ำแล้วซ้ำอีก ที่น่าสนใจก็คือ แฮคเกอร์ ไม่ได้สนใจข้อมูลส่วนอื่นๆ ไม่ว่าจะเป็นบันทึกการวินิจฉัยโรค หรือบันทึกผลการตรวจสอบโรค หรือคำแนะนำของแพทย์ แต่มุ่งไปที่ข้อมูลส่วนตัวของผู้ป่วยแต่ละรายเท่านั้น ในจำนวนผู้ป่วย 1.5 ล้านรายที่ถูกฉกข้อมูลส่วนตัวไปนี้ ส่วนหนึ่งคือราว 160,000 รายเป็นผู้ป่วยนอก กิจการของ สิงค์เฮลธ์ นั้นมีโรงพยาบาลอยู่ในเครือ 2 โรงพยาบาล มีสถานพยาบาลเฉพาะทางอีก 5 ศูนย์ รองรับผู้ป่วยจากทั่วโลก

ข้อมูลเหล่านี้ทำให้มีความเป็นไปได้ว่า กรณีนี้เหมือนกับหลายๆ กรณีทั่วไปที่เคยปรากฏในหลายประเทศ ทั้งในโลกตะวันตกและบ้านใกล้เรือนเคียงของเรา อาทิ ฮ่องกง เป็นต้น เป้าหมายของผู้ไม่ประสงค์ดีในกรณีนี้ก็คือ การนำเอาข้อมูลที่ได้ ไปขายให้กับคนร้ายอื่นๆ ข้อมูลที่ขายได้ มีตั้งแต่ ข้อมูลบัตรเครดิต เรื่อยไปจนถึงข้อมูลสำหรับทำบัตรหรือเอกสารประจำตัวปลอมขึ้นมา ตั้งแต่พาสปอร์ต บัตรประชาชน หรืออื่นๆ ในบางกรณีที่เคยเกิดขึ้นกับเอเยนซีท่องเที่ยวรายใหญ่ของฮ่องกง แฮคเกอร์แสดงตนชัดเจน เรียกค่าไถ่ข้อมูลลูกค้าที่ถูกเข้ารหัสให้บริษัทเข้าถึงไม่ได้ เป็นเงินหลายล้าน เป็นต้น แต่ในกรณีของสิงคโปร์ ผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ และรัฐมนตรีอิสวารัน บอกตรงกันว่า ร่องรอยที่ทิ้งไว้ให้พอตรวจสอบย้อนรอยกลับคืนได้นั้น แสดงให้เห็นว่าคนลงมือเป็น “สเตท แอคเตอร์” ซึ่งคำนี้เป็นคำที่คนในวงการความปลอดภัยทางไซเบอร์ รู้กันดีว่า หมายถึง “เจ้าหน้าที่ของรัฐ” หรือ “บุคคลที่ทำงานให้กับรัฐบาล” สำหรับใช้เป็นเครื่องมือในการโจมตีทางไซเบอร์ต่ออีกประเทศหนึ่ง และผู้ลงมือทำงานต่อเนื่อง วางแผนมาเป็นอย่างดี ไม่ได้ต้องการเงิน แต่ต้องการ “ข้อมูล” หรือไม่ก็ต้องการ “ขัดขวาง” การดำเนินการของเป้าหมาย และแต่ยกตัวอย่างผลงานที่ “สเตท แอคเตอร์” ทำไว้ในระยะหลังๆ แล้วเป็นข่าวคราวดังไปทั่วโลกไว้ด้วย อาทิ เช่นการเจาะระบบคอมพิวเตอร์ของพรรคเดโมแครตในปี ค.ศ. 2016 ซึ่งถูกหน่วยข่าวกรองอเมริกันระบุว่าเป็นผลงานของแฮคเกอร์ที่ทำงานให้กับทางการรัสเซีย หรือในกรณี การเจาะระบบของสำนักงาน

บริหารงานบุคคลแห่งสหรัฐอเมริกา ฉกข้อมูลทหารไปกว่า 20 ล้านข้อมูล ซึ่งถูกระบุว่า มีต้นตอจากประเทศจีน แต่ไม่ใช่เพียง 2 ประเทศนี้เท่านั้นที่มีแฮคเกอร์มือดีทำงานประสงค์ร้ายให้กับทางการ ยังมีอีกหลายต่อหลายประเทศ บางประเทศอย่างเช่น เกาหลีเหนือ ถึงกับมี “กองทัพไซเบอร์” ของตัวเองด้วยซ้ำไป (ไพรัตน์ พงศ์พานิชย์, 2561)

กรณีการโจมตีทางไซเบอร์ต่อสิงคโปร์ จึงเป็นเรื่องที่ผู้วิจัย สนใจศึกษาไว้เป็นบทเรียน เพราะถือเป็นภัยคุกคามทางไซเบอร์ที่ไม่เพียงแค่กระทบความมั่นคงปลอดภัยไซเบอร์เท่านั้น แต่ยังส่งผลถึงความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล เรื่องใกล้ตัวของประชนชนที่ทุกองค์กร ควรให้ความสำคัญเป็นอย่างมากในการหาแนวทางการป้องกันภัยคุกคามทางไซเบอร์ไว้ในอนาคต เพราะยิ่งทุกระบบเชื่อมต่อออนไลน์มากขึ้น ความเสียหายจากการโจมตีทำนองนี้ยิ่งมากขึ้นเป็นเงาตามตัว

2.2.3.6 การโจมตีไซเบอร์ในประเทศสหรัฐอเมริกา

เมื่อปี พ.ศ. 2564 ที่ผ่านมา ในรัฐฟลอริดา ประเทศสหรัฐอเมริกา แฮกเกอร์ได้ทำการเจาะระบบเครือข่ายคอมพิวเตอร์ที่โรงบำบัดน้ำ Oldsmar รัฐฟลอริดา โดยใช้โปรแกรมควบคุมคอมพิวเตอร์ระยะไกล หรือ TeamViewer เข้าบุกรุกระบบคอมพิวเตอร์บนหน้าจอเพื่อปรับแต่งค่าแรงดันน้ำและได้ทำการเปลี่ยนระดับโซเดียมไฮดรอกไซด์ (Sodium Hydroxide) ซึ่งใช้ในการกำจัดโลหะ และควบคุมความเป็นกรดในน้ำ โดยปรับจากอัตราส่วนเดิมคือ 100 ส่วนต่อล้านให้กลายเป็น 11,100 ส่วนต่อล้าน จนถึงขั้นที่เรียกได้ว่า “อันตรายถึงขีดสุด” เสี่ยงคนตายยกเมืองหากมีการใช้น้ำในการบริโภค แต่ในขณะนั้นมีพนักงานได้สังเกตเห็นความผิดปกติ และรีบดำเนินการจัดการปรับค่าสารเคมีในน้ำให้กลับมาอยู่ที่ระดับเดิมทันที ไม่เช่นนั้นแล้วน้ำที่ปนเปื้อนโซเดียมไฮดรอกไซด์ในปริมาณที่สูงเกินไปนี้ อาจจะถูกส่งไปยังบ้านเรือนต่าง ๆ และประชาชนทั่วไปอาจดื่มเข้าไปได้ โดยข้อมูลนี้ ถูกเปิดเผยโดย Bob Gualtieri ดำรงตำแหน่งนายอำเภอของเมือง Pinellas ในขณะนั้น อย่างไรก็ตาม นายอำเภอได้เพิ่มเติมว่าในกรณีที่น้ำปนเปื้อนก็จะมีระบบป้องกันเพิ่มเติมเพื่อไม่ให้น้ำที่ปนเปื้อนนี้เข้าถึงประชาชนได้ง่าย ๆ เช่นกัน (Peiser, 2021)

ซึ่งเป็นที่น่าตกใจว่า โครงสร้างพื้นฐานที่สำคัญในสหรัฐอเมริกาเสี่ยงต่อการถูกโจมตีทางไซเบอร์ โดยองค์กรด้านความมั่นคงปลอดภัยไซเบอร์และความปลอดภัยของโครงสร้างพื้นฐาน (Cybersecurity and Infrastructure Security Agency) เตือนว่าโครงสร้างพื้นฐาน เช่น น้ำและโรงไฟฟ้า บริการฉุกเฉิน และระบบขนส่ง ทำให้เป็นเป้าหมายที่น่าสนใจสำหรับมหาอำนาจต่างชาติที่พยายามทำอันตรายต่อผลประโยชน์ หรือตอบโต้ต่อการรับรู้ของสหรัฐอเมริกา

ผู้วิจัยสนใจว่า การใช้โปรแกรมเข้าถึงเครื่องคอมพิวเตอร์ในระยะไกลอย่าง TeamViewer นั้น หน่วยงานที่เกี่ยวข้องอาจตรวจสอบรายละเอียดทางเทคนิค เช่น อาชญากรไซ

เบอร์ ได้รับข้อมูลรับรองการเข้าสู่ระบบคอมพิวเตอร์ที่สามารถเข้าควบคุมระบบน้ำที่เป็นหน่วยงานโครงสร้างพื้นฐานด้านสาธารณูปโภคของประเทศได้อย่างไร ซึ่งการเข้าถึงระบบจำเป็นต้องมีการตั้งค่าและเข้ารหัสบนอุปกรณ์เท่านั้น เป็นไปได้หรือไม่อาจมีสาเหตุมาจากการไม่ระมัดระวังของคนในการใช้งานระบบคอมพิวเตอร์ดังกล่าว ทำให้เกิดช่องโหว่และเป็นช่องทางในการแฮกของอาชญากรไซเบอร์เพื่อเข้าถึงระบบและข้อมูลที่สำคัญ

2.2.4 สถานการณ์ภัยคุกคามทางไซเบอร์ในประเทศไทย

ปฏิเสธไม่ได้ว่า ปัจจุบันการโจมตีทางไซเบอร์ในประเทศไทยเกิดขึ้นจำนวนมากโดยเฉพาะในช่วงการแพร่ระบาดของโรคติดเชื้อไวรัสโคโรนา 2019 (COVID-19) ที่ผู้คนต้องปรับเปลี่ยนเป็นการทำงานจากที่บ้าน (Work from Home) โดยกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี มีสถิติตัวเลขการแจ้งความออนไลน์ผ่านเว็บไซต์องค์กรโดยสรุประยะเวลา 4 เดือนระหว่างวันที่ 1 มีนาคม ถึง 27 มิถุนายน พ.ศ. 2565 พบว่า มียอดสะสมสูงถึง 44,144 คดี คิดเป็นความเสียหายมากกว่า 3 พันล้านบาท

ตารางที่ 2 การแจ้งความออนไลน์ผ่านเว็บไซต์ www.thaipoliceonline.com

ประเภท	คดีออนไลน์ (1 มี.ค. – 27 มิ.ย. 2565) มี 44,144 เรื่อง
1. การหลอกลวงด้านการเงิน	1.1 หลอกให้ทำงานออนไลน์ 5,633 เรื่อง 1.2 หลอกให้กู้เงินแต่ไม่ได้เงิน 4,481 เรื่อง 1.3 ข่มขู่ให้เกิดความหวาดกลัว 3,266 เรื่อง 1.4 หลอกให้ลงทุนในรูปแบบต่างๆ 2,344 เรื่อง 1.5 หลอกให้รักแล้วลงทุน 1,443 เรื่อง 1.6 แชร์ลูกโซ่ 1,028 เรื่อง 1.7 หลอกให้รักและโอนเงิน 382 เรื่อง 1.8 หลอกลวงเกี่ยวกับเงินดิจิทัล 38 เรื่อง
2. การหลอกลวงจำหน่ายสินค้า	2.1 ซื้อสินค้าแต่ไม่ได้รับสินค้า 16,950 เรื่อง 2.2 ซื้อสินค้าแต่ได้ไม่ตรงตามที่โฆษณา 614 เรื่อง
3. ข่าวปลอม	211 เรื่อง
4. ล่วงละเมิดทางเพศ	78 เรื่อง
5. การพนันออนไลน์	428 เรื่อง

ที่มา : สำนักงานตำรวจแห่งชาติ, 2565

สรุปรูปแบบการหลอกลวงแบ่งออกเป็น 5 ประเภท คือ หลอกลวงด้านการเงิน หลอกลวงจำหน่ายสินค้าข่าวปลอม ล่วงละเมิดทางเพศ และการพนันออนไลน์ โดยประเภทที่มีคดีความมากที่สุดคือ การหลอกลวงด้านการเงิน โดยมีจำนวน 22,561 เรื่อง และลองลงมาคือ การหลอกลวงจำหน่ายสินค้า มีจำนวน 18,358 เรื่อง ทั้งนี้พบว่า สถิติการรับแจ้งคดีออนไลน์ในระหว่างเดือนมีนาคมจนถึงเดือนมิถุนายน เพิ่มขึ้นทุกเดือน โดยในเดือนมีนาคม มี 8,806 เรื่อง เดือนเมษายน มี 9,553 เรื่อง เดือนพฤษภาคม มี 12,719 เรื่อง และ 1-27 มิถุนายน มี 14,393 เรื่อง โดยจากการประมวลผลพบว่า เป็นคดีที่มีความเชื่อมโยงกันถึง 15,376 เรื่อง และไม่เชื่อมโยงกัน 28,768 เรื่อง

การโจมตีทางไซเบอร์ดังกล่าวเกิดขึ้นกับทั้งบุคคลธรรมดาและองค์กร ซึ่งแม้แต่องค์กรที่มีระบบความมั่นคงปลอดภัยสารสนเทศที่ดีในระดับหนึ่ง เช่น บริษัทจดทะเบียนในตลาดหลักทรัพย์ก็ยังถูกโจมตีได้ รวมไปถึงหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ หรือ Critical Infrastructure (CI) ที่มีทั้งหน่วยงานของรัฐ และองค์กรภาคเอกชน ตัวอย่างหน่วยงาน CI ยกตัวอย่าง เช่น โรงไฟฟ้า ผู้ให้บริการเครือข่ายโทรคมนาคม รถไฟฟ้าทั้งบนดินและใต้ดิน สนามบินทั้งในเมืองหลวงและหัวเมืองต่างๆ สถาบันการเงิน ธนาคารแห่งประเทศไทย ตลาดหลักทรัพย์ ตลอดจนหน่วยงานด้านสาธารณสุข ทั้งโรงพยาบาลของรัฐ เอกชน รวมถึงหน่วยงานรัฐในการให้บริการประชาชน เช่น กรมการปกครอง สำนักงานเขต สำนักงานที่ดิน ซึ่งหน่วยงานเหล่านี้ล้วนมีความสำคัญต่อการดำเนินชีวิตประจำวันของประชาชนทั้งสิ้น ซึ่งปัจจุบันการโจมตีทางไซเบอร์ในประเทศไทย ที่พบเจอได้บ่อย และ ค่อนข้างมีผลกระทบทางเศรษฐกิจสูง ยกตังอย่างได้ 2 กรณี ใหญ่ๆ ดังนี้

(1) การโจมตีในรูปแบบ Business Email Compromised Attack คือ การหลอกด้วยอีเมล ทำให้เหยื่อเข้าใจผิดว่าเป็นคู่ค้า โดยหลอกฝ่ายบัญชีหรือฝ่ายการเงินให้นำเสนอผู้บริหารทำการโอนเงินเข้าไปยังบัญชีของแฮกเกอร์โดยไม่รู้ตัว ซึ่งเป็นรูปแบบหนึ่งของการโจมตีแบบ Social Engineering นับเป็นความเสียหายสูงสุดในประเทศไทย โดยบริษัทจดทะเบียนในตลาดหลักทรัพย์ ดำเนินธุรกิจด้านพลังงานให้ข่าวยอมรับการสูญเสียทางการเงินให้กับแฮกเกอร์ราว 660 ล้านบาท และยังมีบริษัทในอุตสาหกรรมอื่นไม่ว่าจะเป็น ด้านการเงิน การนำเข้าส่งออก การประกันภัย ล้วนตกเป็นเหยื่อแฮกเกอร์มาแล้วทั้งสิ้นในตลอด 5 ปีที่ผ่านมา คิดเป็นความเสียหายทางการเงินต่อปีกว่าหนึ่งพันล้านบาท

(2) การโจมตีในรูปแบบ Ransomware Attack คือ คนร้ายจะใช้วิธีการปล่อยมัลแวร์หรือเจาะระบบองค์กรผ่านทางอินเทอร์เน็ต ทำให้ข้อมูลถูกเข้ารหัสจนเจ้าของข้อมูลหรือผู้ดูแลระบบไม่สามารถเข้าไปใช้งานข้อมูลได้ ก่อนจะนำมาสู่ขั้นตอนการเรียกค่าไถ่แลกกับรหัสปลดล็อก รวมถึงการใช้ประโยชน์จากข้อมูลที่ถูกแฮก ซึ่งวิธีการนี้เป็นขั้นตอนการกรรโชกทรัพย์ที่คนร้ายใช้มาอย่างต่อเนื่อง แต่ปัญหา Ransomware ในปัจจุบันมีการพัฒนาจากการเรียกค่าไถ่

แบบเดิม ๆ เพิ่มขึ้นเป็น 3 ขั้นตอน เรียกว่า “Triple Extortion Ransomware” โดยในขั้นที่ 1 แฮกเกอร์มักจะเรียกค่าไถ่ด้วยข้อเสนอในการส่ง Decryption Key หรือกุญแจถอดรหัสในการกู้คืนข้อมูลให้เหยื่อ หากเหยื่อยังไม่ยอมจ่ายก็ไปต่อที่ขั้นที่ 2 โดยแฮกเกอร์จะนำข้อมูลไปโพสต์แล้วทำการเรียกค่าไถ่ให้จ่ายเพื่อลบข้อมูลออกจากการ Publish ใน Dark Web หรือ Public Web และหากเหยื่อยังไม่ยอมจ่ายอีก แฮกเกอร์ก็จะดำเนินการในขั้นที่ 3 คือ ปล่อยข้อมูลส่วนบุคคลของลูกค้าต่อสาธารณะ จากนั้นเมื่อข้อมูลลูกค้ารั่วไหลออกไปแล้ว เหยื่ออาจถูกลูกค้าฟ้องร้องเพราะ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลมีผลบังคับใช้แล้ว นับตั้งแต่วันที่ 1 มิถุนายน 2565 ซึ่งทั้ง 3 ขั้นตอนที่กล่าวมานี้เป็นวิธีการที่แฮกเกอร์นิยมใช้ แต่แฮกเกอร์ได้คิดวิธีใหม่ๆ ในการเรียกค่าไถ่ที่ซับซ้อนและสร้างความเสียหายให้มากขึ้นจากมัลแวร์เรียกค่าไถ่ โดยมีแนวโน้มที่อาจจะขยายวงกว้างอย่างรวดเร็วนับจากปี 2022 นี้เป็นต้นไป

วิธีการใหม่ๆ ของแฮกเกอร์ ยกตัวอย่าง เช่น ข่มขู่ว่าจะถล่มด้วย DDoS Attack ถ้าเหยื่อยังไม่ยอมจ่ายเงินเรียกค่าไถ่ ซึ่งอาจจะโจมตีจนทำให้เว็บไซต์ของเหยื่อล่มไม่สามารถใช้งานได้ หรือขู่ว่าจะติดต่อไปหาเจ้าของข้อมูลส่วนบุคคลเป็นรายบุคคลซึ่งเกิดขึ้นแล้วในต่างประเทศ แฮกเกอร์ได้นำข้อมูลผู้ป่วยที่แฮกมาจากโรงพยาบาล ติดต่อไปยังผู้ป่วยแต่ละรายเพื่อข่มขู่ หรือแฮกเกอร์อาจขายข้อมูลให้แฮกเกอร์รายอื่นๆ ซึ่งข้อมูลที่แฮกเกอร์ที่รับซื้อได้ไปนั้น ก็จะนำไปหลอกเหยื่อโดยการส่งอีเมลหรือ SMS ไปยังเจ้าของข้อมูลส่วนบุคคลแต่ละราย ทั้งสองกรณีหลังนี้ เจ้าของข้อมูลส่วนบุคคลสามารถจะร้องเรียนดำเนินคดีองค์กรที่เก็บข้อมูลของเหยื่อ จากข้อหากระทำข้อมูลรั่วไหลโดยขาดความระมัดระวังที่เหมาะสม

หลายปีที่ผ่านมา บริษัทจดทะเบียนในตลาดหลักทรัพย์และหน่วยงานโครงสร้างพื้นฐานในประเทศไทย ได้รับความเสียหายกว่าหนึ่งพันล้านบาทจากการที่องค์กรไม่สามารถดำเนินธุรกิจและธุรกรรมได้อย่างต่อเนื่อง ต้องเสียเวลาในการกู้ข้อมูล และสร้างระบบขึ้นมาใหม่ อุตสาหกรรมที่เกิดความเสียหายชัดเจน ได้แก่ ธุรกิจผลิตส่งออกและนำเข้า โรงพยาบาลทั้งรัฐและเอกชน สายการบิน โรงงานอุตสาหกรรม รวมถึง หน่วยงานรัฐและรัฐวิสาหกิจที่เป็นหน่วยงานโครงสร้างพื้นฐานที่สำคัญของประเทศ ปัญหาที่อาจเกิดขึ้นกับประชาชนในอนาคตอันใกล้ และเคยเกิดมาแล้วก็คือ ปัญหาหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศดังที่กล่าวมาแล้ว ระบบคอมพิวเตอร์ล่มใช้งานไม่ได้ หรือ ปัญหาระบบสารสนเทศถูกแฮกเกอร์เจาะเข้ามาขโมยข้อมูลหรือทำลายข้อมูล ทำให้ระบบหยุดชะงัก ไม่สามารถให้บริการประชาชนได้ ทำให้เกิดผลกระทบต่อประชาชน เมื่อพิจารณาให้ละเอียดพบว่า ระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญดังกล่าว ล้วนทำงานด้วยระบบคอมพิวเตอร์อยู่เบื้องหลัง ซึ่งภัยคุกคามไซเบอร์ที่บทเรียนสำหรับประเทศไทย ตัวอย่างสถานการณ์ภัยคุกคามไซเบอร์ในประเทศไทยเห็นได้ชัดเจนจากเหตุการณ์ล่าสุดของการโจมตีโรงพยาบาลสระบุรีที่ถูกไวรัสเรียกค่าไถ่กว่า 6 หมื่นล้านบาท จากการสอบเบื้องต้นพบว่า เป็นมัลแวร์จากยุโรปทำให้เกิดสถานการณ์วุ่นวายในโรงพยาบาล ไม่ว่าจะเป็นข้อมูลของผู้ป่วย ระบบการสั่งยา ระบบการ

จ่ายค่ารักษาพยาบาล (ทีเอ็นเอ็น, 2563) กรณีระบบสารสนเทศของโรงพยาบาลถูกไวรัสโจมตีเรียกค่าไถ่ชื่อ Voidcrypt/Spade ทำให้ระบบการจัดการและรักษาพยาบาล รวมถึงข้อมูลระบบสนับสนุนบริการทั้งหมดได้รับความเสียหาย และโรงพยาบาลไม่สามารถเข้าถึงข้อมูลได้ ซึ่งส่งผลกระทบต่อประชาชน ทำให้ได้รับบริการล่าช้า และข้อมูลการรักษาพยาบาลเดิมไม่สามารถใช้งานได้ในระยะหนึ่ง จากเหตุการณ์ดังกล่าว แม้ทางโรงพยาบาลสระบุรีมีการสำรองข้อมูลสม่ำเสมอ แต่เนื่องจากการโจมตีฐานข้อมูลได้กระทำอย่างรวดเร็ว และกระทำในระหว่างการสำรองข้อมูล ซึ่งไม่สามารถป้อนกันฐานข้อมูลไว้ได้ สำหรับการบุกรุกโจมตีฐานข้อมูลในครั้งนี้ ส่งผลกระทบต่อโรงพยาบาลเครือข่ายโรงพยาบาลชุมชนใน จ.สระบุรีด้วยเช่นกัน และอาจกระทบต่อการรักษาพยาบาลผู้ป่วยที่เป็นผู้ป่วยเดิมกับทางโรงพยาบาล ซึ่งประวัติการรักษาสูญหายไป ทางโรงพยาบาลมีความกังวลด้านการจ่ายยาให้แก่ผู้ป่วย ซึ่งทางกองบังคับการปราบปรามการการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) ได้จัดส่งกำลังเจ้าหน้าที่ เร่งแก้ไขให้ระบบฐานข้อมูลต่างๆ ให้กลับมาใช้ได้ปกติ (ผู้จัดการออนไลน์, 2563)

ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในประเทศไทย มีทั้งกรณีที่อยู่ในระดับไม่ร้ายแรง คือทำให้หน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศหรือการให้บริการของรัฐด้อยประสิทธิภาพ และกรณีที่อยู่ในระดับร้ายแรง คือ การโจมตีระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์ ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและการสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหาย จนไม่สามารถทำงานหรือให้บริการได้ ภัยคุกคามทางไซเบอร์ได้เพิ่มระดับความรุนแรง และมีความซับซ้อนในการโจมตีมากขึ้น ความเสียหายที่เกิดจากการอาชญากรรมและการโจมตีทางไซเบอร์จะมีผลต่อธุรกิจอย่างร้ายแรง ซึ่งในทุกองค์กรทั้งภาครัฐ และภาคเอกชน จะต้องตระหนักและต้องมีการกำหนดมาตรการในการป้องกันภัยคุกคามทางไซเบอร์ดังกล่าว แม้ว่าในบางองค์กรนั้นอาจจะยังไม่เคยถูกโจมตีทางไซเบอร์มาก่อนก็ตาม แต่ในองค์กรส่วนใหญ่ล้วนให้ความสำคัญกับการป้องกันภัยคุกคามทางไซเบอร์ โดยมีการวางแนวทางป้องกันภัยคุกคามทางไซเบอร์ มีการปรับเปลี่ยนมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ ให้สอดรับกับการเปลี่ยนแปลงยุทธศาสตร์และการดำเนินการทางธุรกิจ และเพื่อให้สอดคล้องกับการเปลี่ยนแปลงทางสภาพแวดล้อมภายนอกของธุรกิจซึ่งผู้บริหารต้องมองลักษณะของภัยคุกคามทางไซเบอร์ให้รอบด้าน

อย่างไรก็ตาม แม้ว่าภัยคุกคามและการโจมตีทางไซเบอร์ในประเทศไทย ยังไม่เข้าสู่ระดับวิกฤติหรือเป็นการก่อการร้ายตามประมวลกฎหมายอาญา แต่ผู้วิจัยสนใจว่า ปัญหา “Cyber Attack” ไม่ใช่การแก้ปัญหาทางด้านเทคนิคเพียงอย่างเดียว หากแต่การแก้ปัญหาทางด้านเทคนิคก็เป็นเรื่องสำคัญที่เราจะมองข้ามไม่ได้ ซึ่งในภาพรวมนั้นหน่วยงานต้องให้ความสำคัญกับ 3 ด้าน คือ People Process Technology และไม่ว่าจะเป็นเรื่องนโยบาย กลยุทธ์ กฎหมาย เศรษฐกิจ

และสังคม การศึกษาเพื่อการฝึกอบรมบุคลากรในระดับองค์กร ก็เป็นองค์ประกอบที่ควรให้ความสำคัญด้วยเช่นกัน

2.3 ทฤษฎีอาชญาวิทยาและภัยคุกคามทางไซเบอร์

2.3.1 ทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory)

หากมองสาเหตุของการเกิดอาชญากรรมจากทฤษฎีสามเหลี่ยมอาชญากรรม (The Crime Triangle) จะมีเพียง 3 องค์ประกอบอาชญากรรม คือ

(1) ผู้กระทำผิดหรือคนร้าย (criminals) หมายถึง ผู้ที่มีความต้องการ (desire) จะก่อเหตุลงมือกระทำผิด

(2) เหยื่อ (victims) หรือเป้าหมาย (target) หมายถึง บุคคล สถานที่ หรือวัตถุที่ผู้กระทำผิดหรือคนร้าย มุ่งหมาย กระทำต่อ หรือเป็นเป้าหมายที่ต้องการ

(3) โอกาส (opportunity) หมายถึง ช่วงเวลา (time) และสถานที่ (place) ที่เหมาะสมที่ผู้กระทำผิดหรือคนร้าย มีความสามารถจะลงมือกระทำผิดหรือก่ออาชญากรรม

โดยเมื่อเหตุการณ์หรือสถานการณ์ครบองค์ประกอบทั้ง 3 ด้านดังกล่าวข้างต้นจะทำให้เกิดอาชญากรรมขึ้น ทฤษฎีดังกล่าวได้เสนอแนวคิดในการแก้ไขปัญหาอาชญากรรมหรือการป้องกันไม่ให้เกิดอาชญากรรม โดยต้องพยายามหาวิธีการว่าทำอย่างไรที่จะให้องค์ประกอบของสามเหลี่ยมอาชญากรรม ด้านใด ด้านหนึ่งหายไป ก็จะทำให้อาชญากรรมไม่เกิดขึ้น

ภาพที่ 3 ทฤษฎีสามเหลี่ยมอาชญากรรม

หากพิจารณาถึงปัจจัยที่ทำให้เกิดภัยคุกคามทางไซเบอร์และอาชญากรรมไซเบอร์ ซึ่งอธิบายถึงสาเหตุและองค์ประกอบการเกิดอาชญากรรมมี 3 ด้านดังที่กล่าวมา ในหนังสือของ

George W. Reynolds (2012) เรื่อง Ethics in Information Technology ได้จำแนกออกเป็น 3 ประเด็น คือ

(1) ผู้ใช้งานคอมพิวเตอร์มีความคาดหวังต่อการใช้คอมพิวเตอร์สูงมากขึ้น เนื่องจากปัจจุบัน เวลานั้นเป็นเงินเป็นทอง คอมพิวเตอร์มีความเร็วมากขึ้น ผู้ใช้สามารถแก้ปัญหาเองได้ ในอนาคต ผู้ใช้สามารถที่จะผลิตได้เอง คนทำงานคอมพิวเตอร์ที่แผนกช่วยเหลือ (Help Desks) ต้องตกอยู่ภายใต้แรงกดดันในการที่จะทำให้คำตอบจากผู้ใช้ที่ร้องขอข้อมูลเข้ามาอย่างรวดเร็ว จากภายใต้แรงกดดันที่ว่านี้ บางครั้งพนักงานคอมพิวเตอร์ที่แผนกช่วยเหลือ ลืมตรวจสอบไอดีของผู้ใช้ หรือลืมตรวจสอบการอนุญาตสิทธิ์การใช้รหัสผ่าน และผู้ใช้คอมพิวเตอร์บางคน ได้แชร์ไอดีการเข้าระบบและรหัสผ่าน (Login ID and Password) ทำให้ผู้ไม่ประสงค์ดีนำรหัสผ่านเหล่านั้นไปใช้ในการแสวงหาผลประโยชน์ในทางที่มิชอบ โดยเฉพาะผลประโยชน์ทางด้านการเงิน

(2) สิ่งแวดล้อมทางคอมพิวเตอร์มีความซับซ้อนมากขึ้น กล่าวคือ สิ่งแวดล้อมทางคอมพิวเตอร์มีความซับซ้อนขึ้นอย่างมากมาย ได้แก่ เครื่องคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ การปฏิบัติการ ระบบ การประยุกต์ใช้เว็บไซต์ สวิตช์ เราเตอร์ และเกตเวย์ ที่เชื่อมต่อกัน และมีแรงผลักดันจากหลายร้อยล้านเส้นทางของรหัสการเขียนโปรแกรม สิ่งแวดล้อมของความซับซ้อนทางคอมพิวเตอร์เหล่านี้ ยังคงมีเพิ่มมากขึ้นอย่างต่อเนื่องทุกวัน จำนวนตัวเลขของเครือข่ายคอมพิวเตอร์ที่เชื่อมต่อเข้ามายังมีการขยายตัวเพิ่มมากขึ้นอย่างต่อเนื่อง อาทิเช่น การเชื่อมต่อจากอุปกรณ์ต่างๆ อย่างมากมาย ไม่ว่าจะเป็นคอมพิวเตอร์ส่วนบุคคล (Personal Computer: PC) แท็บเล็ต สมาร์ทโฟน เป็นต้น ในขณะเดียวกัน ก็มีการละเมิดความปลอดภัยทางด้านคอมพิวเตอร์อย่างต่อเนื่องด้วยเช่นกัน นอกจากนี้ องค์กรและพนักงานเป็นจำนวนมากหันมาใช้คอมพิวเตอร์การประมวลผลแบบกลุ่มเม (Cloud computing) ในการทำงานและใช้ในการจัดเก็บข้อมูลการให้บริการผ่านอินเตอร์เน็ต เช่น Google Drive, One Drive, Drop Box, Amazon Cloud เป็นต้น และซอฟต์แวร์เสมือนจริงเช่นเดียวกัน ซอฟต์แวร์เสมือนจริงเป็นซอฟต์แวร์ที่เลียนแบบการทำงานของคอมพิวเตอร์ฮาร์ดแวร์ โดยสามารถปฏิบัติการได้หลายระบบที่ทำงานอยู่บนคอมพิวเตอร์แม่ข่ายที่เดียว ด้วยสถานการณ์ดังกล่าวนี้ ทำให้ยากต่อการควบคุมความมั่นคงปลอดภัย

(3) การขยายตัวและการเปลี่ยนแปลงของระบบเครือข่ายคอมพิวเตอร์เท่ากับความเสี่ยงใหม่ ธุรกิจได้เคลื่อนย้ายจากยุคของการใช้เครื่องคอมพิวเตอร์ทำงานเพียงเครื่องเดียว ซึ่งมีการเก็บข้อมูลที่สำคัญไว้ในคอมพิวเตอร์เมนเฟรม (Mainframe) แยกไว้ในห้องจัดเก็บ จนต่อมาได้เข้าสู่ยุคที่คอมพิวเตอร์ส่วนบุคคลที่เชื่อมต่อกับเครือข่ายคอมพิวเตอร์อื่น ๆ ที่มีจำนวนนับล้านๆ เครื่อง และที่มีความสามารถในการใช้ข้อมูลร่วมกัน เรียกว่าเป็นยุคของเครือข่าย (Network Era) และคอมพิวเตอร์ที่เชื่อมต่อกันด้วยอินเตอร์เน็ตทั้งหมดเหล่านั้น สามารถแบ่งปันสารสนเทศร่วมกันได้ ไม่ว่าจะเป็นคอมพิวเตอร์ แท็บเล็ต หรือสมาร์ทโฟน ที่มีการใช้แพลตฟอร์มต่าง ๆ เช่น Facebook, Line, Twitter, YouTube หรือแม้กระทั่งแอปพลิเคชันทางด้านการเงินต่างๆ เช่น เป๋าตังค์ เป็นต้น ซึ่งการใช้งานอินเตอร์เน็ตและแอปพลิเคชันเหล่านี้ มีสถิติการใช้งานเพิ่มมากขึ้นอย่างก้าวกระโดด เมื่อกล่าวถึงเรื่องของเทคโนโลยีดิจิทัล ซึ่งในปัจจุบันสามารถพบเห็นได้โดยทั่วไป ทุกคนต่างยอมรับว่า เทคโนโลยีสารดิจิทัลถือว่าเป็นเครื่องมืออันทรงพลังอย่างหนึ่ง ที่มีส่วนช่วยผลักพันทำให้องค์กรประสบความสำเร็จตามเป้าหมายที่วางไว้ และด้วยความเจริญก้าวหน้าของเทคโนโลยีดิจิทัลนี่เอง ทำให้มีความยากเพิ่มขึ้นในการที่จะทำให้การเปลี่ยนแปลงเทคโนโลยีนำมาปรับให้เข้ากันได้

ผู้วิจัยสนใจว่า การนำทฤษฎีสามเหลี่ยมอาชญากรรมมาอธิบายการเกิดภัยคุกคามทางไซเบอร์จะทำให้มองภาพได้ชัดเจนมากขึ้น โดยเฉพาะเมื่อมนุษย์กำลังอยู่ในยุคดิจิทัลที่มาพร้อมกับการแพร่ระบาดของโรคโควิด-19 ยิ่งเป็นสิ่งเร้าทำให้เกิดการเปลี่ยนแปลงที่รวดเร็วยิ่งขึ้นและทำให้มนุษย์ต้องปรับเปลี่ยนพฤติกรรมอย่างที่เห็นได้ชัดคือ การเปลี่ยนรูปแบบการทำงานจากที่ทำงานเป็นที่บ้านหรือ Work from home ทำให้หลายองค์กรต้องมีการเตรียมความพร้อมในการปฏิบัติงานของพนักงานเพื่อให้สามารถเข้าถึงข้อมูลและนำไปใช้งานได้อย่างปกติ และจำเป็นต้องมีวิธีการป้องกันความมั่นคงปลอดภัยในการใช้อินเตอร์เน็ตให้ดีเสียก่อน โดยเฉพาะการใช้จุดเชื่อมโยงสาธารณะ (Public Hotspot) เนื่องจากกิจกรรมการใช้อินเตอร์เน็ตเหล่านั้น อาจมีคนสอดแนม (Snooping) อยากรู้อยากเห็นความเคลื่อนไหวต่าง ๆ การใช้เครือข่ายเสมือนจริงส่วนบุคคล (Virtual Private Network: VPN) คือเส้นทางความปลอดภัยของอินเตอร์เน็ต หลายองค์กรใช้ VPN ในการป้องกันข้อมูลที่ไวต่อการสัมผัส เช่น การส่งข้อความรีบด่วน ข้อมูลบัตรเครดิต และกิจกรรมของเว็บบราว์เซอร์ ดังนั้น ปัจจุบันจึงมีเกราะป้องกันที่จุดเชื่อมโยงและเพิ่มระดับการป้องกันความมั่นคงปลอดภัยไซเบอร์ให้กับองค์กร

2.3.2 ทฤษฎีการกระทำที่เป็นกิจวัตร (Routine Activity Theory)

ทฤษฎีการกระทำที่เป็นกิจวัตร เสนอครั้งแรกโดย โคเฮนและเฟลสัน (Lawrence E. Cohen and Marcus Felson, 1979) อธิบายเชิงลึกไปที่โอกาสอาชญากรรม (Crime Opportunity) ในสถานการณ์ที่หลอมรวมกันพอดีของพื้นที่และเวลา (Space and Time) เมื่อเหยื่อมีพฤติกรรมที่เป็นกิจวัตร เช่น กินอาหารร้านเดิมเป็นประจำ เดินทางไปทำงานเส้นทางเปลี่ยวเป็นประจำ เปิดหน้าต่างห้องนอนเป็นประจำ ไม่ล็อคประตูหอพักเป็นประจำ สวมเครื่องประดับราคาแพงเป็นประจำ โดยมีองค์ประกอบ 3 ประการที่เป็นเหตุทำให้เกิดอาชญากรรม ได้แก่

(1) เป้าหมายที่เหมาะสม (Suitable Target) โดยเงื่อนไขประการแรกของการเกิดอาชญากรรม คือ เหยื่อหรือเป้าหมายที่เหมาะสม แบ่งออกเป็น 3 ประเภท คือ คน สิ่งของ และสถานที่ ซึ่งอะไรก็ตามที่เคยเป็นเหยื่อหรือเป้าหมายแล้ว ก็สามารถกลับไปเป็นเหยื่อหรือเป้าหมายได้อีก เช่น เหยื่อ Romance Scam ที่มีทรัพย์สิน สูงวัย เชื่อคนง่าย ขาดประสบการณ์ ขาดความรักความอบอุ่น หรือเหยื่อใช้ชีวิตเพียงลำพัง เป็นต้น

(2) การขาดผู้ดูแลสถานที่นั้นๆ (Absence of a Capable Guardian) โดยมีเงื่อนไข คือ ผู้ดูแลไม่อยู่หรือมีอยู่แต่ไม่มีประสิทธิภาพ ไม่สามารถยับยั้งการเกิดอาชญากรรมได้ จึงจำเป็นต้องมีผู้ดูแลที่คอยสอดส่องรักษาความสงบเรียบร้อย เช่น ตำรวจ ผู้ปกครอง เพื่อนบ้าน คนเฝ้าประตูหรือกล้องวงจรปิด เป็นต้น

(3) แรงจูงใจอาชญากร หรือบุคคลที่มีแนวโน้มหรือแรงจูงใจที่จะก่อให้เกิดการกระทำผิด (Likely and Motivated Offenders) โดยมีเงื่อนไข คือ ตัวผู้กระทำผิดซึ่งคิดว่าเหยื่อหรือเป้าหมายที่มีความเหมาะสมขาดการดูแลปกป้อง อาชญากรเห็นโอกาสจึงตัดสินใจกระทำผิดหรือก่ออาชญากรรม เช่น เห็นพฤติกรรมเหยื่อผ่านโซเชียลมีเดีย สถานที่ เวลา ที่อาชญากรเห็นช่องโหว่หรือโอกาสที่จะบุกรุกเข้าไป หรือหาอรรถประโยชน์จากเหยื่อได้ตลอดเวลา

ภาพที่ 4 องค์ประกอบของการกระทำผิดตามทฤษฎีกิจวัตรประจำวัน

จากสาเหตุและปัจจัยการตกเป็นเหยื่อภัยคุกคามทางไซเบอร์และแนวคิดทฤษฎีกิจวัตรประจำวัน ดังกล่าวข้างต้น ผู้วิจัยนำมาใช้อธิบายสถานการณ์และวิเคราะห์ถึงสาเหตุของการเกิดอาชญากรรมไซเบอร์ได้ว่า พฤติกรรมของคนจำนวนมากในการใช้งานคอมพิวเตอร์หรืออินเตอร์เน็ตในการรับ-ส่งข้อมูลระหว่างคอมพิวเตอร์กับอุปกรณ์อิเล็กทรอนิกส์ หรือระหว่างบุคคลกับบุคคล หรือระหว่างคอมพิวเตอร์กับบุคคล ซึ่งไม่ค่อยตรวจเช็คความปลอดภัยของไฟล์ข้อมูลให้รอบคอบก่อนที่จะเปิด หรือดาวน์โหลดมาใช้งานบนเครื่องคอมพิวเตอร์ หรืออุปกรณ์ดิจิทัลของตนเอง หรือผู้ที่มักเข้าใช้งานเว็บไซต์จากแหล่งที่ไม่น่าเชื่อถืออยู่เป็นประจำ โดยเฉพาะอย่างยิ่งเว็บไซต์ภาพหรือวิดีโอลามกก็มักนำไปสู่การตกเป็นเหยื่อของโปรแกรมอันตราย (Malicious software) ที่ถูกติดตั้งหรือเผยแพร่ไว้โดยอาชญากรคอมพิวเตอร์ด้วย

2.3.3 ทฤษฎีการเลือกอย่างเป็นเหตุเป็นผล (Rational Choice Theory)

หากพิจารณาการเข้าถึงข้อมูลทางอินเตอร์เน็ตโดยมิชอบที่กลายเป็นปัญหาภัยคุกคามทางไซเบอร์ สามารถแบ่งออกเป็น 3 ส่วน กล่าวคือ

1) หน่วยงานภาครัฐ พบว่า มีมาตรการป้องกันปัญหานี้ยังไม่ดีพอเนื่องด้วยข้อจำกัดเรื่องงบประมาณและกำลังคน ขาดผู้เชี่ยวชาญที่มีความรู้ความสามารถเฉพาะด้าน และไม่มีงบประมาณด้านการเงินที่เพียงพอในการจัดซื้อเครื่องมือหรืออุปกรณ์ป้องกันที่ทันสมัย ทั้งนี้ หากมี

ระบบรักษาความปลอดภัยหรือป้องกันการเข้าถึงระบบข้อมูลเครือข่ายทางอินเตอร์เน็ตที่ดีและมีประสิทธิภาพ จะเป็นการปิดโอกาสหรือปิดช่องทางไม่ให้อาชญากรไซเบอร์กระทำการนั้นได้

2) องค์กร พบว่า หน่วยงานหรือองค์กรต่างๆส่วนใหญ่จะมีมาตรการรักษาความปลอดภัยไว้เป็นอย่างดี เพราะถือว่าความปลอดภัยของข้อมูลเป็นเรื่องสำคัญมาก เพื่อเป็นการป้องกันความเสียหายของธุรกิจและสร้างความเชื่อมั่นทางด้านความปลอดภัยข้อมูลของผู้ใช้บริการเพื่อให้เกิดความเชื่อมั่นว่า ข้อมูลของตนจะไม่ถูกโจรกรรมไปได้จากผู้ไม่หวังดี นำไปก่อความเสียหาย เป็นการสร้างความน่าเชื่อถือให้กับผู้ให้บริการเองด้วยว่า มีระบบป้องกันการเข้าถึงข้อมูลได้อย่างแน่นหนายากต่อการถูกโจมตี หรือเจาะข้อมูลได้ ระบบรักษาความปลอดภัยในเรื่องป้องกันการเข้าถึงข้อมูลทางอินเตอร์เน็ตขององค์กร แต่ยังมีองค์กรหรือหน่วยงานบางแห่งที่ยังมีมาตรการป้องกันปัญหานี้ไม่ดีเพียงพอ ยังขาดแนวคิดและการปฏิบัติที่ควรคำนึงถึงปัญหาด้านความมั่นคงปลอดภัยตั้งแต่ขั้นตอนแรกในการวางระบบ ซึ่งหมายถึง ควรมีการวางระบบรักษาความมั่นคงปลอดภัยหรือมาตรการที่เกี่ยวข้องตั้งแต่ต้นว่าจะมีระบบป้องกันอย่างไร และบริการต่างๆขององค์กรตลอดจนการออกแบบฮาร์ดแวร์และซอฟท์แวร์ ที่จะออกมาสู่ผู้ใช้งานหรือลูกค้า นอกจากนี้ ต้องมีการตรวจสอบ วิเคราะห์ประเมินความเสี่ยงหรือโอกาสที่จะเกิดปัญหาและได้รับการรับรองมาตรฐานความปลอดภัยจากองค์กรที่ได้รับความเชื่อถือ (Analysis Risk and Security Certification) รวมถึงผู้ปฏิบัติหน้าที่หรือผู้ปฏิบัติงานจะต้องปฏิบัติตามกฎระเบียบการใช้งานอย่างเคร่งครัด หมั่นตรวจสอบเครื่องมืออย่างสม่ำเสมอ ไม่ปล่อยให้เป็นช่องทางให้เกิดโอกาสของคนร้าย

3) ผู้ใช้งาน พบว่า ผู้ใช้งานยังไม่ตระหนักถึงปัญหาภัยคุกคามทางไซเบอร์และการป้องกันยังไม่ดีพอ ไม่มีการติดตั้งซอฟต์แวร์ป้องกันหรือโปรแกรมแอนติมัลแวร์ ติดตั้งโปรแกรมที่ไม่ถูกกฎหมาย ไม่ทันสมัย ทำให้เกิดปัญหานี้ตามมามากมาย

ซึ่งสอดคล้องกับแนวคิด ทฤษฎีเหตุผลในการเลือกประกอบอาชญากรรม (Rational Choice Theory : Marcus Felson , Ronald v. Clark,1993) ทฤษฎีนี้ได้อธิบายถึงลักษณะของการเกิดอาชญากรรม โดยเน้นไปที่สาเหตุของการเกิดอาชญากรรม (Root Cause) หรือโอกาสในการเกิดอาชญากรรมซึ่งกล่าวถึงพฤติกรรมบุคคลของผู้กระทำผิดว่า เป็นผลผลิตจากการเปลี่ยนแปลงทางด้านสังคมและเทคโนโลยีที่รวดเร็ว การติดต่อสัมพันธ์ระหว่างบุคคลในสังคมของตนที่เข้าถึงง่าย โดยให้ความสำคัญกับผู้ก่ออาชญากรรมที่มีพื้นฐานทางการศึกษาค่อนข้างดี มีความรู้ ได้ใช้โอกาสทางสังคมในการกระทำความผิด และยังได้กล่าวถึงการป้องกันอาชญากรรมว่าต้องปิดกั้นโอกาส หรือช่องทางการก่ออาชญากรรม สามารถลดปัญหาอาชญากรรมเหล่านั้นได้ สามารถนำมาอธิบายประเด็นนี้ได้ว่า ผู้ที่มีความรู้ความเชี่ยวชาญด้านคอมพิวเตอร์ ได้ใช้ความรู้ความมสามารถของตนเองสร้างโอกาสในการกระทำผิด ยกตัวอย่างเช่น สร้างโปรแกรมมัลแวร์เจาะระบบข้อมูลทางอินเตอร์เน็ตของผู้ใช้งาน

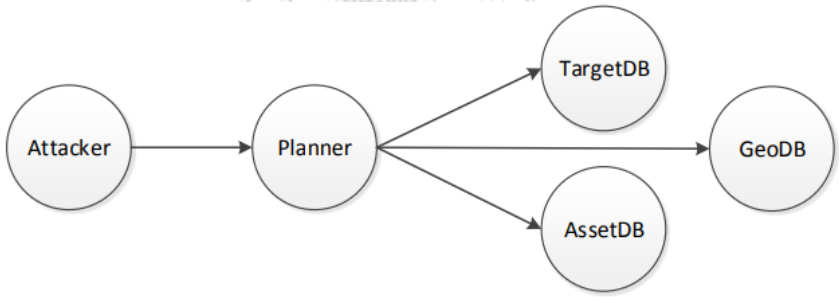
หรือหน่วยงาน องค์กรต่างๆที่มีการป้องกันหรือระบบรักษาความปลอดภัยข้อมูลไม่ดีพอ กลายเป็นช่องทางหรือโอกาสให้คนร้าย เป็นต้น ซึ่งหน่วยงานหรือองค์กรที่เกี่ยวข้องจะต้องป้องกันหรือปิดกั้นโอกาสของคนร้ายเหล่านี้ โดยการสร้างระบบรักษาความปลอดภัยให้กับสังคมผู้ใช้งานทางอินเตอร์เน็ตหรือไซเบอร์ เช่นมาตรการทางเทคนิคและมาตรการทางกฎหมาย สร้างกฎระเบียบปฏิบัติ ให้ทันกับความก้าวหน้าทางเทคโนโลยี และยังสอดคล้องกับงานวิจัยของ เบญจรัตน์ ธารารักษ์ (2551) ซึ่งศึกษาเกี่ยวกับความรู้และความเข้าใจพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของบุคลากรในสำนักงานมหาวิทยาลัยเชียงใหม่ พบว่า บุคลากรในสำนักงานฯ มีความรู้ความเข้าใจพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ฯ อยู่ในระดับน้อย และพบว่าเงื่อนไขในการควบคุมและป้องกันการกระทำผิดตาม พ.ร.บ. ฉบับนี้อยู่ในระดับน้อยเช่นเดียวกัน เนื่องด้วยบุคลากรในหน่วยงานหรือผู้ใช้งานอินเตอร์เน็ตในองค์กร ยังไม่ตระหนักหรือรับรู้ถึงความผิดที่เกี่ยวกับคอมพิวเตอร์ได้ดีเท่าที่ควร ทั้งๆที่มีส่วนเกี่ยวข้องในกิจวัตรหรืองานที่ตนได้รับมอบหมายหรือทำอยู่ ซึ่งเป็นความเสี่ยงต่อความเสียหายที่อาจเกิดขึ้นหากมีผู้กระทำผิดที่เกี่ยวกับคอมพิวเตอร์ทำการเจาะระบบข้อมูลเข้ามาก่อความเสียหายให้แก่องค์กร อาจทำให้บุคคลในองค์กรนั้นปล่อยปละละเลยไม่สนใจกับปัญหาที่เกิดขึ้น และไม่ใส่ใจที่จะหาคนผิดมารับโทษตามกฎหมาย จะทำให้มาตรการป้องกันปัญหานี้ไม่มีประสิทธิภาพ

จากการกระทำผิดในปัจจุบันเห็นว่า มีช่องทางและวิธีการในการก่อเหตุที่หลากหลายและแยบยล จากพัฒนาการของเทคโนโลยีที่ล้ำสมัย และเห็นว่าประโยชน์ที่ได้รับจากการประกอบอาชญากรรมมีความคุ้มค่ามากยิ่งกว่าโทษที่จะได้รับ อีกทั้ง ภัยคุกคามทางไซเบอร์ยังคงเป็นปัญหาเรื้อรังของสังคมที่ไม่มีวันสิ้นสุด ตราบใดที่ความก้าวหน้าทางเทคโนโลยียังมีช่องโหว่ให้ผู้ไม่ประสงค์ดีนำมาใช้ในการกระทำความผิดได้อย่างต่อเนื่อง และไม่ได้รับการเข้มงวดในบทลงโทษด้านกฎหมายอย่างจริงจัง และมีผลต่อการออกนโยบายและกฎหมายใหม่ที่ครอบคลุมและป้องกันโอกาสและช่องทางในการกระทำผิด และการคิดที่จะกระทำผิดได้

2.3.4 ทฤษฎีการโจมตีทางไซเบอร์ (Cyber Attack Theory)

ความสำเร็จในการโจมตีทางไซเบอร์ขึ้นอยู่กับข้อมูลที่ผู้โจมตีต้องการครอบครอง โดยเมื่อเปิดการโจมตี ผู้โจมตีจะวัดผลจากข้อมูลที่ได้รับหรือแก้ไขอันเป็นผลมาจากการโจมตี ดังนั้น ข้อมูลจึงเป็นองค์ประกอบที่สำคัญของทฤษฎีการโจมตีทางไซเบอร์ อย่างไรก็ตาม ข้อมูลที่น่าสนใจสำหรับผู้โจมตีเป็นมากกว่าข้อมูลการกำหนดค่าทั่วไป ตัวอย่างเช่น สถานะและข้อมูลการดำเนินการของระบบเป้าหมายไม่ใช่ข้อมูลการปันส่วนที่เป็นค่าคงที่ทั่วไป แต่เป็นข้อมูลที่มีความสำคัญต่อการโจมตีหลายประเภทและเก็บข้อมูลทั้งหมดที่น่าสนใจไว้

Rui Zhuang, Alexandru G. Bardas, Scott A.Deloach และ Xinming Ou (2015) นักวิจัยจากมหาวิทยาลัย Kansas State Universtity ประเทศสหรัฐอเมริกา ได้อธิบายว่า ทฤษฎีการโจมตีทางไซเบอร์ ด้วยการวิเคราะห์การป้องกันเป้าหมายเคลื่อนที่ หรือ Moving Target Defenses (MTD) ได้รับการขนานนามว่าเป็นแนวทางการเปลี่ยนวิธีการรักษาความปลอดภัยคอมพิวเตอร์ที่ขจัดลักษณะคงที่ของระบบคอมพิวเตอร์ในปัจจุบัน อธิบายให้เข้าใจง่ายๆได้ว่า เป็นการเปลี่ยนแปลงระบบคอมพิวเตอร์อย่างต่อเนื่องเพื่อลดหรือย้ายพื้นผิวการโจมตีที่ใช้ประโยชน์ได้ ซึ่งเป็นทรัพยากรที่มีให้สำหรับผู้โจมตี เช่น ซอฟต์แวร์ พอร์ต องค์ประกอบของช่องโหว่ ฯลฯ ที่สามารถใช้เพื่อรับรองระบบจนถึงปัจจุบัน เทคนิค MTD อาจทำงานได้อย่างมีประสิทธิภาพในระบบจริงเมื่อเทียบกับการโจมตีบางประเภท ระบบ MTD ก่อให้เกิดความท้าทายใหม่ภายใต้สถานะและการวัดประสิทธิภาพของระบบดังกล่าว สิ่งที่น่าสนใจคือ ทฤษฎีที่ครอบคลุมของ MTD จะกำหนดว่าระบบ MTD คืออะไร ทำงานอย่างไร และโต้ตอบการโจมตีและผู้โจมตีเพื่อขัดขวางผู้ที่โจมตีอย่างไร ยกตัวอย่างการอธิบายด้วยสถานการณ์สร้างแรงจูงใจ หรือ Motivating Scenario ที่ทีมนักวิจัยได้รับการสนับสนุนจากสำนักงานวิจัยวิทยาศาสตร์กองทัพอากาศ และมูลนิธิวิทยาศาสตร์แห่งชาติจากสหรัฐอเมริกา เริ่มต้นด้วยระบบการวางแผนภารกิจทางทหารที่เรียบง่าย ซึ่งแสดงในภาพที่ 5



ภาพที่ 5 Motivating Attack Scenario

ในสถานการณ์สมมตินี้ ผู้ใช้ที่ได้รับอนุญาตจากระยะไกลได้เข้าถึงผู้วางแผนภารกิจเพื่อสร้าง Missions ประเภททหาร Planner (เว็บเซิร์ฟเวอร์ที่มีอินเทอร์เฟซผู้ใช้) และอนุญาตให้ผู้ใช้ดำเนินการที่ได้รับสิทธิในการเพิ่มกลยุทธ์ใหม่ การจัดทำแผน/ยุทธวิธี หรือการจัดสรรทรัพยากรใหม่เพื่อสนับสนุนการดำเนินการเหล่านี้ ผู้วางแผนจะเข้าถึงฐานข้อมูลที่เกี่ยวข้อง คือ AssetDB, GeoDB และ TargetDB ซึ่งผู้โจมตีพยายามหาช่องโหว่ในการวางแผน และถ้ามีช่องโหว่อยู่ ผู้โจมตีสามารถใช้ประโยชน์จากช่องโหว่นั้น (Zhuang, Bardas, A.Deloach และ Ou, 2015)

จากแนวคิดและทฤษฎีการโจมตีทางไซเบอร์และกรณีตัวอย่างการเกิดภัยคุกคามทางไซเบอร์ในประเทศต่าง ๆ นั้นกล่าวได้ว่า

(1) การโจมตีไซเบอร์มีความสลับซับซ้อนในการตัดสินใจเกี่ยวกับวิธีการรับมือกับการโจมตีดังกล่าวเช่น ภัยคุกคามไซเบอร์ต้องรุนแรงเพียงใดถึงจะต้องอาศัยการรับมือในระดับของกองทัพ (Military response) หรือการเผยแพร่ข้อมูลที่บิดเบือน (Disinformation) ในบางประเด็นในพื้นที่ไซเบอร์จัดว่าเป็นภัยคุกคามต่อรัฐหรือไม่ เป็นต้น สภาวการณ์เช่นนี้เอื้อให้เกิดการตัดสินใจเชิงยุทธศาสตร์ที่ผิดพลาดและทำให้การรับมือกับภัยคุกคามไม่มีประสิทธิภาพ วิธีการสำคัญที่จะจัดการกับความท้าทายนี้คือการวิเคราะห์สภาพการณ์ความเสี่ยง โอกาสและความท้าทายทางไซเบอร์ของประเทศในปัจจุบัน โดยวิเคราะห์ความพร้อมและจุดอ่อนของระบบและโครงสร้างพื้นฐานไซเบอร์ ศึกษาแนวโน้มของความเสี่ยงไซเบอร์อันเกิดจากความก้าวหน้าของการพัฒนาเทคโนโลยีและพิจารณาถึงเวกเตอร์การโจมตี (Attack vector) ใหม่ ๆ การวิเคราะห์สภาพการณ์ควรดำเนินควบคู่ไปกับการวิเคราะห์ฉากทัศน์เพื่อเสนอภาพความเป็นไปได้ต่าง ๆ ที่เกี่ยวข้องกับการโจมตีไซเบอร์ที่รัฐอาจเผชิญและระดมสมองเพื่อหาแนวทางในการรับมือกับแต่ละฉากของความเป็นไปได้ ผลที่ได้จากการวิเคราะห์สภาพการณ์และวิเคราะห์ฉากทัศน์คือการออกแบบระบบเตือนภัยและเตรียมพร้อมรับมือกับความเสี่ยงไซเบอร์ซึ่งต้องเป็นกระบวนการที่ปฏิบัติซ้ำได้ (Repeatable processes) (Swedberg, 2018) ทั้งนี้ระบบดังกล่าวจะต้องคำนึงถึงการรักษาความต่อเนื่องของการใช้พื้นที่ไซเบอร์ภายใต้ชุดของเงื่อนไขและสถานการณ์ต่าง ๆ ดังนั้นเมื่อมีการออกแบบระบบแล้ว จะต้องมีการทดสอบระบบผ่านการซ้อมปฏิบัติการทางไซเบอร์

(2) ความมั่นคงไซเบอร์มีทั้งมิติที่เป็นประเด็นทางทหารและไม่เป็นประเด็นทางทหาร ดังนั้น จึงต้องมีการบูรณาการความร่วมมือระหว่างภาครัฐ เอกชนและกองทัพ โดยเฉพาะอย่างยิ่งในการออกแบบระบบเตือนภัยและเตรียมพร้อมรับมือกับความเสี่ยงไซเบอร์ นอกจากนี้เนื่องจากทรัพยากรบุคคลที่มีความรู้เชิงเทคนิคเกี่ยวกับความมั่นคงไซเบอร์ในภาครัฐมีไม่มากนัก ซึ่งเป็นข้อจำกัดที่หลายประเทศเผชิญ โมเดล Cyber Defence Unit of the Estonian Defence League ของประเทศเอสโตเนียจึงน่าสนใจเพราะหน่วยป้องกันไซเบอร์นี้เป็นหน่วยอาสาสมัครที่ทำหน้าที่ปกป้องคุ้มครองพื้นที่ไซเบอร์ของเอสโตเนียและมีกฎหมายรองรับสถานะและการมีอยู่ของหน่วย อย่างไรก็ตาม หากจะมีการจัดตั้งหน่วยตามโมเดลนี้ ประเด็นสำคัญที่ต้องคำนึงคือเรื่องจริยธรรมไซเบอร์ กล่าวคือการปฏิบัติการของหน่วยเพื่อป้องกันพื้นที่ไซเบอร์ของประเทศจะต้องอยู่บนพื้นฐานของประโยชน์สาธารณะและการเคารพสิทธิและเสรีภาพของประชาชน ในแง่นี้หน่วยอาสาสมัครป้องกันไซเบอร์ใด ๆก็ตามจะต้องเป็นชุมชนของแฮกเกอร์ที่มีจริยธรรมหรือพวกหมวกขาว (Ethical/white hat hacker community)

(3) สิ่งที่มักจะมาพร้อมกับการโจมตีไซเบอร์คือการปล่อยข้อมูลที่บิดเบือน (Disinformation) ในพื้นที่ไซเบอร์เพื่อยุยงปลุกปั่นและสร้างความสับสนงุนงงให้กับสังคมของประเทศ

ที่ตกเป็นเป้าหมายการโจมตี เท่ากับเป็นการสร้างความเปราะบางจากภายใน ดังนั้นการรู้เท่าทันสื่อดิจิทัล (Digital literacy) จึงเป็นสิ่งจำเป็นในการรับมือกับข้อมูลที่บิดเบือนที่สำเร็จ โจทย์สำคัญจึงอยู่ที่ว่าเราจะสร้างพลเมืองรู้เท่าทันสื่อได้อย่างไร ในกรณีของสหภาพยุโรปมีการทำแคมเปญ “EU vs Disinformation” ซึ่งดำเนินการโดย European External Action Service East Stratcom TaskForce กลุ่มงาน เฉพาะกิจนี้มีภารกิจในการรวบรวมข้อมูลที่บิดเบือน เกี่ยวกับสหภาพยุโรปและประเทศสมาชิกที่ถูก เผยแพร่โดยสื่อของรัสเซีย จากนั้นก็มีการจัดทำเอกสาร Disinformation Review รายสัปดาห์ เพื่อชี้ให้เห็นการบิดเบือนข้อเท็จจริงโดยเทียบ ข้อเท็จจริงหรือข้อมูลที่สามารถยืนยันที่มาได้กับ ข้อมูลที่บิดเบือน เอกสารดังกล่าวสามารถเข้าถึงได้ ผ่านช่องทางออนไลน์และผู้ที่ลงทะเบียนไว้ก็จะได้รับ เอกสารนี้ทางจดหมายอิเล็กทรอนิกส์รายสัปดาห์ในกรณีของเอสโตเนีย เนื่องจากประชากรเอสโตเนีย ที่มีเชื้อสายรัสเซียรับข้อมูลข่าวสารจากสื่อของ รัสเซียเป็นหลัก รัฐบาลเอสโตเนียจึงลงพื้นที่จัด กิจกรรมเผยแพร่ประชาสัมพันธ์ (Outreach activities) ข้อมูลที่เป็นข้อเท็จจริง โดยหลักการสำคัญ ของการจัดกิจกรรมนี้คือการนำเสนอข้อเท็จจริงชุด หนึ่งโดยไม่บังคับให้เชื่อ ดังนั้นอำนาจการตัดสินว่า ชุดข้อมูลใดน่าเชื่อถือกว่ากันจึงอยู่ที่ประชาชน (Lindau, 2012)

(4) การโจมตีไซเบอร์จะสำเร็จ ส่วนหนึ่งก็ด้วยความบกพร่องหรือความไม่รู้ของ ผู้ใช้พื้นที่ไซเบอร์ ดังนั้นการสร้างสุขอนามัยไซเบอร์ที่ดี (Cyber hygiene) ของผู้ใช้พื้นที่ไซเบอร์จึงจำเป็น อย่างยิ่ง หลักสำคัญของสุขอนามัยไซเบอร์ที่ดีคือ พฤติกรรมการใช้พื้นที่ไซเบอร์ที่ลดความเสี่ยงไซเบอร์ ทุกรูปแบบ ไม่ว่าจะเป็นการอัพเดทซอฟท์แวร์ที่ป้องกัน ไวรัสสม่ำเสมอ, การไม่เข้าเว็บไซต์ที่ไม่น่าเชื่อถือ, การ เก็บรักษารหัสผ่านและเปลี่ยนเมื่อถึงกำหนดเวลา, การแจ้งหน่วยงานที่เกี่ยวข้องหากพบความผิดปกติ ของระบบ เป็นต้น แนวทางหนึ่งในการสร้างสุข อนามัยไซเบอร์ที่ดีคือการจัดฝึกอบรม (Training) ให้กับผู้ใช้พื้นที่ไซเบอร์และการเผยแพร่องค์ความรู้ ต่อสาธารณะผ่านช่องทางต่าง ๆ ในกรณีของประเทศ เอสโตเนีย ได้มีการจัดสอบวัดความรู้เกี่ยวกับ สุขอนามัยไซเบอร์ที่ดีให้กับบุคลากรในภาครัฐผ่าน ช่องทางออนไลน์ โดยคำถามจะเป็นสถานการณ์ สมมติจำนวนหนึ่งและให้ผู้ทำสอบเลือกคำตอบในแง่นี้ การจัดฝึกอบรมและทดสอบผ่านช่องทาง ออนไลน์จึงเป็นอีกหนึ่งหนทางที่จะลดความเสี่ยง ไซเบอร์โดยรวม

2.3.5 ทฤษฎีการป้องกันอาชญากรรมตามสถานการณ์ (Situational Crime Prevention)

อาณาจักรดิจิทัลหรือการเชื่อมต่อระหว่างอุปกรณ์และอินเทอร์เน็ตมีมากขึ้นเรื่อย ๆ ที่สำคัญต่อสังคมยุคใหม่ ตั้งแต่ความสำคัญที่เพิ่มขึ้นของอุปกรณ์พกพาไปจนถึงความพร้อมใช้งานของคอมพิวเตอร์โน๊ตบุ๊ค อุปกรณ์ขนาดเล็กและพกพาอื่นๆ ผู้คนเชื่อมต่อถึงกันมากขึ้นและพึ่งพาอินเทอร์เน็ตในการดำเนินกิจกรรมประจำวัน โดยเฉพาะอย่างยิ่งในบริบทของยุคข้อมูลข่าวสารและความก้าวหน้าทางเทคโนโลยีที่แข่งขันได้เปลี่ยนไปเกือบทุกด้านสังคมโลกกายภาพ สู่สังคมโลกดิจิทัล

ตัวอย่างเช่น ระบบอาหารและน้ำ ระบบสุขภาพและเหตุฉุกเฉินบริการ สถาบันการศึกษา และสถาบันการธนาคารและการเงินล้วนพึ่งพาระบบสารสนเทศและอินเทอร์เน็ตอย่างมาก เพื่อให้เกิดการเชื่อมต่อระหว่างระบบโครงสร้างพื้นฐานที่สำคัญ (Lewis, 2006; Skopik, Bleier, & Fiedler, 2012) แม้ว่าความก้าวหน้าดังกล่าวทำให้บางแง่มุมของชีวิตง่ายขึ้น แต่ก็สร้างช่องโหว่ให้กับโลกไซเบอร์ด้วยภัยคุกคามที่สามารถคุกคามความมั่นคงของชาติและความมีชีวิตชีวาทางเศรษฐกิจ (Ten, Manimaran, & Liu, 2010) นอกจากนี้ เหตุการณ์ด้านความปลอดภัยที่สำคัญบนระบบไซเบอร์สามารถก่อให้เกิดผลกระทบอย่างมากต่อโครงสร้างพื้นฐาน

ตามพระราชบัญญัติการฉ้อโกงและการละเมิดทางคอมพิวเตอร์ของสหรัฐอเมริกา (พ.ศ. 2527) และพระราชบัญญัติการใช้ในทางที่ผิดทางคอมพิวเตอร์ของสหราชอาณาจักร (พ.ศ. 2533) อาชญากรรมทางไซเบอร์หมายถึงการกระทำความผิดทางอาญาที่ทำลายชื่อเสียงของเหยื่อ ทั้งทางร่างกายและจิตใจ ทำร้ายหรือข่มขู่กรรโชกผู้เสียหายทางตรงหรือทางอ้อมผ่านเครือข่าย คอมพิวเตอร์ และโทรศัพท์มือถือ (Casey, Blitz, & Steuart, 2004; Choi, 2015; Thomas & Loader, 2000) ในการตอบสนองต่ออาชญากรรมทางไซเบอร์ เป้าหมายหลักของระบบความปลอดภัยทางไซเบอร์ ได้แก่ การรักษาความเป็นส่วนตัว การรักษาข้อมูล ความสมบูรณ์ การพิสูจน์ตัวตนผู้ใช้ที่ได้รับอนุมัติของทรัพยากรเครือข่าย และทำให้ผู้ใช้ที่ได้รับอนุญาตสามารถเชื่อมต่อได้ไปยังเครือข่ายภายในอย่างปลอดภัยจนถึงปัจจุบัน การวิจัยเกี่ยวกับการป้องกันอาชญากรรมทางไซเบอร์ (ความปลอดภัยทางไซเบอร์) ยังคงมีอยู่อย่างจำกัด

ในขณะที่ประเทศไทย ยังพบว่า อาชญากรไซเบอร์ที่ก่อความผิดอยู่ต่างประเทศ ไม่สามารถบังคับใช้กฎหมายตาม พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ฉบับนี้ได้ ต้องอาศัย กฎหมายระหว่างประเทศและอนุสัญญาระหว่างประเทศที่ประเทศไทยเข้าร่วมเป็นภาคีสมาชิกอยู่ด้วย ทำให้การบังคับใช้กฎหมายซึ่งเป็นมาตรการป้องกันและปราบปรามการกระทำผิดในลักษณะนี้มีข้อจำกัดและยังไม่เกิดประสิทธิภาพดีเท่าที่ควร ซึ่งมีเจ้าหน้าที่ระดับสูงของกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) ท่านหนึ่งกล่าวว่า “อาชญากรรมประเภทนี้มีความซับซ้อนในการกระทำความผิด เนื่องจากคนร้ายมีการเชื่อมโยง WIFI internet จากที่ไหนก็ได้ ทำให้การติดตามสืบสวนตัวผู้กระทำผิดได้ยากมาก ซึ่งมีกรณีที่เคยพบคือ เจ้าหน้าที่ได้ตรวจสอบ IP Address ของคนร้ายปรากฏว่า มีหลาย IP Address ปรากฏขึ้นเป็นสถานที่ของรัฐ สถานที่ต่างๆ ในเวลาที่ไล่เลี่ยกัน หรือไม่ก็ในเวลาที่ไม่แน่นอน เป็นไปได้ทั้งกลางวันและกลางคืน ทำให้ตรวจสอบยากนั่นคือ คนร้ายจะใช้สถานที่ก่อเหตุได้หลาย ๆ ที่ ที่ไหนก็ได้ เวลาใดก็ได้ไม่มีข้อจำกัดในการกระทำความผิด”

ผู้วิจัยจึงเห็นว่า การนำทฤษฎี Situational Crime Prevention (SCP) มาอธิบายแนวทางการป้องกันอาชญากรรมตามสถานการณ์ จะชี้ให้เห็นว่าอาชญากรรมสามารถป้องกันได้ด้วยสิ่งแวดล้อมที่ส่งผลกระทบทางตรงและทางอ้อมต่อการรับรู้ของอาชญากร เพราะในช่วงไม่กี่ปีที่ผ่านมา การใช้ทฤษฎีการป้องกันอาชญากรรมตามสถานการณ์ในกระบวนการยุติธรรมทางอาญาได้เกิดขึ้นอย่างมากจากนักวิชาการและผู้กำหนดนโยบายในสหราชอาณาจักรและสหรัฐอเมริกา (Welsh & Farrington, 2547) และ Cornish and Clarke (2003) สังเกตว่าการเลือกอย่างมีเหตุผล กิจวัตรประจำวัน และทฤษฎีรูปแบบอาชญากรรมพบได้ในทฤษฎีการป้องกันอาชญากรรมเชิงสถานการณ์และมีความเชื่อมโยงกัน **ประการแรก** ทฤษฎีทางเลือกที่มีเหตุผล (Rational Choice Theory : RCT) มีพื้นฐานมาจากหลักการอรรถประโยชน์ ซึ่งผู้คนจะเลือกอย่างมีเหตุผลตามขอบเขตที่พวกเขาคาดหวังการตัดสินใจที่จะให้ผลประโยชน์และหลีกเลี่ยงการสูญเสียตาม RCT ผู้กระทำผิดจะเลือกเป้าหมายและกำหนดวิธีการเพื่อให้บรรลุวัตถุประสงค์ และ RCT ให้มุมมองทางทฤษฎีเพื่ออธิบายว่าการทำงานของ SCP เพื่อป้องกันอาชญากรรมเป็นอย่างไร **ประการที่สอง** ทฤษฎีการกระทำที่เป็นกิจวัตร (Routine Activity Theory : RAT) อธิบายว่าเหตุการณ์อาชญากรรมเกิดขึ้นเมื่อใดนั้น ประกอบด้วย 3 ประการ คือ ผู้กระทำความผิดที่มีแรงจูงใจ เป้าหมายที่เหมาะสม และไม่มีผู้ปกครองที่มีความสามารถมาบรรจบกัน ซึ่งในแง่ที่เกี่ยวข้องกับข้อเสนอหลักของ RAT กล่าวคือ ยิ่งบุคคลมีแรงจูงใจในการก่ออาชญากรรมมากเท่าใด อาชญากรรมก็ยิ่งเกิดขึ้นเมื่อมีเป้าหมายที่เหมาะสมมากเท่านั้น และขาดการคุ้มครองทั้งที่เป็นทางการและไม่เป็นทางการ (Akers, 2013; Cohen & Felson, 1979) นำมาซึ่งสร้างกรอบทฤษฎี SCP เพื่ออธิบายว่าบทบาทของตัวแสดงหลัก สถานที่ และเป้าหมายที่เหมาะสม เกี่ยวข้องกับการเกิดเหตุการณ์อาชญากรรมอย่างไร **ประการที่สาม** ตามทฤษฎีรูปแบบอาชญากรรม (Crime Pattern Theory : CPT) คือ รูปแบบการเคลื่อนไหวตามปกติของอาชญากรมีความสัมพันธ์กับพฤติกรรมอาชญากร (Brantingham & Brantingham, 1993, 1995) ตัวอย่างเช่น ทฤษฎีรูปแบบอาชญากรรม อธิบายว่าการกระจายตัวของผู้กระทำความผิด เป้าหมาย ผู้ดำเนินการ ผู้พิทักษ์ ในช่วงเวลาและสถานที่เกี่ยวข้องกับรูปแบบของอาชญากรรมตามเหตุการณ์ โดยเฉพาะอย่างยิ่ง Eck and Weisburd (2015) กล่าวว่า "ปฏิสัมพันธ์ของผู้กระทำความผิดด้วยสภาพแวดล้อมทางกายภาพและทางสังคม” ส่งผลต่อกระบวนการเลือกเป้าหมายของอาชญากร ในเรื่องนี้ กรอบทฤษฎีของ CPT มีอิทธิพลต่อมาตรการ SCP ที่เกี่ยวข้องกับการอธิบายการรวมกลุ่มของอาชญากรรมเป็นประเด็นสำคัญ กล่าวอีกนัยหนึ่ง คุณลักษณะของ RCT, RAT และ CPT ได้ช่วยในการพัฒนาการจัดประเภทของ SCP อย่างมีแบบแผน ตามที่กล่าวไว้ข้างต้น เทคนิค SCP สามารถขยายไปยังการตั้งค่าทางไซเบอร์เพื่อเพิ่มกรอบการป้องกันอาชญากรรมทางไซเบอร์ ในโลกเสมือนจริง ผู้ใช้ออนไลน์ที่มีเทคนิคการเจาะเป้าหมายทางไซเบอร์ (เช่น ระบบไฟร์วอลล์) อาจมีโอกาสน้อยที่จะประสบกับการบุกรุกทางไซเบอร์และการเข้าถึงโดยไม่ได้รับอนุญาต ระบบไฟร์วอลล์เป็นฮาร์ดแวร์หรือซอฟต์แวร์ที่ 1) อนุญาตการ

รับส่งข้อมูลสำหรับการเชื่อมต่อที่สร้างไว้ และ 2) ปฏิเสธการรับส่งข้อมูลสำหรับ Malicious Packets หรือแพ็กเก็ตที่เป็นอันตรายและมีข้อมูลข่าวสารที่เป็นเท็จ เพื่อให้สามารถป้องกันเครือข่ายจากการเข้าถึงโดยไม่ได้รับอนุญาตและเป็นอันตรายต่อการถูกการโจมตี (Holden, 2003) ตัวอย่างเหล่านี้สนับสนุนเทคนิคการป้องกันอาชญากรรมตามสถานการณ์ ไม่เพียงสามารถใช้เพื่อลดอาชญากรรมในโลกกายภาพเท่านั้น แต่ยังสามารถนำไปใช้เพื่อลดอาชญากรรมทางไซเบอร์ได้อีกด้วย โดยเฉพาะอย่างยิ่งสถาบันอุดมศึกษาสามารถใช้เทคนิคการป้องกันอาชญากรรมในสถานการณ์ต่างๆเพื่อปกป้องข้อมูลที่มีค่าและละเอียดอ่อนด้วยเครื่องมือดังกล่าว เช่น ไฟร์วอลล์ การเข้ารหัส ความปลอดภัยทางไซเบอร์ การฝึกอบรมคณาจารย์ บุคลากร และนักศึกษา (Back & LaPrade, 2020)

2.4 พลวัตของภัยคุกคามความมั่นคงปลอดภัยไซเบอร์

พัฒนาการครั้งสำคัญที่เปลี่ยนผ่านสู่โลกอนาคต เมื่อยุคแห่งคอมพิวเตอร์เข้ามามีบทบาทระบบดิจิทัล เข้ามาแทนที่ ซึ่งสามารถรับส่งสัญญาณได้อย่างมีประสิทธิภาพและซับซ้อนมากกว่าระบบอะนาล็อก ที่มีความแม่นยำน้อยกว่า การเปลี่ยนแปลงนี้มีส่วนช่วยให้เทคโนโลยีถูกพัฒนาต่อไปอย่างก้าวกระโดด เมื่อเทคโนโลยีมีการพัฒนามากขึ้น การเข้าถึงเทคโนโลยีของผู้คนจึงเป็นไปได้โดยสะดวกมากขึ้นตามไปด้วย ยุคของการถือกำเนิดขึ้นของเครื่องคอมพิวเตอร์เครื่องแรกที่เป็นโมเดลต้นแบบของเครื่องคอมพิวเตอร์ที่ใช้กันอยู่ในปัจจุบัน หรือราว ๆ ปี ค.ศ. 1960 แน่นอนว่าในยุคดังกล่าวยังไม่มีการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์เข้าด้วยกันจนกลายเป็นเครือข่ายไม่ว่าจะภายในหรือระหว่างองค์กร ซึ่งลักษณะการทำงานจะอาศัยเครื่องคอมพิวเตอร์เป็นเครื่องมือในการสร้าง เก็บรักษา หรือประมวลผลข้อมูลตามภารกิจของแต่ละหน่วยงานหรือองค์กรเท่านั้น คอมพิวเตอร์ในยุคนี้จึงไม่ได้อยู่ในฐานะของอุปกรณ์การสื่อสารระหว่างมนุษย์หรือระหว่างคอมพิวเตอร์ด้วยกันเอง ต่อมาในปี ค.ศ. 1969 ที่เครือข่ายคอมพิวเตอร์หรืออินเตอร์เน็ตได้รับการพัฒนาจนสำเร็จภายใต้โครงการวิจัยและพัฒนาระบบการติดต่อสื่อสารขององค์กรในกระทรวงกลาโหมประเทศสหรัฐอเมริกา หรือ ARPAnet ยุคนี้เองที่เป็น “ยุคแรก” ของการเชื่อมต่อโดยใช้เครื่องคอมพิวเตอร์เป็นเครื่องมือเพื่อติดต่อสื่อสารระหว่างบุคคลกับบุคคล และถูกพัฒนาให้เป็นเทคโนโลยีใหม่ที่สำคัญคือ เว็บไซต์ เชื่อมโยงเครือข่ายแบบ World Wide Web (www) จนกลายมาเป็น “ยุคข้อมูลข่าวสาร” (Information Age) ที่สถานะของผู้ใช้งานเว็บไซต์เป็นผู้อ่านอย่างเดียว (Read-Only Web) ต่อมาผู้ใช้งานอินเตอร์เน็ตสามารถสร้างเนื้อหาในอินเตอร์เน็ตได้ด้วยตัวเอง (User Generate Content) เนื่องจากโปรแกรมคอมพิวเตอร์ แพลตฟอร์ม (Platform) หรือเครื่องมือทางเทคโนโลยีต่าง ๆ ที่ถูกพัฒนาขึ้นเพื่อช่วยอำนวยความสะดวกให้แก่ผู้ใช้บริการ เป็นยุคเพื่อการอ่านและการเขียนอีกทั้งส่งเสริมการแบ่งปันข้อมูล (Share file) และแพร่กระจายอย่างรวดเร็ว มีคำที่ใช้เรียกยุคนี้ว่า ยุค Web 2.0 หรือ Web Two Point Oh ในเวลาต่อมา เครื่องคอมพิวเตอร์ได้ถูกพัฒนา

ให้ผู้ใช้สามารถพกพาได้ (Computer Notebook) เพื่อเชื่อมต่อกับอุปกรณ์อิเล็กทรอนิกส์อื่นๆ เช่น โทรศัพท์มือถืออัจฉริยะ (Smartphone) และคอมพิวเตอร์แท็บเล็ต (Tablet Computer) ส่งผลให้การให้บริการ การบริหารจัดการ และการเก็บรักษาข้อมูลในฝั่งของผู้ให้บริการอินเตอร์เน็ตเองก็พัฒนาอย่างมากเช่นเดียวกัน ซึ่งอาจเรียกได้ว่าเป็นยุค Cloud Computing ที่ผู้ใช้งานอุปกรณ์อิเล็กทรอนิกส์เหล่านี้ หันไปฝากข้อมูลของตนไว้ที่คลาวด์ หรือบริการที่ให้ทั้งพื้นที่จำนวนมากในการจัดเก็บ และช่วยบริหารจัดการข้อมูลเหล่านั้นให้ด้วย (สาวตรี สุขศรี, 2560)

อนึ่ง การพัฒนาระบบคอมพิวเตอร์ยังไม่ถึงจุดสิ้นสุด ยุคปัจจุบันเป็นยุคของการเชื่อมต่อและสื่อสารระหว่างกัน อุปกรณ์อิเล็กทรอนิกส์จำนวนมากจะสามารถเชื่อมโยงกับอินเตอร์เน็ต และเชื่อมโยงระหว่างอุปกรณ์ต่ออุปกรณ์ด้วยกันเอง หรือที่เรียกว่า “อินเตอร์เน็ตของสรรพสิ่ง” (Internet of Things) โดยเป้าหมายของการเชื่อมโยงนั้น มีทั้งเพื่อความสะดวกสบายให้กับผู้ใช้งาน ทำให้มนุษย์สามารถสั่งการ ควบคุม ใช้งาน ผ่านอุปกรณ์และอินเตอร์เน็ตได้ เช่น สั่งเปิด-ปิดเครื่องใช้ไฟฟ้า รถยนต์ เครื่องมือ เครื่องจักรในโรงงานอุตสาหกรรม เป็นต้น ไปจนถึงเพื่อการวิเคราะห์ วิจัย และพัฒนาผลิตภัณฑ์หรือบริการใหม่ๆ ให้ตอบสนองต่อความต้องการของผู้ใช้บริการได้มากขึ้น สำหรับอนาคตอันใกล้ที่หลายคนเรียกว่า ยุค Web 3.0 นั้น ตั้งอยู่บนแนวคิดและเทคโนโลยีที่อาศัยฐานข้อมูลขนาดใหญ่ (Big Data) ร่วมกับปัญญาประดิษฐ์ (Artificial Intelligent : AI) ที่อุปกรณ์หรือเครื่องจักรสามารถเรียนรู้การทำงานต่าง ๆ ได้ด้วยตัวเอง และเพื่อให้บริการและจัดการข้อมูล เพื่อสร้างสรรค์สิ่งใหม่ๆ ให้ตอบสนองความต้องการของมนุษย์

อย่างไรก็ตาม วิวัฒนาการและความก้าวหน้าทางเทคโนโลยีสารสนเทศและนวัตกรรมใหม่อย่างคอมพิวเตอร์ การเชื่อมต่อระหว่างกันจนเกิดเป็นเครือข่ายขนาดเล็กและใหญ่ในช่วงปลายทศวรรษที่ 60 หรือ ปี ค.ศ. 1969 ต้นกำเนิดอินเตอร์เน็ตนั้น ด้านหนึ่งได้สร้างคุณูปการต่าง ๆ แต่ในอีกด้านหนึ่ง ก็ถูกใช้เป็นเครื่องมือในการกระทำความผิด หรือตกเป็นเป้าหมายแห่งการกระทำความผิด เพราะเหตุที่คอมพิวเตอร์เป็นอุปกรณ์ เก็บรักษา และรับ-ส่ง ข้อมูลข่าวสาร ซึ่งกลายเป็นทรัพย์สินที่อาจมีค่ายิ่งกว่าทรัพย์ที่มีรูปร่าง และหากไล่เรียงมาตั้งแต่วันที่มีคอมพิวเตอร์เครื่องแรกจนถึงปัจจุบัน เป้าหมาย ลักษณะ และรูปแบบของการกระทำความผิดที่เกี่ยวข้องกับคอมพิวเตอร์หาได้คงที่ ตายตัว หรือให้ภาพจำ อย่างการบุกรุกคอมพิวเตอร์ การโจรกรรมข้อมูล หรือการเผยแพร่ข้อมูลผิดกฎหมายอย่างที่เข้าใจกันอยู่ในปัจจุบันไม่ เป้าหมายแห่งการกระทำความผิดมีความเป็นพลวัต พัฒนา และขยายตัวอย่างต่อเนื่อง และกระทบต่อความมั่นคงปลอดภัยในหลายประเทศทั่วโลก ซึ่งทั้งหมดนี้เกิดขึ้นในช่วงระยะเวลาเพียงไม่กี่สิบปีเท่านั้น

ในทำนองเดียวกัน ปัจจัยที่ก่อให้เกิดภัยคุกคาม อาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์ บางกรณีอาจมีสาเหตุมาจากการเปลี่ยนแปลงของสถานการณ์โลก เช่น สงครามโลก เศรษฐกิจ

ตกต่ำ การเมือง ปัญหาสังคม ความก้าวหน้าของเทคโนโลยี และความรู้สึกนึกคิดของมนุษย์ หรือหลายๆ ปัจจัยประกอบกันทำให้จากภัยคุกคามทวีความรุนแรงจนกลายเป็นอาชญากรรม โดยจากความคิดเห็นของนักวิชาการหลากหลายประเทศ ได้จำแนกออกเป็น 2 กลุ่มใหญ่ คือ 1) อาชญากรรมรูปแบบดั้งเดิม อย่างการโจรกรรม หรือการฉ้อโกง ที่มีเพียงจุดเชื่อมโยงบางอย่างกับเทคโนโลยีคอมพิวเตอร์ เมื่อมีการกระทำความผิดเท่านั้น กับ 2) อาชญากรรมรูปแบบใหม่ ซึ่งจะเกิดขึ้นได้โดยอาศัยเทคโนโลยีคอมพิวเตอร์เท่านั้น เช่น การแพร่โปรแกรมไวรัสทำลายระบบคอมพิวเตอร์ หรือโจมตีด้วยการระดมส่งคำสั่งให้ระบบปฏิเสธการให้บริการ (Dos or DDos Attack) การเข้าถึงข้อมูลโดยไม่มีอำนาจ รวมถึงการเผยแพร่หรือการแสวงหาประโยชน์จากข้อมูล ซึ่งอาจเป็นข้อมูลที่สำคัญและมีมูลค่าทางธุรกิจอย่างความลับทางการค้า ผลงานลิขสิทธิ์ หรือข้อมูลที่ล่วงละเมิดบุคคลอื่น รวมทั้งสิ่งลามกอนาจาร เป็นต้น (Bronitt & Gani, 2005)

2.4.1 อาชญากรรมคอมพิวเตอร์ (Computer Crime)

เหตุการณ์ประวัติศาสตร์อาชญากรรมคอมพิวเตอร์ในยุคแรกโดย โธมัส ไวต์ไซด์ (1978) ได้กล่าวไว้ว่า ในช่วงต้น ค.ศ. 1970s คือการทำลายคอมพิวเตอร์ทางกายภาพ (physical attacks on computer) ถูกทุบ ถูกทำลาย ถูกยิง ถูกระเบิด ซึ่งเกิดจากอุบัติเหตุ การจลาจล การประท้วง การก่อวินาศกรรม (Computer sabotages) การจารกรรมอุตสาหกรรม (Industrial espionage) เกิดขึ้นหลายแห่งทั้งใน สหรัฐอเมริกา อิตาลี ออสเตรเลีย แอฟริกาใต้ โดยเฉพาะมหาวิทยาลัยหลายแห่งในสหรัฐอเมริกา เกิดการรวมตัวประท้วงของนักศึกษาต่อต้านสงครามเวียดนาม และเมื่อการประท้วงเกิดความรุนแรงขึ้น ผลกระทบนอกจากความเสียหายต่ออาคารเรียนยังรวมถึงระบบคอมพิวเตอร์ของมหาวิทยาลัย นับตั้งแต่ปี ค.ศ. 1970 – 1978 โดยในปี ค.ศ.1978 ฐานทัพอากาศ Vandenburg ในแคลิฟอร์เนีย ถูกนักเคลื่อนไหวเพื่อสันติภาพทำลาย เครื่องคอมพิวเตอร์ IBM 3031 ที่ยังไม่ได้ใช้ด้วยค้อน ชะแลง เครื่องตัดสายไฟ และสว่านเพื่อต่อต้านระบบนำร่องดาวเทียม NAVSTAR (Whiteside, 1978)

ต่อมาในปี ค.ศ. 1980 คอมพิวเตอร์ถูกใช้อย่างแพรหลายมากขึ้น และเริ่มมีคอมพิวเตอร์ส่วนบุคคล (Personal Computer) ออกวางจำหน่ายในตลาด แม้ว่ายังไม่มีอินเตอร์เน็ต แต่ระบบโทรศัพท์ก็เติบโตอย่างกว้างขวาง โดยยุคนี้ เกิดการขโมยข้อมูล เปลี่ยนแปลงข้อมูลของบุคคล ธุรกิจ และธนาคาร เช่น ปลอมบัตรเครดิต ปลอมบัญชีธนาคาร เป็นยุคแรกของอาชญากรรมประเภท Identity Theft และเกิดอาชีพ Dumpster Diver (คนคุ้ยขยะ) ทำหน้าที่ขุดคุ้ยขยะหาข้อมูลใบเสร็จ สำเนาบัตรเครดิต ข้อมูลลูกค้า ข้อมูลธุรกิจ ไปขายต่อ เพื่อที่อาชญากรจะได้นำข้อมูลมาปลอมแปลงเพื่อใช้งาน เป็นอาชีพที่สร้างรายได้มากในอเมริกา โดยมีอาชญากรวัยรุ่นชื่อดังอย่าง Jerry Neal Schneider เป็นผู้นำสร้างความเสียหายต่อธุรกิจหลายแห่ง กระทั่งเริ่มมีการเข้าถึง

ข้อมูลคอมพิวเตอร์ผ่านเครือข่ายโทรคมนาคมในยุคต่อมา และราวปี ค.ศ. 1986 โปรแกรมไวรัสที่มีเป้าหมายในการทำลายล้างหรือเพื่อก่อวินาศกรรม (Sabotage) ตัวแรกถูกเขียนขึ้นในชื่อ “Pakistani Brain” มีลักษณะการประกอบอาชญากรรมโดยการเขียนโปรแกรมขึ้นเพียงครั้งเดียว แต่สามารถส่งต่อและเผยแพร่จนสร้างความเสียหายให้เหยื่อได้จำนวนมาก โดยการทำลายนี้มีผลต่อ Bootsektor อันเป็นส่วนประกอบสำคัญของเครื่องคอมพิวเตอร์ (Kabay, 2008)

อย่างไรก็ตาม โปรแกรมไวรัสมีจำนวนมากและหลากหลายชนิด ถูกเขียนขึ้นมาก่อนหน้าไวรัส “Pakistani Brain” ก็มี เพียงแต่ยังไม่ได้ถูกนำมาใช้เพื่อเป้าหมายในการโจมตีเหยื่อหรือก่อวินาศกรรม โดยไวรัสตัวแรก เป็นผลงานปริญญาเอกของ Fred Cohen เมื่อปี ค.ศ. 1983 จนกระทั่งก้าวสู่ยุคการกำเนิดอินเตอร์เน็ตในปี ค.ศ. 1990 การทำลายข้อมูลหรืออุปกรณ์คอมพิวเตอร์ด้วย ไวรัสผ่านโครงข่ายอินเทอร์เน็ตได้ก่อตัวขึ้นจากอาชญากรรมคอมพิวเตอร์ กลายเป็นอาชญากรรมไซเบอร์ (Cybercrime) เมื่อการทำลายอุปกรณ์คอมพิวเตอร์ และข้อมูลคอมพิวเตอร์ จากคอมพิวเตอร์ Stand alone ได้เปลี่ยนช่องทางการทำลายผ่านเครือข่ายอินเทอร์เน็ตขยายอำนาจสร้างความเสียหายในวงกว้างขึ้น

2.4.2 อาชญากรรมไซเบอร์ (Cyber Crime)

“อาชญากรรมไซเบอร์” (Cybercrime) เป็นปรากฏการณ์ทางสังคมที่ถือกำเนิดขึ้นจากการพัฒนาเทคโนโลยีคอมพิวเตอร์ ปฏิเสธไม่ได้ว่าในปัจจุบันเทคโนโลยีคอมพิวเตอร์ ได้เข้ามาเป็นส่วนหนึ่งในชีวิตประจำวันของกลุ่มคนส่วนใหญ่ในสังคม ไม่ว่าจะเป็นในระดับปัจเจกบุคคลที่ใช้เทคโนโลยีคอมพิวเตอร์ผ่านอุปกรณ์สมาร์ท ดีไว (Smart Devices) ที่เป็นตัวเชื่อมต่อกับระบบอินเทอร์เน็ต เข้ามาช่วยเหลือกิจกรรมส่วนตัวต่าง ๆ และในระดับกลุ่มที่ใหญ่ขึ้นจากสังคมรอบตัวที่นำเอาเทคโนโลยีคอมพิวเตอร์ เข้ามาเป็นตัวช่วยเสริมกิจกรรมทางสังคมในหลากหลายด้าน เทคโนโลยีคอมพิวเตอร์นั้นไม่ได้เป็นสิ่งที่อยู่ไกลตัว แต่กลับเข้ามาอยู่รอบตัวของเราโดยที่เราไม่ทันรู้ตัว การพัฒนาเทคโนโลยีคอมพิวเตอร์ในยุคปัจจุบัน ถูกพัฒนาอยู่บนพื้นฐานของระบบอินเทอร์เน็ต เกิดการเปลี่ยนแปลงไปสู่สังคมดิจิทัล (Digitalization) นำมาซึ่งภัยคุกคามความมั่นคงในลักษณะของการใช้อินเทอร์เน็ตและคอมพิวเตอร์เป็นช่องทางในการโจมตี หรือที่เรียกว่า อาชญากรรมไซเบอร์ ซึ่งการให้คำนิยามในยุคแรกของปัญหาอาชญากรรมไซเบอร์ หรือ ในช่วงปีพุทธศักราช 2519 นำโดย Don B. Parker (1976) ชาวสหรัฐอเมริกา ผู้ที่ได้ชื่อว่าเป็นบิดาแห่งอาชญากรรมคอมพิวเตอร์ในยุคนั้น ได้นิยามถึงถึงการกระทำความผิดทางคอมพิวเตอร์ไว้ในหนังสือ Crime by Computer ไว้ว่า

“การกระทำความผิดทางคอมพิวเตอร์ หรือ การใช้คอมพิวเตอร์ในทางที่ผิด (Computer abuse) สามารถตีความหมายได้แบบกว้าง คือ การกระทำใด ๆ ก็ตามที่ได้นำเอา

เทคโนโลยีทางคอมพิวเตอร์ เข้าไปมีส่วนในการกระทำจนเป็นเหตุให้เหยื่อต้องได้รับความเสียหาย หรือ เกิดความสูญเสีย และการกระทำดังกล่าวนั้นเป็นการกระทำที่เกิดขึ้นโดยเจตนาของผู้กระทำความผิด หรือกระทำไปเพื่อให้ได้รับประโยชน์จากการกระทำความผิดนั้น – Computer abuse is broadly defined to be any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator by intention made or could have made gain." (Parker, 1976)

ภายหลังจากนั้นเป็นต้นมาก็ได้มีการให้คำนิยามการกระทำความผิดทางคอมพิวเตอร์ตามมาอีกมากมายตามยุคสมัยที่เปลี่ยนแปลงไป โดยเฉพาะในช่วงเวลาหลังปีพุทธศักราช 2543 เป็นปีที่สังคมกระแสหลักได้เริ่มสัมผัสกับเทคโนโลยีคอมพิวเตอร์ที่มีชื่อเรียกว่า ระบบอินเทอร์เน็ต หรือ ระบบเครือข่ายคอมพิวเตอร์ ส่งผลให้คำนิยามที่ถูกนำมาอธิบายในยุคสมัยดังกล่าวได้มีการเริ่มกล่าวถึงระบบอินเทอร์เน็ตในนิยามจำกัดความของการกระทำความผิดทางคอมพิวเตอร์มากขึ้น พร้อมทั้งมีการปรับเปลี่ยนชื่อเรียกการกระทำความผิดทางคอมพิวเตอร์เหล่านี้ว่าเป็น "อาชญากรรมไซเบอร์(Cybercrime)" คำนิยามอาชญากรรมไซเบอร์ที่มีการกล่าวถึงระบบอินเทอร์เน็ต หรือ ระบบเครือข่ายคอมพิวเตอร์ ได้ปรากฏให้เห็นในหนังสือ Introduction to Cybercrime ที่แต่งโดย Joshua B. Hill และ Nancy E. Marion ที่ได้ให้คำนิยามอาชญากรรมไซเบอร์เอาไว้ว่า

"อาชญากรรมไซเบอร์เป็นอาชญากรรมที่มีความเกี่ยวข้องกับคอมพิวเตอร์และเครือข่ายระบบคอมพิวเตอร์ โดยทั่วไปแล้วหมายถึงการกระทำที่อาชญากรใช้ระบบอินเทอร์เน็ตหรือ ระบบคอมพิวเตอร์อื่น ๆ กระทำอันตราย หรือ สร้างความรบกวนให้กับระบบคอมพิวเตอร์ – Cybercrime can be thought of as crime that involves computers and computer networks. Generally, it refers to acts that involves criminal uses of the internet or other networked systemsto cause harm to others or some from of a disturbance." (Marion, Hill & Nancy, 2016)

ต่อมาอาชญากรรมไซเบอร์เติบโตกว้างขวางไปมากมายในหลายมิติในปัจจุบัน กล่าวคือ เป็นอาชญากรรมที่จะเกิดขึ้นไม่ได้ หากไม่มีการใช้อุปกรณ์คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์เชื่อมต่ออินเทอร์เน็ต แนวทางหลักในการกำกับดูแลอาชญากรรมไซเบอร์ของไทยนั้นได้รับอิทธิพลมาจาก Convention on Cyber crime โดยสภาแห่งยุโรป (The Council of Europe) และกฎหมายหลายฉบับของสหรัฐอเมริกา เช่น กฎหมายการใช้คอมพิวเตอร์ในทางที่ผิด (Computer Fraud and Abuse Act 1986) ซึ่งเป็น กฎหมายกำหนดฐานความผิด เช่น การเข้าถึงคอมพิวเตอร์โดยไม่ได้รับอนุญาตหรือเกินขอบเขตที่ได้รับอนุญาต กฎหมาย แคนสแปม (CAN-SPAM Act ย่อมา

จาก Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003) เป็นการกำหนดมาตรฐานการห้ามการส่งอีเมล์ขยะ กฎหมายการขโมยข้อมูลระบุตัวตน และการปลอมตน (Identity Theft and Assumption Deterrence Act) ส่วนในฝั่งอังกฤษ เช่น กฎหมายการใช้คอมพิวเตอร์ในทางที่ผิด (Computer Misuse Act) และกฎหมายการคุ้มครองข้อมูล (Data Protection Act) เป็นต้น ซึ่งรากฐานเหล่านี้ก็ได้เกิดเป็น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 (ฉบับที่ 2) ได้ประกาศบังคับใช้เป็นการทั่วไปแล้ว พรบ.คอมพิวเตอร์ฯ มิได้เพียงแค่ห้ามกระทำความผิดทางอาญาต่อคอมพิวเตอร์ หากแต่รวมถึงการนำคอมพิวเตอร์ไปก่ออาชญากรรมด้วย โดยเฉพาะเป็นภัยต่อความมั่นคงของชาติและระบบเศรษฐกิจ (ปรเมศวร์ กุมารบุญ, 2563) โดยอาชญากรรมทางไซเบอร์มีความผิดทางอาญาสองรูปแบบ ได้แก่

(1) อาชญากรรมที่ขึ้นกับไซเบอร์(Cyber-dependent Crimes) คืออาชญากรรมที่เกิดขึ้นจากการใช้อุปกรณ์ทางเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งอุปกรณ์ดังกล่าวเป็นเครื่องมือในการก่ออาชญากรรมและเป้าหมายของอาชญากรรม เช่น การพัฒนาและแพร่กระจายมัลแวร์สำหรับหวังผลทางการเงิน การแฮกเพื่อโจรกรรมข้อมูลและทำให้เกิดความเสียหาย การบิดเบือนหรือทำลายข้อมูล หรือเครือข่ายหรือกิจกรรม

(2) อาชญากรรมแบบที่ใช้ไซเบอร์ (Cyber-enabled Crimes) เป็นอาชญากรรมแบบดั้งเดิมที่สามารถเพิ่มขนาดหรือเข้าถึงได้โดยใช้คอมพิวเตอร์เครือข่ายคอมพิวเตอร์หรือ ICT รูปแบบอื่น ๆ เช่น การฉ้อโกงบนโลกไซเบอร์และการโจรกรรมข้อมูล

ดังนั้น ผู้วิจัยขอให้คำนิยามจำกัดความอาชญากรรมไซเบอร์ในปัจจุบัน ไว้ว่า “อาชญากรรมไซเบอร์ หมายถึง การประกอบอาชญากรรมที่ใช้เทคโนโลยีคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์เชื่อมต่อระบบเครือข่ายหรือระบบอินเตอร์เน็ต มาเป็นเครื่องมือในการกระทำความผิด หรือ การกระทำความผิดใดก็ตามที่สร้างความเสียหายต่อระบบคอมพิวเตอร์และระบบเครือข่ายทั้งทางตรงและทางอ้อม โดยการกระทำนั้นกฎหมายได้ระบุไว้ว่าเป็นความผิด”

ถึงแม้ว่าจะสามารถระบุผู้ที่ต้องรับผิดชอบต่อการกระทำทางอาชญากรรมไซเบอร์ที่สร้างความเสียหายต่อประเทศได้นั้น แต่ยังมีความยากลำบากสำหรับประเทศและหน่วยงานบังคับใช้กฎหมายระหว่างประเทศในการฟ้องร้องเมื่อบุคคลเหล่านั้นอยู่ในเขตอำนาจศาลที่มีข้อจำกัดหรือไม่มีข้อตกลงในเรื่องการส่งผู้ร้ายข้ามแดน กลุ่มแฮกเกอร์หลักๆจากทั่วทุกมุมโลก ได้ทำการพัฒนาและใช้งานมัลแวร์ขั้นสูงที่เผยแพร่ต่อคอมพิวเตอร์และเครือข่ายของประชากรโลกและรัฐบาลของประเทศต่าง ๆ ซึ่งผลกระทบได้กระจายไปทั่วรวมทั้งประเทศไทยด้วยเช่นเดียวกัน โดยการโจมตี

เหล่านี้มีความก้าวร้าวและเผชิญหน้ามากขึ้น ซึ่งเห็นได้จากการใช้ Ransomware เพิ่มมากขึ้นและภัยคุกคามจากการโจมตีระบบเครือข่ายแบบ Distributed denial of service (DDoS) ที่เป็นการโจมตีเว็บไซต์หรือบริการด้วยการส่งการเชื่อมต่อหรือคำขอในการเข้าถึงข้อมูลจำนวนมาก ๆ พร้อม ๆ กัน ซึ่งโดยปกติแล้วเว็บไซต์ต่าง ๆ จะทำเซิร์ฟเวอร์ให้มีขนาดมากพอสำหรับรองรับผู้ใช้ในปริมาณที่เหมาะสม เช่น อาจสามารถรองรับให้คนเข้ามาดูเว็บไซต์ได้พร้อมกัน 1 แสนคนในยามปกติ ซึ่งการโจมตีแบบ DDoS นั้นจะส่งผู้ใช้ในจำนวนที่มากกว่าที่เซิร์ฟเวอร์จะรองรับไหว (เช่น 1 ล้านคน) มาเข้าเว็บไซต์พร้อมกัน ทำให้เว็บไซต์รองรับผู้ใช้ไม่ไหวจนล่มและไม่สามารถใช้งานได้ในที่สุด (อีวาน พอร์ทเตอร์, 2565)

2.4.3 อาชญาวิทยาไซเบอร์ (Cyber Criminology)

การนำทฤษฎีดั้งเดิมของสาขาวิชาต่างๆ ที่ใช้ในการอธิบายสาเหตุอาชญากรรมโดยทั่วไปมาประยุกต์ใช้กับอาชญากรรมคอมพิวเตอร์หรืออาชญากรรมไซเบอร์ดังกล่าวข้างต้นแล้ว ในทศวรรษที่ผ่านมา มีนักอาชญาวิทยาร่วมสมัยที่ยังพยายามคิดค้นหรือพัฒนาทฤษฎีใหม่ๆ ขึ้นเฉพาะสำหรับอาชญากรรมคอมพิวเตอร์หรืออาชญากรรมไซเบอร์ และทฤษฎีใหม่ที่เป็นที่รู้จักกันในหมู่นักอาชญาวิทยาบ้างแล้วนั้น คือ “ทฤษฎีการเปลี่ยนพื้นที่” (Space Transition Theory) ของ K. Jaishankar (2007) นักอาชญาวิทยาชาวอินเดีย หนึ่งในกลุ่มนักวิชาการที่ช่วยกันพัฒนาและขยายขอบเขตการศึกษาอาชญาวิทยาไปสู่อาชญากรรมในพื้นที่ใหม่ที่เรียกว่า “อาชญาวิทยาไซเบอร์” (Cyber Criminology) โดยให้นิยามว่า *“การศึกษาสาเหตุการก่ออาชญากรรมที่เกิดขึ้นในโลกไซเบอร์ และผลกระทบในพื้นที่ทางกายภาพ”* ซึ่งคำนิยามนี้มีลักษณะของความเป็น “สหสาขาวิชาการ” ที่ต้องอาศัยความรู้และข้อมูลเชิงลึกจากทั้งทางสังคมและวิทยาศาสตร์คอมพิวเตอร์มาประกอบกัน ในขณะที่กรอบของการศึกษาสาเหตุอาชญากรรมคอมพิวเตอร์หรืออาชญากรรมไซเบอร์ผ่านทฤษฎีอาชญาวิทยาดั้งเดิม อาจไม่ค่อยให้ความสำคัญ หรือละทิ้งการทำความเข้าใจเทคโนโลยีคอมพิวเตอร์และธรรมชาติที่แตกต่างของพื้นที่ไซเบอร์ (Cyberspace) กับโลกทางกายภาพ ซึ่ง Jaishankar เห็นว่าพฤติกรรมของมนุษย์ในโลกกายภาพ (Physical space) กับในโลกไซเบอร์ (Cyberspace) มีความแตกต่างกัน ทฤษฎีของเขาอธิบายว่า โดยธรรมชาติของมนุษย์นั้นพฤติกรรมของพวกเขามักเปลี่ยนแปลงไปเมื่อมีการเคลื่อนย้ายหรือเปลี่ยนแปลงพื้นที่ ซึ่งพฤติกรรมที่แสดงออกมามีได้ทั้งที่สอดคล้อง และไม่สอดคล้องกันในระหว่างสองพื้นที่ โดยมีข้อสมมติฐานของการเกิดอาชญากรรมไซเบอร์ตามทฤษฎีของ Jaishankar ดังนี้

(1) บุคคลที่อัดอั้นเพราะไม่ได้กระทำความผิดในพื้นที่ทางกายภาพ เพราะเหตุผลด้านสถานภาพ หรือตำแหน่งหน้าที่ มักชอบที่จะกระทำผิดในโลกไซเบอร์ สมมติฐานนี้มาจากแนวคิดที่ว่า คนทั่วไปมักชั่งน้ำหนักความเสี่ยงทั้งทางกฎหมายและทางสังคมระหว่างการกระทำ

ความผิดกับการปฏิบัติตามกฎระเบียบ และมนุษย์ส่วนใหญ่เหมือนกันตรงที่ จะมีความกังวลกับสถานภาพของตนในพื้นที่ทางกายภาพ แต่จะไม่ใส่ใจสิ่งนี้ในโลกไซเบอร์ เนื่องจากไม่มีคนคอยจับตาหรือตีตราพวกเขาอยู่ การกระทำความผิดจึงเกิดขึ้นได้ง่ายกว่าโดยไม่ต้องชั่งน้ำหนักกับผลเสียของอะไร

(2) ความยืดหยุ่นจากการปิดบังตัวตนได้ และการขาดปัจจัยในการป้องปราม ทำให้โลกไซเบอร์เป็นพื้นที่เหมาะสำหรับการกระทำความผิด ซึ่งข้อนี้มาจากแนวคิดว่า เหตุผลที่สมาชิกในสังคมกายภาพส่วนใหญ่ต้องมีความซื่อสัตย์ หรือทำสิ่งที่ถูกต้องต่อกัน ก็เพราะกลัวการถูกจับได้ เมื่อโลกไซเบอร์สร้างพื้นที่ที่ยากแก่การตรวจจับขึ้น จึงทำให้คนกล้าที่จะแสดงอารมณ์ความรู้สึกอันไม่พึงประสงค์ กระทั่งกล้าล่วงละเมิดบุคคลอื่น ตัวอย่างเช่น แม้นักเจาะระบบจะมีมูลเหตุจูงใจที่แตกต่างกันไปในการลงมือกระทำความผิด แต่คุณสมบัติร่วมกันที่พบในนักเจาะระบบทั้งหลายคือการปิดบังตัวตนแท้จริงของพวกเขาในโลกไซเบอร์

(3) พฤติกรรมที่เป็นอาชญากรรมในโลกไซเบอร์มีแนวโน้มที่จะนำไปสู่การกระทำผิดในโลกทางกายภาพ ในขณะที่พฤติกรรมอาชญากรรมในโลกทางกายภาพก็อาจถูกส่งออกสู่พื้นที่ในโลกไซเบอร์ได้เช่นเดียวกัน ซึ่งหมายความว่า คนที่มีประวัติหรือเคยกระทำความผิดในโลกทางกายภาพมาแล้ว จะมีแนวโน้มเข้ามากระทำความผิดในโลกไซเบอร์ได้เช่นกัน และสิ่งนี้จะเกิดขึ้นในทางกลับกัน ตัวอย่างเช่น ผู้ที่มีพฤติกรรมชอบล่วงละเมิดทางเพศเด็กและเยาวชนในโลกทางกายภาพมักจะเป็นผู้เผยแพร่สื่อลามกอนาจารเด็กและเยาวชนเสียเองด้วยในเครือข่ายคอมพิวเตอร์ หรือแสวงหาเพื่อให้ได้มาซึ่งการครอบครองภาพลามกเด็กจากโลกออนไลน์ ในทางกลับกัน แม้จะยังไม่มีงานศึกษาวิจัยที่ชี้ชัดว่า ผู้ที่ได้ดูหรือเสพสื่อลามกเด็กที่เผยแพร่อยู่ในโลกออนไลน์อยู่เป็นประจำ จะหันไปเป็นผู้กระทำความผิดฐานล่วงละเมิดทางเพศกับเด็กจริงๆ แต่เหตุผลหนึ่งที่กฎหมายของหลาย ๆ ประเทศ รวมทั้งประเทศไทยที่กำหนดให้เพียงการมีไว้ในครอบครองซึ่งสื่อลามกเด็กเป็นความผิดตามกฎหมาย คือ การกระทำเช่นนั้นอาจเป็นปัจจัยที่ก่อให้เกิดการล่วงละเมิดทางเพศต่อเด็กและส่งผลกระทบต่อสวัสดิภาพของเด็ก

(4) กิจกรรมที่ทำในโลกไซเบอร์ กับความลื่นไหลไม่หยุดนิ่ง (Dynamic) ซึ่งเป็นธรรมชาติของโลกไซเบอร์ เปิดโอกาสให้ผู้กระทำความผิดหลบหนีได้ หมายความว่า การที่มนุษย์ไม่ได้อาศัยหรือใช้ชีวิตอยู่ในพื้นที่ของโลกไซเบอร์ตลอดเวลาเหมือนกับที่อยู่อาศัยในโลกทางกายภาพ อินเตอร์เน็ตที่เป็นเพียงพื้นที่สำหรับเที่ยวชม ทำกิจกรรมจากนั้นก็กลับออกมา จึงทำให้โลกไซเบอร์ไม่หยุดนิ่งและเปลี่ยนแปลงอยู่ตลอดเวลา เช่น เราสามารถเผยแพร่เนื้อหาเว็บไซต์ และลบเนื้อหานั้นออกได้ในเวลาใกล้เคียงกันได้ เป็นต้น เช่นนี้เองจึงเป็นการยากลำบากที่จะระบุหรือกำหนดสถานที่เกิดเหตุ หรือที่ก่ออาชญากรรมในอินเตอร์เน็ตได้อย่างชัดเจน และทั้งยังเปิดโอกาสให้ผู้กระทำความผิดหลบหนี หรือเปลี่ยนที่ทางในการทำกิจกรรมความผิดนั้นได้ง่ายอีกด้วย

(5) คนแปลกหน้าจะรวมตัวกันในโลกไซเบอร์เพื่อประกอบอาชญากรรมในโลกทางกายภาพ และการสมาคมกันในโลกทางกายภาพ จะนำไปสู่การประกอบอาชญากรรมในโลกไซเบอร์ ขยายความได้ว่า อินเตอร์เน็ตเป็นพื้นที่สื่อกลางที่มีประสิทธิภาพในการหาสมัครพรรคพวกในการประกอบอาชญากรรม หรือเผยแพร่เทคนิคการกระทำความผิดให้กับคนที่ชอบอะไรเหมือนๆกัน ในขณะที่กลุ่มคนที่ผิดหวังหรือเจ็บแค้นบริษัทหรือองค์กรที่ทำงานอยู่ ก็สามารถร่วมกันประกอบอาชญากรรมไซเบอร์ด้วยการเจาะระบบ สอดแนม หรือขโมยข้อมูลเพื่อทำลายองค์กรนั้นๆ ได้

(6) ผู้คนที่อยู่ในสังคมปิด (Close societies) มีแนวโน้มที่จะประกอบอาชญากรรมในโลกไซเบอร์ได้ง่ายกว่าผู้ที่อยู่ในสังคมเปิด (Open societies) โดยคำว่า “สังคมปิด” และ “สังคมเปิด” ในที่นี้มีนัยทางการเมือง กล่าวคือ สังคมเปิด คือสังคมที่ผู้ปกครองสามารถถูกโค่นล้มได้โดยไม่ต้องใช้ความรุนแรง หรือนองเลือด เช่น สังคมในระบบประชาธิปไตย ในขณะที่สังคมปิดคือสังคมที่ต้องอาศัยความรุนแรง เมื่อต้องการเปลี่ยนแปลงผู้นำอย่างสังคมในระบบเผด็จการ หรือที่กษัตริย์มีอำนาจเต็ม เป็นต้น ซึ่งจะเห็นได้ว่าสังคมแบบเปิดที่ประชาชนมีเสรีภาพในการคิดเชิงวิพากษ์ (Critical thinking) แสดงความคิดเห็น และมีส่วนร่วมทางการเมืองได้ภายใต้ความคุ้มครองของกฎหมาย มีแนวโน้มที่จะกระทำความผิดในโลกออนไลน์น้อยกว่าคนในสังคมเผด็จการที่ถูกปิดกั้นทั้งทางความคิด และการแสดงออก เพราะคุณสมบัติของพื้นที่ไซเบอร์ก็คือสถานที่แห่งการปลดปล่อยของผู้คนที่ต้องเก็บกดในโลกทางกายภาพ

(7) ความขัดแย้งกันระหว่างมาตรฐานและคุณค่าของโลกทางกายภาพ กับมาตรฐานและคุณค่าของโลกไซเบอร์อาจนำไปสู่การประกอบอาชญากรรมไซเบอร์ได้ (Jaishankar, 2007)

จากตัวอย่างที่กล่าวมา ผู้วิจัยสนใจประเด็นข้อสมมติฐานของ Jaishankar ในการนำมาอธิบายสาเหตุการเกิดภัยคุกคามทางไซเบอร์และอาชญากรรมไซเบอร์ได้ค่อนข้างชัดเจน แม้ในบางทฤษฎี อาจตั้งข้อสังเกตหรือข้อควรระวังในการนำมาอธิบายอยู่บ้าง เนื่องจากธรรมชาติและลักษณะของทั้งอาชญากรรมและตัวอาชญากรทางคอมพิวเตอร์แตกต่างไปจากอาชญากรรมโดยทั่วไปก็ตาม แต่สิ่งที่ควรเกิดขึ้นในอนาคตคือ การเก็บรวบรวมข้อมูลและการทดสอบข้อสมมติฐานตามทฤษฎีต่างๆ อย่างกว้างขวางและครอบคลุมประเภทของอาชญากรรม และให้เป็นระบบมากขึ้น เพื่อนำไปสู่แนวทางการป้องกันและปราบปรามการกระทำความผิดที่มีประสิทธิภาพและประสิทธิผลยิ่งขึ้น ในส่วนของ อาชญาวิทยาไซเบอร์ (Cyber Criminology) และ ทฤษฎีการเปลี่ยนพื้นที่ นั้น อาจยังมีนักอาชญาวิทยาจำนวนไม่มากนักที่นำข้อสมมติฐานของทฤษฎีนี้ไปทดสอบเชิงประจักษ์ แต่ในมุมมองของผู้วิจัย แนวคิดนี้ก็สามารถสร้างมุมมองใหม่ ๆ ให้เกิดแก่วงการอาชญาวิทยา หรืออาจนำไปสู่การ

วิพากษ์ ถกเถียง กระทั่งเกิดความคิดที่อยากจะพัฒนาทฤษฎีใหม่ ๆ เพื่ออธิบายปรากฏการณ์หรือสถานการณ์ภัยคุกคามและอาชญากรรมไซเบอร์ให้สมบูรณ์แบบมากยิ่งขึ้น

2.5 แนวทางการกำกับดูแลและรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์

2.5.1 การเตรียมองค์กรสอดรับกฎหมายและยุทธศาสตร์ทางไซเบอร์

ความมั่นคงปลอดภัยไซเบอร์มีความสำคัญอย่างยิ่งในการปกป้องทรัพยากรขององค์กร National Cyber Security Centre (NCSC) หรือ ศูนย์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติของสหราชอาณาจักร ให้ความหมายของความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ไว้กว้าง ๆ ว่าคือ “วิธีที่บุคคลหรือหน่วยงานทำเพื่อลดความเสียงต่อการถูกโจมตีทางไซเบอร์” ในขณะที่หน่วยงานความมั่นคงปลอดภัยไซเบอร์และความมั่นคงปลอดภัยของโครงสร้างพื้นฐานของสหรัฐอเมริกา (Cybersecurity & Infrastructure Security Agency) ให้คำนิยามไว้ว่า “ศิลปะในการป้องกันเครือข่าย อุปกรณ์ และข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาตหรือการนำไปใช้ทางอาชญากรรม และการทำให้มั่นใจว่าข้อมูล (information) ได้รับการรักษาความลับ (confidentiality) การรักษาความครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability)”

สำหรับในประเทศไทย มาตรการทางกฎหมาย ระเบียบปฏิบัติ และยุทธศาสตร์ที่สำคัญในด้านการกำกับดูแลและรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ มีดังนี้

2.5.1.1 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่ให้ความหมาย “การรักษาความมั่นคงปลอดภัยไซเบอร์” ไว้ หมายความว่า “มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ” (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2564) โดยแบ่งออกเป็น 4 ส่วน คือ นโยบายและแผน การบริหารจัดการ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการรักมือกับภัยคุกคามทางไซเบอร์ โดยภัยคุกคามทางไซเบอร์แบ่งเป็น 3 ระดับ คือ ระดับไม่ร้ายแรง ระดับร้ายแรง และระดับวิกฤต

2.5.1.2 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือที่รู้จักในนาม PDPA ย่อมาจาก Personal Data Protection Act เป็นกฎหมายว่าด้วยการให้สิทธิ์กับเจ้าของข้อมูลส่วนบุคคล สร้างมาตรฐานการรักษาข้อมูลส่วนบุคคลให้ปลอดภัย และนำไปใช้ให้ถูกวัตถุประสงค์ตามคำยินยอมที่เจ้าของข้อมูลส่วนบุคคลอนุญาต โดยหลักเกณฑ์หลักๆ คือต้องขอความยินยอมจาก "เจ้าของข้อมูล" ก่อนการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลเสมอ หากไม่ดำเนินการตามหลักของ PDPA ต้องรับโทษร้ายแรงทั้งทางแพ่ง อาญา และปกครอง บุคคลที่ต้องปฏิบัติตามกฎหมาย PDPA ประกอบด้วย เจ้าของข้อมูลส่วนบุคคล (Data Subject) และผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) โดยผู้ควบคุมข้อมูลส่วนบุคคลนั้นเปรียบเสมือนผู้ดูแลระบบ เป็นฝ่ายปฏิบัติงาน มีหน้าที่เก็บรวบรวม และนำข้อมูลส่วนบุคคลที่ขอความยินยอม (Consent) จากเจ้าของข้อมูลไปใช้ ยกตัวอย่างเช่น เว็บไซต์ขายของออนไลน์ ตัวผู้จัดทำเว็บไซต์ก็จะต้องขอข้อมูลทั้งชื่อ ที่อยู่ เบอร์โทรศัพท์ ข้อมูลการจ่ายเงิน เพื่อนำไปดำเนินการสั่งซื้อและจัดส่งสินค้าไปยังที่อยู่ของเจ้าของข้อมูล ซึ่ง PDPA เมื่อได้ข้อมูลมาแล้ว ก็ต้องจัดให้มีมาตรการรักษาความปลอดภัยข้อมูลด้วย

2.5.1.3 พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ฉบับล่าสุดได้มีการประกาศใช้เมื่อเดือนพฤษภาคม พ.ศ.2560 ซึ่งเป็น พ.ร.บ.คอมพิวเตอร์ ฉบับที่ 2 ซึ่งดูแลควบคุม ตั้งแต่การเข้าถึงระบบข้อมูลของผู้อื่นโดยมิชอบ แก้ไข บิดเบียนข้อมูลจนเป็นเหตุให้ผู้อื่นเสียหาย ส่งอีเมล์ spam รบกวนผู้อื่น หรือรบกวนระบบหน่วยงานจนเป็นเหตุให้หน่วยงานมิสามารถทำงานได้ ลักลอบเข้าระบบความมั่นคงของรัฐ นำข้อมูลที่ผิดกฎหมายมาเผยแพร่ ตัวอย่างการกระทำความผิด มาตรา 5 การเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบ เช่น การแฮกเข้าไปดูข้อมูลคอมพิวเตอร์ผู้อื่น การใช้ Username Password ของผู้อื่นโดยไม่ได้รับอนุญาต หรือตัวอย่างบทลงโทษ เช่น มาตรา 7 ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ ทั้งนี้ หน่วยงานหลักที่คอยกำกับดูแลในเชิงนโยบาย คือ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และหน่วยงานในการควบคุมดูแล เช่น สำนักงานตำรวจแห่งชาติ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี สำนักคดีเทคโนโลยีและสารสนเทศสังกัดกรมสอบสวนคดีพิเศษ (DSI) สำนักงานป้องกันและปราบปรามการฟอกเงิน เป็นต้น

2.5.1.4 ประกาศคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่สำคัญในการรับมือภัยคุกคามทางไซเบอร์ ที่ได้ประกาศออกมาบังคับใช้ในปี พ.ศ. 2564 ได้แก่

(1) การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ.2564

(2) ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัย ระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ.2564

(3) การจัดตั้ง หน้าที่และอำนาจของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ พ.ศ.2564

(4) ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564

(5) ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ.2564

(6) การกำหนดระดับความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อแต่งตั้งเป็นพนักงานเจ้าหน้าที่ พ.ศ.2564

จนกระทั่ง ในปี 2566 ได้มีประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ว่าด้วยเรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ.2566 โดยกำหนดให้คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์กำหนดหลักเกณฑ์และวิธีการรายงานเมื่อมีเหตุภัยคุกคามทางไซเบอร์ต่อระบบหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามกำหนดในเอกสาร ก1 ข้อมูลที่ต้องแจ้ง ก2 แบบรายงานภัยคุกคามทางไซเบอร์ และ ก3 แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี โดยประกาศฉบับนี้มีความเชื่อมโยงกับประกาศคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่กล่าวในข้างต้น และให้หน่วยงานที่เกี่ยวข้องถือปฏิบัติเพื่อให้เกิดความชัดเจนในการรายงานเหตุภัยคุกคามทางไซเบอร์ในปัจจุบัน

อนึ่ง การเชื่อมโยงประเทศต่างๆ ในโลกด้วยไซเบอร์สเปซ (Cyber Space) มีผลกระทบในด้านความมั่นคงในระดับนานาชาติมากขึ้นเป็นลำดับ โดยสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU) ได้ให้คำจำกัดความความมั่นคงไซเบอร์ไว้ว่า ความมั่นคงไซเบอร์คือชุดของเครื่องมือ นโยบาย วิธีคิดเกี่ยวกับความมั่นคง แนวทางการรักษาความปลอดภัย วิธีการจัดการความเสี่ยง การลงมือปฏิบัติการฝึกอบรม วิธีปฏิบัติที่เป็นเลิศ การสร้างความเชื่อมั่นและเทคโนโลยีที่สามารถนำมาใช้ปกป้องสิ่งแวดล้อมทางไซเบอร์และทรัพย์สินขององค์กรและผู้ใช้ ทรัพย์สินขององค์กรและผู้ใช้ประกอบไปด้วยอุปกรณ์ที่เชื่อมต่อด้วยคอมพิวเตอร์ บุคลากรโครงสร้างพื้นฐาน แอปพลิเคชัน การให้บริการ ระบบโทรคมนาคมและองค์รวมของข้อมูลที่ถูกส่งผ่านหรือรักษาไว้ในสิ่งแวดล้อมทางไซเบอร์ ความมั่นคงไซเบอร์มุ่งที่จะทำให้ได้มาและรักษาไว้ซึ่งความมั่นคงของทรัพย์สินขององค์กรและผู้ใช้จากความเสี่ยงในสิ่งแวดล้อมทางไซเบอร์ โดยวัตถุประสงค์ด้านความมั่นคงไซเบอร์ประกอบด้วย 1) การรักษาสภาพความพร้อมใช้งานของข้อมูล (Availability) 2) การรักษาความครบถ้วนสมบูรณ์ของข้อมูล (Integrity) ซึ่งรวมถึงการยืนยันตัวตน (Authenticity) และการห้ามปฏิเสธความรับผิดชอบของทั้งผู้รับและผู้ส่งข้อมูล (Non-repudiation) 3) การรักษาความลับของข้อมูล (Confidentiality) (ITU, 2021) ทั้งนี้ ประเทศต่างๆ หันมาให้ความสนใจในการวางยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ให้เป็นยุทธศาสตร์ระดับชาติ เพื่อที่จะสามารถใช้ระบบไซเบอร์ในการขับเคลื่อนเศรษฐกิจและสังคมให้เจริญก้าวหน้าด้วยความเสี่ยงที่น้อยที่สุด ซึ่งประเทศไทยเป็นประเทศหนึ่งที่มีความเจริญก้าวหน้าทางด้านเทคโนโลยีดิจิทัล การสื่อสารโทรคมนาคม และมีการใช้งานเป็นลำดับต้นๆ ของประเทศในภูมิภาคอาเซียน จึงปฏิเสธไม่ได้ว่ามีระดับความเสี่ยงในระดับสูงที่ระบบไซเบอร์ของประเทศจะถูกโจมตีและคุกคามจนเกิดความเสียหายต่อความมั่นคงทางเศรษฐกิจและสังคมของประเทศ

ผู้วิจัยจึงสนใจศึกษาแนวคิดในการจัดทำยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติของต่างประเทศ ที่ได้รับการยอมรับอย่าง The Global Cybersecurity Capacity Centre (GCSCC) แห่ง University of Oxford ประเทศสหราชอาณาจักร โดยตามกรอบแนวคิดแบบจำลองวุฒิภาวะความสามารถด้าน ความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ (National cybersecurity capacity maturity model: CMM) ขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ ประกอบด้วย

มิติที่ 1 National Cybersecurity framework and policy ขีดความสามารถในการพัฒนานโยบาย และยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ ความสามารถในการรับมือกับภัยคุกคามทางไซเบอร์ การบริหารจัดการในภาวะวิกฤต การปกป้องโครงสร้างพื้นฐานที่สำคัญ การเตือนภัยล่วงหน้า การฟื้นฟูหรือซ่อมแซมความเสียหาย รวมถึงความสามารถในการพัฒนานโยบายความมั่นคงที่มีประสิทธิภาพในการป้องกันและทนทานต่อภัยคุกคามไซเบอร์

มิติที่ 2 Cyber culture and society ขีดความสามารถด้านความรู้ความเข้าใจของประชาชนในเรื่องความเชื่อมั่นต่อบริการอินเตอร์เน็ต บริการอิเล็กทรอนิกส์ของภาครัฐ และพาณิชย์อิเล็กทรอนิกส์ และความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลบนโลกออนไลน์ ความเข้าใจของประชาชนในเรื่องความเสี่ยงที่เกี่ยวข้องกับโลกไซเบอร์ต่าง ๆ กลไกการให้ผู้ใช้งานรายงานอาชญากรรมทางไซเบอร์ รวมถึงบทบาทของเครือข่ายสังคมออนไลน์ต่อการเปลี่ยนแปลงทัศนคติ และพฤติกรรมของผู้ใช้งาน

มิติที่ 3 Cybersecurity education, training and skills ขีดความสามารถด้านความตระหนักรู้ (Awareness) ถึงความสำคัญในเรื่องความมั่นคงปลอดภัยไซเบอร์ ตลอดจนการเข้าถึงและคุณภาพของการให้ความรู้และการอบรมด้านความมั่นคงปลอดภัยไซเบอร์ของภาครัฐ ภาคเอกชน และประชาชนทั่วไป

มิติที่ 4 Legal and regulatory frameworks ขีดความสามารถในการออกแบบและบังคับใช้กฎหมาย รวมถึงการตัดสินคดีความที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ทั้งในด้านความมั่นคงด้านเทคโนโลยีสารสนเทศและการสื่อสาร การคุ้มครองข้อมูลส่วนบุคคล และการคุ้มครองความเป็นส่วนตัว (Privacy Protection) ถือว่าเป็นอีกมิติที่มีความจำเป็นต้องพัฒนาเพื่อให้เท่าทันการเปลี่ยนแปลงทางดิจิทัล (Digital Transformation) ที่กำลังเกิดขึ้นและส่งผลกระทบต่อการดำเนินชีวิตของประชาชนทั่วโลก

มิติที่ 5 Standards, organizations, and technologies ขีดความสามารถด้านการใช้เทคโนโลยีที่มีประสิทธิภาพเพื่อรักษาความมั่นคงปลอดภัยด้านไซเบอร์ให้กับประชาชนทั่วไป องค์กร โครงสร้างพื้นฐานของประเทศ มาตรฐานและการถอดบทเรียนจากกรณีศึกษาที่ดีด้านความมั่นคงปลอดภัยทางไซเบอร์ ตลอดจนเทคโนโลยีเพื่อลดความเสี่ยงที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

ส่วนระยะของการกำหนดยุทธศาสตร์ ประกอบด้วย 5 ระยะ ได้แก่ ระยะที่ 1 Start-up เป็นระดับที่เพิ่งเริ่มอภิปรายเกี่ยวกับแนวทาง การสร้างขีดความสามารถ แต่ยังไม่เริ่มดำเนินการ ระยะที่ 2 Formative เป็นระดับที่เริ่มปรากฏแนวทางที่ชัดเจนแล้ว แต่ยังไม่จัดเป็นระเบียบหรือไม่เป็นหมวดหมู่ ระยะที่ 3 Established เป็นระดับที่เริ่มดำเนินการตามแนวทางแล้ว อยู่ในขั้นตอนของการตัดสินใจทางเลือกต่าง ๆ และ จัดสรรทรัพยากร ระยะที่ 4 Strategic เป็นระดับที่มีการจัดลำดับความสำคัญของแนวทางว่า อยู่ในระดับองค์กรหรือในระดับชาติ และระยะที่ 5 Dynamic เป็นระดับที่มีความชัดเจนในด้านกลไกนำไปสู่การเปลี่ยนแปลงยุทธศาสตร์ที่ขึ้นอยู่กับภัยคุกคามไซเบอร์ที่เกิดขึ้นจริงในปัจจุบัน (ปริญญา หอมอเนก, 2562)

ปัญหาความไม่พร้อมในการปกป้อง ป้องกัน รับมือและแก้ไขภัยคุกคามทางไซเบอร์ และ ความไม่พร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ เปรียบเสมือนยอดภูเขาน้ำแข็ง (Tip of the iceberg) ที่ส่วนใหญ่เป็นภัยคุกคามไซเบอร์ทางกายภาพ ซึ่งสามารถรับรู้ได้ชัดเจน ปัญหาความไม่พร้อมในการรับมือปรากฏการณ์ ที่ใช้ในการรุกรานอธิปไตยทางไซเบอร์ (Cyber sovereignty) นั้นเปรียบเสมือนส่วนของภูเขาน้ำแข็งที่จมอยู่ใต้น้ำ (Submerged part of the iceberg) ซึ่งเป็นส่วนที่ใหญ่กว่าการโจมตีทางกายภาพมาก กฎหมายที่เกี่ยวข้อง ได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงยุทธศาสตร์ชาติ 20 ปี ด้านความมั่นคง และยุทธศาสตร์ด้านความมั่นคงไซเบอร์แห่งชาติ (2560-2564) ยังไม่ครอบคลุมทั้ง 5 มิติด้าน ความมั่นคงปลอดภัยไซเบอร์ ตามมิติที่ 2 ของกรอบแนวคิด CMM ในเรื่อง Cyber culture and society ความรู้ความเข้าใจ ความเชื่อมั่นของผู้ใช้บริการเกี่ยวกับการละเมิดและนำข้อมูลส่วนบุคคลไปใช้โดยไม่ได้รับอนุญาตช่องทางการรายงานอาชญากรรมทางไซเบอร์อิทธิพลของ Social media และอธิปไตยไซเบอร์

2.5.2 ความร่วมมือด้านการกำกับดูแลและรับมือภัยคุกคามทางไซเบอร์

องค์การสหประชาชาติ (United Nations: UN) ได้เริ่มพัฒนากรอบนโยบายด้านอาชญากรรมทางคอมพิวเตอร์ขึ้นในปี พ.ศ. 2533 และในการประชุมสภาว่าด้วยการป้องกันอาชญากรรมและการปฏิบัติต่อผู้กระทำผิดขององค์การสหประชาชาติ ครั้งที่ 8 ได้มีกำหนดมาตรการเกี่ยวกับอาชญากรรมคอมพิวเตอร์ขึ้น ได้จัดทำคู่มือการป้องกันและควบคุมอาชญากรรมทางคอมพิวเตอร์

(UN manual on the prevention and control of computer-related crime) ออกเผยแพร่ ซึ่งมีเนื้อหาเกี่ยวกับแนวทางการบัญญัติฐานความผิดและกฎหมายวิธีพิจารณาความที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ รวมไปถึงกลไกความร่วมมือระหว่างประเทศ และที่ประชุมของสมัชชาใหญ่แห่งองค์การสหประชาชาติเมื่อวันที่ 4 ธันวาคม พ.ศ. 2543 ได้มีออกข้อมติที่ 55/63 เกี่ยวกับอาญากรรมทางคอมพิวเตอร์ เพื่อการรับมือกับการใช้งานเทคโนโลยีข้อมูลข่าวสารในทางที่ผิดของอาชญากร โดยมีเนื้อหาดังนี้ 1) รัฐควรทำให้แน่ใจว่ามีกฎหมายและการดำเนินการเพื่อทำลายแหล่งหลบภัยของผู้ซึ่งกระทำผิดโดยอาศัยเทคโนโลยีข้อมูลข่าวสารเป็นเครื่องมือและ 2) ระบบยุติธรรมควรคุ้มครองความลับ ความสมบูรณ์ และสภาพพร้อมใช้งานของข้อมูลและระบบคอมพิวเตอร์ จากการเข้ามาสร้างความเสียหายโดยไม่ได้รับอนุญาต และรับรองว่าการกระทำผิดของอาชญากรต้องได้รับการลงโทษนอกจากนี้ข้อมติที่ 56/121 ของที่ประชุมของสมัชชาใหญ่แห่งองค์การสหประชาชาติก็ได้เชิญชวนให้ประเทศสมาชิกนำเอางานและผลสัมฤทธิ์ของคณะกรรมการป้องกันอาชญากรรมและกระบวนการทางอาญาขององค์การสหประชาชาติ มาใช้เพื่อประกอบการพิจารณาด้วยเมื่อประเทศสมาชิกจะมีออกกฎหมายนโยบาย หรือแนวทางปฏิบัติระดับชาติในการรับมือกับการใช้ข้อมูลข่าวสารเพื่อกระทำผิดของอาชญากร

จากการประชุมระดับโลกว่าด้วยเรื่องสังคมข้อมูลข่าวสาร ครั้งที่ 1 (World Summit on Information Society: WSIS) ในเดือนธันวาคม พ.ศ.2546 ณ กรุงเจนีวา ประเทศสวิสเซอร์แลนด์ และครั้งที่ 2 ในเดือนมิถุนายน พ.ศ.2548 ณ กรุงตูนิส ประเทศตูนีเซีย คณะทำงานเรื่องการกำกับดูแลอินเตอร์เน็ต (The Working Group on Internet Governance: WGIG) ได้นำเสนอรูปแบบกลไกทางกฎหมายที่เหมาะสมสำหรับการกำกับดูแลอินเตอร์เน็ต โดยมุ่งเน้นประเด็นทางกฎหมายเกี่ยวกับกระบวนการและวิธีการสำหรับการกำกับดูแลอินเตอร์เน็ตภายใต้กรอบกฎหมายภายในประเทศและกฎหมายระหว่างประเทศ ซึ่งประเด็นที่นำเสนอดังกล่าว ได้แก่ กระบวนการมีส่วนร่วมของผู้มีส่วนได้เสีย (Stakeholders) ในการกำกับดูแลอินเตอร์เน็ต เครื่องมือทางกฎหมายระหว่างประเทศที่เหมาะสมในการกำกับดูแลอินเตอร์เน็ต ตลอดจนความสัมพันธ์ระหว่างกฎหมายระหว่างประเทศแผนกคดีเมืองและแผนกคดีบุคคลภายใต้กรอบการกำกับดูแลอินเตอร์เน็ตปัจจุบันนี้มุมมองเกี่ยวกับกลไกทางกฎหมายที่เหมาะสมในการกำกับดูแลอินเตอร์เน็ตแบ่งออกเป็น 2 กระบวนทัศน์ (Paradigms) ได้แก่ 1. กระบวนทัศน์ในทางบวก (Techno-optimism) ผู้สนับสนุนกระบวนทัศน์นี้สนับสนุนพัฒนาการของกฎหมายไซเบอร์ (Cyber law) โดยเห็นว่าอินเตอร์เน็ตเป็นวิธีการสื่อสารสมัยใหม่

และไร้พรหมแดน ทำให้เกิดอุปสรรคต่อกฎหมายที่บังคับใช้อยู่ ฉะนั้นกฎหมายไซเบอร์จึงมีความจำเป็นอย่างยิ่งและต้องการการพัฒนาที่ต่อเนื่อง 2. กระบวนทัศน์เทคโนตามความเป็นจริง (Techno-realist) ผู้สนับสนุนกระบวนทัศน์นี้เห็นว่าอินเตอร์เน็ตไม่ได้แตกต่างจากเทคโนโลยีการสื่อสารที่มีมาก่อน เช่น โทรศัพท์ เพียงแต่อินเตอร์เน็ตมีความสะดวกและรวดเร็วกว่าและครอบคลุมระยะทางได้กว้างขวางกว่าเท่านั้น ฉะนั้นกฎหมายที่บังคับอยู่ในปัจจุบันจึงนำมาใช้กับอินเตอร์เน็ตได้ (ชูเกียรติ น้อยฉิม และวรณัฐ บุญเจริญ, 2557)

อย่างไรก็ตาม แนวโน้มความเสี่ยงของภัยคุกคามไซเบอร์ (Cyber Threat) ที่มีต่อเศรษฐกิจของโลกในระดับต้นๆ ก็มีการนำเสนอไว้ในหลายรายงาน เช่น รายงานของ World Economic Forum ที่มีการสำรวจตั้งแต่ปี พ.ศ.2555-2560 พบว่าลำดับความสำคัญของภัยคุกคามไซเบอร์ที่มีต่อเศรษฐกิจของโลกอยู่ในระดับ Top 5 มาโดยตลอด (เอซิสออนไลน์, 2564) การรักษาความมั่นคงปลอดภัยไซเบอร์ จึงจำเป็นต้องใช้มาตรการทั้งทางเทคนิคและทางกฎหมาย ซึ่งในปัจจุบันประเทศไทยได้มีการตราพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ขึ้นบังคับใช้ ซึ่งมีสาระสำคัญตามมาตรา 62(1) ว่าด้วยข้อพิจารณาจากคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ คาดการณ์ว่าจะเกิดภัยคุกคามทางไซเบอร์ที่แบ่งประเภทของภัยคุกคามได้เป็น 3 ระดับ คือระดับไม่ร้ายแรง ระดับร้ายแรง และระดับวิกฤติ แต่พระราชบัญญัติ (พ.ร.บ.) ฉบับนี้กลับมิได้กล่าวถึงการดำเนินการใดๆเพื่อประโยชน์ในการวิเคราะห์สถานการณ์และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง อีกทั้งกำหนดให้พนักงานเจ้าหน้าที่ดำเนินการ โดยมีหนังสือขอความร่วมมือจากบุคคลที่เกี่ยวข้องเพื่อให้ข้อมูลหรือให้ข้อมูลเป็นหนังสือเกี่ยวกับภัยคุกคามทางไซเบอร์ จึงมีข้อพิจารณาว่าถ้อยคำที่ใช้คำว่า “ขอความร่วมมือ” นั้น บุคคลหรือหน่วยงานโดยเฉพาะเอกชนที่ได้รับหนังสือจะสามารถปฏิเสธการให้ความร่วมมือดังกล่าวได้หรือไม่ เพราะการใช้คำว่าขอความร่วมมือไม่ควรเป็นมาตรการบังคับให้บุคคลใดต้องปฏิบัติตามโดยเคร่งครัด อีกทั้งยังกำหนดโทษสำหรับผู้ไม่ให้ความร่วมมือด้วย ซึ่งการใช้คำว่าขอความร่วมมือ ควรนำมาใช้มาตรการที่นำมาใช้กรณีภัยคุกคามในระดับไม่ร้ายแรงจะเหมาะสมและสมเหตุสมผลกว่านำมาใช้กับกรณีภัยคุกคามในระดับร้ายแรง

อนึ่ง พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ของประเทศไทย และกฎหมายว่าด้วยความปลอดภัยไซเบอร์ ค.ศ.2018 (The Cyber Security Act 2018) ของ

สาธารณรัฐสิงคโปร์มีข้อแตกต่างประการหนึ่ง คือ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 62 ประกอบมาตรา 61 มิได้กล่าวถึงการดำเนินการเพื่อประโยชน์ในการวิเคราะห์สถานการณ์และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง โดยมีการกำหนดมาตรการขอความร่วมมือจากบุคคลที่เกี่ยวข้อง เพื่อมาให้ข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ภายในระยะเวลาที่เหมาะสม ขณะที่กฎหมายว่าด้วยความปลอดภัยไซเบอร์ของสาธารณรัฐสิงคโปร์ มีการกำหนดเกี่ยวกับการดำเนินการเพื่อประโยชน์ในการวิเคราะห์สถานการณ์และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์เป็น 3 ระดับอย่างชัดเจน โดยในกรณีของภัยคุกคามที่ไม่ร้ายแรง ผู้เกี่ยวข้องมีสิทธิที่จะปฏิเสธการให้ความร่วมมือกับพนักงานเจ้าหน้าที่ได้ในบางกรณี กล่าวคือ ไม่จำเป็นต้องเปิดเผยข้อมูลใดๆที่เป็นสิทธิ์ หรืออภิสิทธิ์ หรือความคุ้มกันที่ได้รับ หรือภาระผูกพันใด ภายใต้กฎหมายที่บัญญัติคุ้มครองการเปิดเผยข้อมูล ยกเว้นมีการตกลงกันไว้ในข้อสัญญา จึงไม่อาจนำมาอ้างที่จะไม่เปิดเผยข้อมูลดังกล่าวได้ (กัลยา ชินาธิวร, 2562)

ทว่า การใช้อำนาจของคณะกรรมการในกรณีของภัยคุกคามทางไซเบอร์ระดับร้ายแรง และในกรณีเป็นภัยคุกคามทางไซเบอร์ระดับฉุกเฉินหรือวิกฤติ มีการบังคับใช้กฎหมายที่แตกต่างกันตามระดับความร้ายแรง แสดงให้เห็นถึงความสอดคล้องเหตุการณ์ที่เกิดขึ้นกับขอบเขตการใช้อำนาจของเจ้าหน้าที่ ทำให้เห็นว่ากฎหมายของสาธารณรัฐสิงคโปร์มีความเหมาะสมและบัญญัติได้สอดคล้องกับสถานการณ์ของภัยคุกคามทางไซเบอร์มากกว่ากฎหมายไทย เมื่อพิจารณาแนวคิดเกี่ยวกับการควบคุมและตรวจสอบการใช้อำนาจรัฐ ซึ่งมีหลักการสำคัญเกี่ยวข้องประการหนึ่งคือ การคุ้มครองสิทธิและเสรีภาพของประชาชนจากการใช้อำนาจของคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ โดยการออกคำสั่งอย่างใดอย่างหนึ่ง ต้องคำนึงถึงสิทธิและเสรีภาพของประชาชนเป็นหลัก โดยให้ส่งผลกระทบต่อประชาชนเท่าที่จำเป็นและน้อยที่สุด ดังนั้น การใช้อำนาจในการขอความร่วมมือหรือการสั่งให้บุคคลที่เกี่ยวข้องเพื่อมาให้ข้อมูลหรือให้ข้อมูลเป็นหนังสือจึงต้องสอดคล้องกับระดับของภัยคุกคามทางไซเบอร์ที่เกิดขึ้นด้วย (สำนักงานเลขาธิการวุฒิสภา, 2561)

จากการศึกษาแนวคิดในการพัฒนายุทธศาสตร์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และแนวปฏิบัติที่ดี (Best Practice) ของต่างประเทศ พบว่า โครงสร้างยุทธศาสตร์ของประเทศให้ความสำคัญกับวิสัยทัศน์และบทบาทผู้นำ ซึ่งเป็นปัจจัยแห่งความสำเร็จที่จะจุดประกายให้ทุกภาคส่วนมีการบูรณาการ ประสานความร่วมมือ (Inclusiveness) ความเข้าใจต่อปัญหา

ประเภท แหล่งที่มาของภัยคุกคาม การปกป้องโครงสร้างพื้นฐานและบริการที่สำคัญยิ่งยวดของประเทศ การบริหารจัดการความเสี่ยงและการเตือนภัยล่วงหน้า การแลกเปลี่ยนข้อมูลภัยคุกคามไซเบอร์ทั้งภายในและภายนอกประเทศ การเพิ่มขีดความสามารถและความตระหนักรู้ (Awareness) ให้กับประชาชนและบุคลากรภาครัฐ โดยเฉพาะในเรื่องของข้อบัญญัติกฎหมายและการบังคับใช้กฎหมาย การฝึกซ้อมแผนรับมือ การรักษาสมดุลระหว่างความมั่นคงปลอดภัยและเสรีภาพของประชาชน รวมถึงการวิจัยและพัฒนานวัตกรรมด้านเทคโนโลยีดิจิทัลเพื่อรับมือกับภัยคุกคามทางไซเบอร์

2.5.3 การจัดการภัยคุกคามทางไซเบอร์ของประเทศไทย

ประเทศไทยมีการกำหนดมาตรการด้านความมั่นคงปลอดภัยเอาไว้ในกฎหมายที่เกี่ยวข้อง รวมทั้งมีแนวนโยบายระดับชาติฉบับแรกของไทยในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ คือ ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560-2564 (National Cyber security Strategy 2017 – 2021) โดยสำนักงานสภาความมั่นคงแห่งชาติ หรือ สมช. เพื่อให้สอดรับกับสภาพสังคมที่จะเข้าสู่ยุคดิจิทัลอย่างเต็มรูปแบบในอนาคต ซึ่งเป้าหมายหลักของยุทธศาสตร์ฯ ฉบับนี้ คือการสร้างความพร้อมของไทยในการรับมือกับภัยคุกคามทางไซเบอร์อย่างครอบคลุมรอบด้านมากที่สุดเท่าที่สภาวะแวดล้อมเอื้ออำนวย เพื่อเพิ่มขีดความสามารถของไทยที่มีอยู่แล้วให้เข้มแข็งยิ่งขึ้น โดยมุ่งเน้นการมีกลไกกลางในการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ การปกป้องโครงสร้างสาธารณูปโภคพื้นฐาน การสร้างความตระหนักในทุกภาคส่วนและความร่วมมือกับต่างประเทศ โดยให้ความสำคัญในด้านมาตรการป้องกันหรือลดความเสี่ยง สร้างผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยและการกำหนดฐานความผิดและบทลงโทษ ซึ่งอาจครอบคลุมเพียงบางมิติของการรักษาความมั่นคงปลอดภัยทางไซเบอร์เท่านั้น จึงยังจำเป็นต้องยกระดับความเข้มแข็งเพื่อเตรียมความพร้อมของประเทศด้านดังกล่าวให้ครอบคลุมถึงมิติของการเฝ้าระวังภัยคุกคาม หรือการดำเนินการใดๆที่จำเป็นเมื่อมีการโจมตี หรือเมื่อเกิดวิกฤติต่อความมั่นคงปลอดภัยทางไซเบอร์ ตลอดจนการกำหนดมาตรการในการทำงานร่วมกันระหว่างหน่วยงานที่เกี่ยวข้อง เมื่อต้องเผชิญกับการโจมตี หรือภาวะวิกฤติดังกล่าวที่อาจส่งผลกระทบอย่างมีนัยสำคัญและรุนแรง อันส่งผลกระทบต่อความมั่นคงของประเทศในภาพรวม (สำนักงานสภาความมั่นคงแห่งชาติ, 2561)

2.5.3.1 การจัดการกับภัยคุกคามทางไซเบอร์ด้านกฎหมาย

หน่วยงานที่ดูแลด้านความมั่นคงทางไซเบอร์ได้รับการวางกรอบการทำงานตั้งแต่ยุทธศาสตร์ชาติและแผนแม่บทภายใต้ยุทธศาสตร์ชาติประเด็นด้านความมั่นคง พ.ศ.2561 – 2580 ที่เป็นกรอบการดำเนินการด้านความมั่นคงทางไซเบอร์ของประเทศไทยผ่านยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560 – 2564 (National Cybersecurity Strategy 2017 – 2021) ซึ่งเป็นแนวนโยบายระดับชาติฉบับแรกของไทยในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยมีเป้าหมายหลักคือการสร้างความพร้อมของไทยในการรับมือกับภัยคุกคามทางไซเบอร์อย่างครอบคลุมรอบด้านมากที่สุดเท่าที่สภาวะแวดล้อมเอื้ออำนวย โดยมุ่งเน้นให้มีกลไกกลางในการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติการปกป้องโครงสร้างพื้นฐานสำคัญ การสร้างความตระหนักในทุกภาคส่วน และการสร้างความร่วมมือกับต่างประเทศ และการจัดทำพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (ราชกิจจานุเบกษา, 2562) การตั้งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ(กมช.) คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์(กกม.) และสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ(สกมช.) เพื่อสนับสนุนการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ให้มีประสิทธิภาพมากยิ่งขึ้น

2.5.3.2 การจัดการกับภัยคุกคามทางไซเบอร์ของหน่วยงานพลเรือน

หากจะทำการวิเคราะห์ถึงการดำเนินการเกี่ยวกับการจัดการกับภัยคุกคามทางไซเบอร์ของหน่วยงานพลเรือนในประเทศไทยนั้นอาจกล่าวได้ว่าประเทศไทยนั้น นับว่ามีความพร้อมในระดับหนึ่งสำหรับการป้องกันภัยคุกคามทางไซเบอร์ในระดับต้นหรือปานกลางโดยที่ภัยคุกคามทางไซเบอร์ในระดับต้น (Low Level Threat) ที่เป็นภัยคุกคามที่เกิดขึ้นจากการกระทำของบุคคลหรือกลุ่มบุคคลที่มีจุดมุ่งหมายของการดำเนินการเพื่อตอบสนองความต้องการส่วนตัว และภัยคุกคามทางไซเบอร์ระดับปานกลาง (Medium Level Crime) คือการกระทำทางไซเบอร์โดยบุคคลหรือกลุ่มบุคคลที่ผ่านการวางแผนไว้เป็นอย่างดี โดยอาจเป็นการกระทำของกลุ่มก่อการร้ายที่มีความต้องการที่จะสร้างความเสียหายให้แก่รัฐในระดับที่ไม่รุนแรงมากนัก (Bucci, 2012) ซึ่งภัยคุกคามทางไซเบอร์รูปแบบดังกล่าวเป็นลักษณะของภัยคุกคามทางไซเบอร์ที่ประเทศไทยเคยประสบมาแล้ว โดยเฉพาะอย่างยิ่งภัยคุกคามทางไซเบอร์ในระดับต้นที่สามารถพบเห็นได้อยู่บ่อยครั้ง ลักษณะของภัยคุกคามทางไซเบอร์ทั้งสอง

ลักษณะที่กล่าวไปข้างต้น เป็นสิ่งที่หน่วยงานด้านความมั่นคงของประเทศไทยสามารถดำเนินการป้องกันได้อย่างมีประสิทธิภาพ โดยในระยะแรกมีการดำเนินการจากหน่วยงานในกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และเมื่อมี พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ขึ้นมา จึงได้มีการโอนอำนาจหน้าที่ด้านความมั่นคงทางไซเบอร์ให้กับหน่วยงานตามกฎหมายต่อไป

สำหรับในปี พ.ศ. 2562 ได้มีการจัดตั้งหน่วยงานในการดูแลรักษาความมั่นคงทางไซเบอร์ตาม พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยมีวัตถุประสงค์เพื่อกำหนดนโยบาย มาตรการแนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานภาครัฐและภาคเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ไม่ให้เกิดผลกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ รวมทั้งให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ(สกมช.) เป็นหน่วยงานรับผิดชอบงานตามพระราชบัญญัติและประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์ที่เป็นภัยต่อความมั่นคงอย่างร้ายแรง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2563) ในส่วนบทบาทของสำนักงานสภาความมั่นคงแห่งชาติ(สมช.) เกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์นั้น สมช. เป็นหน่วยรับผิดชอบหลักในการจัดทำยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560 – 2564 ซึ่งได้มีการขยายระยะเวลาถึงปี พ.ศ. 2565 เพื่อให้สอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติอีกทั้งได้รับมอบหมายให้ปฏิบัติหน้าที่หน่วยงานกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CIIs) ด้านความมั่นคงของรัฐ (Security Regulator) และเป็นหน่วยงานหลักในการบริหารจัดการภัยคุกคามทางไซเบอร์ในระดับวิกฤต (Cyber Threat Crisis Level) ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

2.5.3.3 การจัดการกับภัยคุกคามทางไซเบอร์ของหน่วยงานทหาร

กองทัพเป็นตัวแสดงหลักที่มีความสำคัญในการจัดการกับภัยคุกคามทางไซเบอร์ของประเทศไทย เนื่องจากกองทัพเป็นหน่วยงานที่มีหน้าที่ในการกำกับดูแล ประเด็นที่มีความเกี่ยวข้องกับความมั่นคง โดยเฉพาะอย่างยิ่งความมั่นคงที่อาจส่งผลกระทบต่อความมั่นคงในภาพรวมของรัฐได้ด้วยเหตุนี้จึงเป็นสาเหตุที่ทำให้ภารกิจการดำเนินงานเกี่ยวกับเรื่องความมั่นคงทางไซเบอร์ของหน่วยงานกองทัพที่ดูมีความชัดเจนมากกว่าหน่วยงานพลเรือนอย่างไรก็ตามอ้างอิงจากวัตถุประสงค์การ

ดำเนินงานที่มีความเกี่ยวข้องกับการจัดการภัยคุกคามทางไซเบอร์จะได้เห็นว่าหน่วยงานภายใต้สังกัดกองทัพจะให้ความสำคัญไปที่ประเด็นหลัก คือ การรักษาความมั่นคงภายในองค์กร (ฤทธี อินทราวุธ, 2557) การดำเนินงานในส่วนนี้เป็นความพยายามของกองทัพในการที่จะรักษาความมั่นคงของฐานข้อมูล เว็บไซต์รวมถึงพื้นที่ทางไซเบอร์ของกองทัพให้มีความปลอดภัย ปราศจากการเจาะเข้าระบบจากภายนอก และการรักษาความมั่นคงของสถาบันหลักของชาติซึ่งประเด็นนี้จะถูกให้ความสำคัญมากเป็นพิเศษกว่าประเด็นอื่น โดยอาจมีสาเหตุมาจากอุดมการณ์ของกองทัพที่จะปกป้องสถาบันหลักของชาติ

ในการรักษาความมั่นคงด้านไซเบอร์ในประเทศนั้น กองทัพอาจมองว่าเป็นหน้าที่ของกองทัพที่ต้องเป็นหน่วยรับผิดชอบในการดำเนินการและกองทัพไทยได้มีปฏิบัติการในด้านความมั่นคงทางไซเบอร์ต่างๆซึ่งเป็นการปฏิบัติงานที่ข้ามขอบเขตของหน่วยงานพลเรือน เช่น กระทรวงดิจิทัลฯ หรือ สกมช. ในกรณีนี้กองทัพได้อ้างถึงประเด็นการรักษาความมั่นคงของประเทศ เพื่อสร้างความชอบธรรมในการดำเนินการด้านความมั่นคงทางไซเบอร์อย่างไรก็ตาม มุมมองที่หน่วยงานทางทหารมีต่อประเด็นการรักษาความมั่นคงทางไซเบอร์มีความแตกต่างจากหน่วยงานพลเรือนอยู่ค่อนข้างมาก เนื่องจากหน่วยงานทางทหารจะมีการให้ความสำคัญกับการดำเนินการจัดการกับภัยคุกคามภายในประเทศเป็นหลัก ในขณะที่หน่วยงานพลเรือนจะให้ความสำคัญกับภัยคุกคามที่มาจากภายนอกประเทศ และมองว่าภัยคุกคามจากนอกประเทศเป็นอันตรายและส่งผลกระทบมากกว่าภัยคุกคามจากภายในประเทศ

จากการวิเคราะห์ผลลัพธ์การดำเนินการจัดการภัยคุกคามทางไซเบอร์ ผู้วิจัยสนใจว่า ประเทศไทยมีการจัดการดูแลด้านความมั่นคงทางไซเบอร์ในหลากหลายมิติโดยผลลัพธ์จากการจัดการทางไซเบอร์นั้นหน่วยงานที่เกี่ยวข้องกับชีวิตประจำวันของประชาชนได้มีการป้องกันการเจาะข้อมูลการฝึกอบรมต่างๆ ที่เกี่ยวข้องกับการป้องกันทางไซเบอร์และในด้านหน่วยทางทหารได้มีการฝึกอบรมและทำระบบป้องกันทางไซเบอร์แต่ในสังคมกลับไม่สามารถรับรู้ได้ถึงระบบป้องกันหรือการป้องกันได้อย่างชัดเจน ซึ่งภาครัฐได้มองว่าพื้นที่ทางไซเบอร์จำเป็นจะต้องได้รับการปกป้องกลายมาเป็นประเด็นด้านความมั่นคงตามแนวคิดของการทำให้เป็นความมั่นคง (Securitization) อย่างไรก็ตามประเทศไทยยังมีความพร้อมในการรับมือกับภัยความมั่นคงทางไซเบอร์ที่ยังไม่เพียงพอเนื่องจากยังขาดผู้เชี่ยวชาญด้านไซเบอร์โดยมีสาเหตุมากจาก 1) ค่าตอบแทนที่ไม่มากพอ 2) การโดนภาคเอกชนดึงตัวไปทำงาน 3) ความก้าวหน้าทางอาชีพที่ไม่ชัดเจน และ 4) บุคลากรด้านไซเบอร์ขาดแคลนทั่วโลก ถึงแม้ว่า

จะมีการอบรมในเรื่องของความมั่นคงทางไซเบอร์แต่ความเชี่ยวชาญของผู้ที่ทำงานในหน่วยงานดังกล่าวก็ยังมีไม่เพียงพอในการจัดการความมั่นคงทางไซเบอร์ทั้งหมดของประเทศไทย

2.5.4 มาตรฐานและกรอบการดำเนินงานการรักษาความมั่นคงปลอดภัยไซเบอร์

2.5.4.1 กรอบการดำเนินงาน NIST Cybersecurity Framework

แนวโน้มในอนาคตภัยคุกคามด้านไซเบอร์ นับวันจะทวีความเข้มข้นและความรุนแรงมากขึ้นตามลำดับ ทั้งนี้เป็นผลมาจากความเจริญก้าวหน้าด้านการพัฒนาเทคโนโลยีสารสนเทศและการสื่อสาร องค์กรหลายแห่งกำลังถูกคุกคามอย่างต่อเนื่องจากการโจมตีทางไซเบอร์ ซึ่งหลายคนอาจมองว่าเป็นภัยที่ไกลตัว รัฐบาลสหรัฐอเมริกา ได้ตระหนักถึงความสำคัญของภัยคุกคามด้านไซเบอร์ดังกล่าว จึงได้มอบหมายให้สถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (National Institute of Standards and Technology ; NIST) ทำการพัฒนากรอบดำเนินงานเพื่อปรับปรุงความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานระบบโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure Security) เพื่อให้เป็นแนวทางและมาตรฐาน ซึ่งครอบคลุมทั้งในระดับนโยบาย (Policy) การจัดการองค์กร (Organization) และเทคโนโลยี (Technology) เพื่อบริหารจัดการความเสี่ยงทางไซเบอร์ (Cyber Risk Management) ที่มีผลกระทบกับหน่วยงานได้อย่างเหมาะสม โดยกำหนดกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ (Framework Core) เพื่อนำมาใช้ในการดำเนินการร่วมกัน ประกอบด้วย กลุ่มหน้าที่งาน (Functions) เป็นกิจกรรมพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์ในระดับภาพรวม จำแนกเป็น 5 Functions (IPDRR : Identify, Protect, Detect, Respond, Recover) โดยจะเห็นปรากฏอยู่ในมาตรา 13 ของ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ของประเทศไทย

ภาพที่ 6 NIST Cybersecurity Framework หรือเรียก NIST CSF Version 1.1
ที่มา: (NIST, 2021)

จากกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity framework) ของสถาบันมาตรฐานและเทคโนโลยี (NIST) เป็นหนึ่งในกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งเป็นที่นิยมใช้อย่างมากในปัจจุบัน ไม่เพียงแค่องค์กรในประเทศสหรัฐอเมริกาเท่านั้น framework ดังกล่าวยังเป็นที่แพร่หลายไปยังทุกภูมิภาคทั่วโลก รวมไปถึงประเทศไทย หลายองค์กรเริ่มนำ Framework นี้ประยุกต์ใช้เพื่อรับมือกับภัยคุกคามไซเบอร์ Framework นี้รวบรวมเอาแนวปฏิบัติที่ดีที่สุดอันหลากหลายเข้าไว้ด้วยกัน เพื่อช่วยให้ธุรกิจองค์กรสามารถกำหนดแนวทางบังคับใช้งาน และปรับปรุงแนวทางการรักษาความมั่นคงปลอดภัย รวมถึงมีภาษากลางสำหรับใช้ในการสื่อสารประเด็นปัญหาต่าง ๆ ที่เกิดขึ้นระหว่างผู้ที่เกี่ยวข้องได้อย่างมีประสิทธิภาพ โดย Framework นี้นำเสนอหลักการและแนวทางปฏิบัติที่ดีที่สุดของการบริหารจัดการความเสี่ยง เพื่อยกระดับความมั่นคงปลอดภัยขององค์กรทุกระดับ รวมไปถึงช่วยให้องค์กรสามารถวางแผนป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและเป็นระบบ ในขณะที่ธุรกิจยังคงดำเนินต่อไปได้อย่างเนื่อง

หัวใจสำคัญของ Framework แบ่งออกเป็น 5 ขั้นตอนที่สำคัญ ได้แก่

(1) การระบุความเสี่ยง (Identity) เป็นขั้นตอนแรกในการศึกษาทำความเข้าใจบริบท ทรัพยากร และกิจกรรมงานสำคัญ เพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มีต่อระบบ ทรัพย์สิน ข้อมูล และขีดความสามารถ

(2) การป้องกันความเสี่ยง (Protect) เป็นการจัดทำและดำเนินการตามมาตรการป้องกันที่เหมาะสมสำหรับการให้บริการโครงสร้างพื้นฐานสำคัญ โดยมีวัตถุประสงค์เพื่อจำกัดระดับผลกระทบของเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ครอบคลุมการฝึกอบรมและการสร้างความตระหนัก มาตรการควบคุมการเข้าถึง และมาตรการด้านความมั่นคงปลอดภัยต่าง ๆ ทั้งกระบวนการและวิธีปฏิบัติ ตลอดจนเทคโนโลยี

(3) การตรวจสอบและเฝ้าระวัง (Detect) เป็นการจัดทำและดำเนินกิจกรรมเพื่อตรวจหาเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น ครอบคลุมถึงกระบวนการเฝ้าระวังหรือตรวจติดตามต่อเนื่อง

(4) การตอบสนอง (Respond) เป็นการจัดทำและดำเนินกิจกรรมเพื่อตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ ครอบคลุมถึงการวางแผนรับมือ การสื่อสาร การวิเคราะห์ การลดความเสี่ยง และการปรับปรุง

(5) การคืนสภาพ (Recovery) เป็นการจัดทำและดำเนินกิจกรรมตามแผนงาน เพื่อรองรับการดำเนินงานต่อเนื่อง รวมถึงแผนการกู้คืนทั้งด้านขีดความสามารถและบริการให้ได้ตามที่กำหนด

เมื่อองค์กรสามารถใช้ทั้ง 5 ขั้นตอนนี้ได้อย่างเหมาะสม โดยการกำหนดผลลัพธ์ที่ต้องการ และกรอบปฏิบัติที่อ้างอิงสำหรับการดำเนินงานเพื่อบรรลุตามวัตถุประสงค์ของแต่ละอุตสาหกรรม/โครงสร้างพื้นฐาน จะช่วยให้องค์กรเข้าใจ และ จัดทำโครงงานและระบบด้าน Cybersecurity ได้อย่างมีประสิทธิภาพมากขึ้น (ปริญญา หอมอเนก, 2561)

นอกจากนี้ โครงสร้างหลักของกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญ (Framework Core) ตามกรอบการดำเนินงาน Cybersecurity Framework นี้ ยังสามารถแบ่งรายละเอียดลงไปในแต่ละหัวข้อของทั้ง 5 Function เพื่อเชื่อมโยงข้อมูลอ้างอิง (Informative references) ซึ่งได้แก่ มาตรฐาน แนวปฏิบัติ หรือข้อกำหนดอื่นๆ ที่สามารถนำมาประยุกต์ใช้ในแต่ละ Function โดยไม่เพียงครอบคลุมการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์สำหรับระบบเทคโนโลยีสารสนเทศ แต่ยังมุ่งเน้นที่ระบบควบคุมอุตสาหกรรม (Industrial Control System: ICS) ซึ่งมีผลกระทบในวงกว้างมากกว่า ทำให้ผู้ใช้ในกลุ่มหน่วยงานระบบโครงสร้างพื้นฐานสำคัญจะได้รับประโยชน์อย่างเต็มที่ในการใช้กรอบการ

ดำเนินงาน Cybersecurity Framework นี้ ซึ่งได้ประยุกต์และอ้างอิงกับมาตรฐานที่องค์กรส่วนใหญ่ได้ดำเนินการอยู่แล้ว อาทิ CCS CSC (Council on Cybersecurity: 20 Critical Security Controls), COBIT 5, ISA 62443-2-1:2009, ISO/IEC 27001:2013 และ NIST SP 800-53 Rev.4 รวมทั้งกรอบการดำเนินงานด้านไซเบอร์โดย NIST โดยผู้วิจัยจะขอกล่าวถึงมาตรฐานที่มีแนวทางในการกำกับดูแลและการรักษาความมั่นคงปลอดภัยไซเบอร์ที่องค์กรทั่วโลกยอมรับและนำไปใช้ตามแนวปฏิบัติ คือ มาตรฐาน ISO 27001 และมาตรฐานที่มีจำนวนแนวปฏิบัติใกล้เคียงกัน คือ มาตรฐาน COBIT

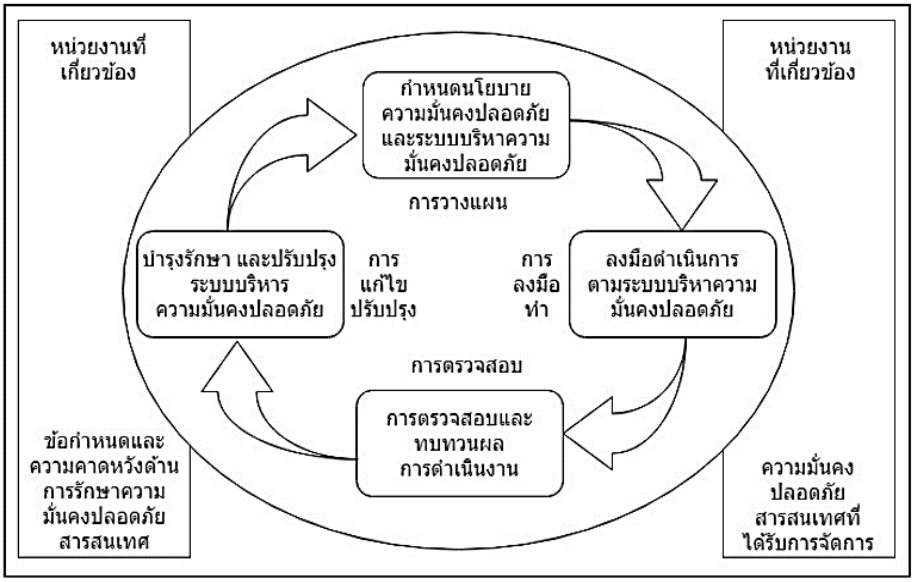
2.5.4.2 มาตรฐานสากล ISO 27001

ISO 27001 ระบบมาตรฐานความมั่นคงปลอดภัยสารสนเทศ ISO 27001 คือมาตรฐานหลักในหมวดระบบมาตรฐานความปลอดภัยสารสนเทศ ซึ่งแนะแนวทางและสนับสนุนให้องค์กรเข้าใจความเสี่ยงและจุดอ่อนด้านการคุ้มครองข้อมูลอย่างเป็นระบบ การดำเนินการให้สอดคล้องกับ ISO 27001 ช่วยเพิ่มความแข็งแกร่งให้กับระบบความปลอดภัยของข้อมูล ลดความเสี่ยง และปกป้องข้อมูลจากการถูกโจรกรรม โดยมาตรฐาน ISO 27001: 2005 คือเวอร์ชั่นแรกได้ถูกประกาศใช้ตั้งแต่ปี พ.ศ. 2548 เป็นมาตรฐานที่มีแนวปฏิบัติที่ได้รับการยอมรับ และนำไปใช้เป็นแนวทางในการรักษาความมั่นคงปลอดภัยไซเบอร์ในองค์กรทั่วโลก ทั้งนี้จากรายงานของ ISMS (Information security management system) พบว่ามีคองค์กรมากกว่า 7,346 แห่ง นำมาตรฐานนี้ไปใช้ โดยในประเทศไทยมีองค์กรที่ผ่านการรับรองมาตรฐานนี้แล้วกว่า 40 แห่ง (ศูนย์ศึกษายุทธศาสตร์, 2557)

ต่อมาประเทศไทยได้นำมาตรฐานสากล ISO/IEC 27001:2013 ซึ่งเป็นเวอร์ชั่นล่าสุด มาใช้ในการบริหารจัดการตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยให้ความสำคัญกับการรักษาความลับของข้อมูลสารสนเทศ (Confidentiality) การรักษาความครบถ้วนสมบูรณ์ของข้อมูลสารสนเทศ (Integrity) และการรักษาสภาพพร้อมใช้งานของระบบ (Availability) ซึ่งเป็นปัจจัยพื้นฐานในการพิจารณาความมั่นคงปลอดภัยทางไซเบอร์โดยอาศัยการประเมินความเสี่ยง (Risk assessment) ที่ข้อมูลสารสนเทศอาจได้รับผลกระทบหรือเกิดความเสียหายจากภัยคุกคามทางไซเบอร์ เช่น ฐานข้อมูลรายชื่อผู้รับบริการของหน่วยงานซึ่งเป็นข้อมูลลับ มีความครบถ้วนสมบูรณ์ และอยู่ในสภาพพร้อมใช้งานตลอดเวลา ซึ่งภัยคุกคามต่อระบบสารสนเทศนั้น

อาจมาจากทั้งทางอิเล็กทรอนิกส์ (Logical) และทางกายภาพ (Physical) ดังนั้นหน่วยงานจึงควรเตรียมการให้สามารถใช้ฐานข้อมูลรายชื่อผู้รับบริการได้แม้มีภัยคุกคามเกิดขึ้น

ระบบมาตรฐาน ISO/IEC 27001:2013 มีการประยุกต์ใช้หลักการ PDCA (Plan- Do -Check- Action) ซึ่งเป็นหลักการสำคัญในการบริหารจัดการที่ใช้กันแพร่หลาย หลักการ PDCA จึงกำหนดมาตรฐานการดำเนินการให้สอดคล้องตามมาตรฐานสากล ISO/IEC 27001:2013 อาทิเช่น การจัดทำนโยบาย กระบวนการ การกำหนดหน้าที่ความรับผิดชอบ การควบคุม การตรวจสอบ การประเมินความเสี่ยง การวางแผนความต่อเนื่องทางธุรกิจ การจัดการเหตุการณ์ที่เกี่ยวข้องกับมั่นคงปลอดภัยได้ ดังภาพที่ 7



ภาพที่ 7 วงจร PDCA สำหรับการรักษาความมั่นคงปลอดภัยสารสนเทศ (วิลาส วิถีไพร, 2561)

โดยประโยชน์ของระบบมาตรฐาน ISO/IEC 27001 มีดังนี้

(1) ปกป้องข้อมูลองค์กร พร้อมใช้ทรัพยากรอย่างมีประสิทธิภาพ

(2) มาตรฐานของระบบจัดการความมั่นคงด้านสารสนเทศ ISO 27001 (ISMS) นำเสนอกรอบการปฏิบัติที่ช่วยองค์กรยกระดับความมั่นคงด้านสารสนเทศ พร้อมกับลดต้นทุนในเวลาเดียวกัน

(3) หากองค์กรได้รับการรับรองมาตรฐาน ISO 27001 อยู่แล้ว และต้องการขยายขอบเขตของระบบ ISMS เดิมให้ครอบคลุมการคุ้มครองข้อมูลส่วนบุคคล การเลือกใช้ ISO 27001 จะเป็นตัวเลือกที่น่าสนใจ เพราะเป็นการขยายกระบวนการ และมาตรการของ ISO 27001 ที่มีอยู่เดิม หรือหากองค์กรต้องการเริ่มต้นในการขอการรับรอง ISO 27001 ก็สามารถดำเนินการจัดทำร่วมกับ ISO 27001 ไปพร้อมกัน ซึ่งถือว่าเป็นประโยชน์แก่องค์กรถึงสองชั้น

2.5.4.3 กรอบการดำเนินงาน COBIT

กรอบการดำเนินงาน COBIT ย่อมาจากคำว่า Control Objectives for Information and Related Technology มีการจัดทำขึ้น โดยสมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ(Information Systems Audit and Control Association) หรือที่เรียกกันอย่างย่อว่า ISACA ตัวกรอบดำเนินงาน COBIT ได้มีเริ่มจัดทำขึ้นมาเป็นครั้งแรกในปี พ.ศ. 2539 ภายใต้ชื่อเรียกว่า First edition of COBIT framework หลังจากนั้นก็ได้มีการพัฒนารูปแบบมาอย่างต่อเนื่องจนกระทั่ง ในปี พ.ศ. 2555 ได้มีการปล่อยตัวรูปแบบที่มีชื่อว่า COBIT 5 ออกมาใช้งานจนได้รับความนิยมอย่างแพร่หลายในระดับสากล ทั้งนี้ ISACA ได้ออกแบบ COBIT 5 โดยมีวัตถุประสงค์หลักเพื่อเป็นแหล่งความรู้สำหรับผู้ประกอบวิชาชีพทาง ด้านการกำกับดูแลไอทีระดับองค์กร (Governance of Enterprise IT -GEIT) การให้ความเชื่อมั่น ความเสี่ยง และการรักษาความมั่นคงปลอดภัย ISACA ไม่ได้อ้างว่าการใช้ข้อมูลใดๆ ใน COBIT 5 จะสามารถรับรองผลสำเร็จ ไม่ควรถือว่าข้อมูลขั้นตอนการปฏิบัติงานและการทดสอบที่จำเป็นทั้งหมดเอาไว้และไม่ควรพิจารณาข้อมูลแยกต่างหากโดยไม่คำนึงถึงข้อมูล ขั้นตอนการปฏิบัติงาน และการทดสอบอื่นๆ ที่พอจะสามารถให้ผลลัพธ์ที่เหมือนกันได้ ในการพิจารณาถึงความเหมาะสมของข้อมูล ขั้นตอนการปฏิบัติงาน หรือการทดสอบใดๆ ควรใช้วิจารณญาณ ด้านวิชาชีพของตนเพื่อพิจารณาถึงการกำกับดูแลไอทีในระดับองค์กร การให้ความเชื่อมั่น ความเสี่ยง และการรักษาความมั่นคงปลอดภัย ในสภาพแวดล้อมของระบบหรือเทคโนโลยีสารสนเทศนั้นๆ

COBIT 5 คือ กรอบการดำเนินงานสำหรับการกำกับดูแลและการบริหารจัดการไอทีหรือเทคโนโลยีสารสนเทศระดับองค์กรในปัจจุบัน ซึ่งบรรจุเนื้อหาที่เป็นกรอบการ

ดำเนินงานที่ใช้สำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร โดยหลักการของกรอบการดำเนินงาน COBIT 5 ถูกกำหนดไว้บนหลักการพื้นฐานสำคัญ 5 ประการ ดังนี้

หลักการที่ 1 ตอบสนองความต้องการของผู้มีส่วนได้เสีย ในส่วนแรก COBIT 5 มีหลักคิดว่าองค์กรแต่ละแห่งล้วนตั้งอยู่ เพื่อที่จะสร้างคุณค่าสำหรับผู้ที่มีส่วนได้เสีย โดยการดำเนินงานจะต้องมีการรักษาความสมดุลระหว่างผลประโยชน์ที่จะได้รับกับความเสี่ยงอันจะเกิดขึ้น ซึ่งกรอบการดำเนินงาน COBIT 5 จะมีส่วนเข้ามาช่วยเสริมสร้างกระบวนการ ที่จำเป็นในการดำเนินงานทั้งหมดรวมไปถึงปัจจัยเอื้ออื่น ๆ ที่ใช้ในการสนับสนุนการสร้างคุณค่าให้แก่ธุรกิจจากการใช้ระบบเทคโนโลยีสารสนเทศ อีกทั้งแต่ละองค์กรล้วนมีวัตถุประสงค์การดำเนินกิจการที่แตกต่างกันออกไป โดยแต่ละองค์กรสามารถนำเอา COBIT 5 ไปปรับแต่งให้มีความเหมาะกับบริบทของตนผ่านทางกระบวนการส่งทอดเป้าหมาย (Goal cascade) ซึ่งจากกระบวนการดังกล่าวจะทำให้เป้าหมายขององค์กรในภาพรวม พึ่งไปไปสู่เป้าหมายในระดับที่สามารถบริหารจัดการได้อย่างมีความเฉพาะเจาะจง

หลักการที่ 2 ครอบคลุมทั่วทั้งองค์กรอย่างครบวงจรกรอบการดำเนินงาน COBIT 5 จะเข้ามาบูรณาการการกำกับดูแลระบบเทคโนโลยีสารสนเทศภายในองค์กร โดยจะเข้ามาช่วยกำกับดูแลครอบคลุมทุกกระบวนการภายในองค์กร COBIT 5 มีหลักคิดที่ว่าระบบเทคโนโลยีสารสนเทศเป็นสินทรัพย์ที่ทุกคนในองค์กรจำเป็นต้องดูแลเช่นเดียวกับสินทรัพย์อื่น ๆ โดยพิจารณาการกำกับดูแลและบริหารจัดการปัจจัยเอื้อที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศทั้งหมด เพื่อให้ครอบคลุมทั่วทั้งองค์กรอย่างครบวงจร

หลักการที่ 3 ประยุกต์ใช้กรอบการดำเนินงานที่บูรณาการเป็นหนึ่งเดียวในปัจจุบันมีหลากหลายองค์กรได้ออกมาตรฐานและแนวปฏิบัติที่ดีที่เกี่ยวข้องกับการกำกับดูแลระบบเทคโนโลยีสารสนเทศอยู่จำนวนมาก ซึ่งแต่ละอย่างก็มีจุดเด่นที่แตกต่างกันในด้านใดด้านหนึ่ง COBIT 5 ได้นำเอามาตรฐานและกรอบการดำเนินงานที่หลากหลากเหล่านั้น มาปรับปรุงจัดเรียงให้สอดคล้องกันในภาพรวม จนสามารถใช้เป็นกรอบการดำเนินงานที่ครอบอยู่เหนือกรอบการดำเนินงานอื่น ๆ สำหรับการกำกับดูแลและการบริหารจัดการระบบเทคโนโลยีสารสนเทศ

หลักการที่ 4 เอื้อให้วิธีปฏิบัติแบบองค์รวมสัมฤทธิ์ผลการกำกับดูแลและการบริหารจัดการระบบเทคโนโลยีสารสนเทศให้มีประสิทธิภาพและประสิทธิผล จะต้องใช้วิธีปฏิบัติแบบองค์รวม โดยการพิจารณาจากองค์ประกอบหลากหลายที่มีปฏิสัมพันธ์ต่อกัน ซึ่งปัจจัยเอื้อที่ใช้สนับสนุนการบริหารจัดการแบบองค์รวม กรอบการดำเนินงาน COBIT 5 ได้มีการระบุถึงปัจจัยเอื้อไว้ 7 ประเภท ดังนี้ (1) หลักการนโยบายและกรอบการดำเนินงาน (2) กระบวนการ (3) โครงสร้างการจัดองค์กร (4) วัฒนธรรม จริยธรรม และพฤติกรรม (5) ระบบสารสนเทศ (6) การบริการโครงสร้างพื้นฐานและระบบงาน (7) บุคลากร ทักษะ และศักยภาพ

หลักการที่ 5 แบ่งแยกการกำกับดูแลออกจากการบริหารจัดการกรอบการดำเนินงานของ COBIT 5 ระบุความแตกต่างอย่างชัดเจนระหว่างการกำกับดูแลและการบริหารจัดการหลักสองประการนี้ครอบคลุมถึงกิจกรรมที่แตกต่างกันจึงต้องการโครงสร้างการจัดองค์กรที่แตกต่างกัน และใช้เพื่อจุดประสงค์ที่แตกต่างกัน ในมุมมองของ COBIT 5 ได้มีการเปรียบเทียบให้เห็นความแตกต่างหลักๆ ที่เห็นเด่นชัดระหว่างการกำกับดูแลและการบริหารจัดการ รายละเอียดตาม

ตารางที่ 3 การเปรียบเทียบความแตกต่างระหว่างการกำกับดูแลและการบริหารจัดการ

การเปรียบเทียบความแตกต่างระหว่างการกำกับดูแลและการบริหารจัดการ	
การกำกับดูแล (Governance)	**การบริหารจัดการ (Management)**
การกำกับดูแลที่ดีจะทำให้มั่นใจได้ว่า ความต้องการ เงื่อนไข และทางเลือกของผู้มีส่วนได้เสียได้รับการประเมิน เพื่อกำหนดวัตถุประสงค์ที่องค์กรต้องการให้บรรลุซึ่งมีความสมดุลและเห็นชอบร่วมกัน การกำหนดทิศทางผ่านการจัดลำดับความสำคัญและการตัดสินใจและการเฝ้าติดตามผลการดำเนินงานและการปฏิบัติตามเทียบกับทิศทางและวัตถุประสงค์ที่ได้ตกลงร่วมกัน	การบริหารจัดการผู้บริหารจะมีการวางแผนการดำเนินงาน และเฝ้าติดตามกิจกรรมต่าง ๆ ให้สอดคล้องกับทิศทางที่กำหนดหน่วยงานการกำกับดูแล(Governance) เพื่อให้บรรลุวัตถุประสงค์ขององค์กร

การเปรียบเทียบความแตกต่างระหว่างการกำกับดูแลและการบริหารจัดการ	
การกำกับดูแล (Governance)	**การบริหารจัดการ (Management)**
ข้อสังเกต ในองค์กรส่วนใหญ่ คณะกรรมการบริหารเป็นผู้รับผิดชอบการกำกับดูแลโดยรวมภายใต้การชี้นำของประธานกรรมการ ในองค์กรขนาดใหญ่และมีความซับซ้อน หน้าที่บางประการสำหรับการกำกับดูแลอาจมอบหมายให้กับหน่วยงานที่จัดตั้งขึ้นเป็นพิเศษในระดับที่เหมาะสม	**ข้อสังเกต** ในองค์กรส่วนใหญ่ การบริหารจัดการรับผิดชอบโดยผู้บริหารระดับสูงภายใต้การชี้นำของประธานเจ้าหน้าที่บริหาร (CEO)

เมื่อนำหลักการทั้ง 5 ประการนี้มารวมกันจะทำให้องค์กรสามารถสร้างกรอบการดำเนินงานสำหรับการกำกับดูแลและการบริหารจัดการที่มีประสิทธิผล ซึ่งส่งผลให้การใช้สารสนเทศและการลงทุนด้านเทคโนโลยีเกิดประโยชน์สูงสุด เพื่อยังประโยชน์ให้กับผู้มีส่วนได้เสีย ทั้งนี้ COBIT 5 ไม่ได้เป็นกฎตายตัว แต่สนับสนุนให้องค์กรนำกระบวนการทางด้านการกำกับดูแลและการบริหารจัดการไปใช้งานให้ครอบคลุมถึงจุดต่างๆที่สำคัญตามที่ได้กล่าวไว้ และมาตรฐานที่องค์กรไม่ควรมองข้ามในปัจจุบันและหลายองค์กรได้นำมาใช้ประกอบการกำกับดูแลในการดำเนินงานด้านเทคโนโลยีดิจิทัลกันมากขึ้น คือ ISO/IEC 38500 เป็นกรอบดำเนินงานที่เกี่ยวเนื่องกับ COBIT 5 และใช้กันมากที่สุดในด้านการกำกับดูแลและแนวปฏิบัติสำหรับผู้บริหารของแต่ละองค์กร และเป็นมาตรฐานการกำกับดูแลเทคโนโลยีสารสนเทศที่ช่วยชี้แนะให้องค์กรต่าง ๆ ทราบถึงกระบวนการและการดำเนินการอย่างเพียงพอในการยกระดับเทคโนโลยีสารสนเทศสู่ระดับกลยุทธ์ และกำหนดวิธีการในการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ ก่อให้เกิดประโยชน์สูงสุด มีความโปร่งใส ตรวจสอบได้ ตอบสนองและรองรับความต้องการด้านเทคโนโลยีสารสนเทศตามสภาพแวดล้อมทางธุรกิจที่เปลี่ยนแปลงไป โดยวัตถุประสงค์ของมาตรฐาน ISO 38500 คือการวางโครงสร้างที่ควรจะเป็นหลักการสำหรับคณะกรรมการบริษัท และผู้บริหารระดับสูงเพื่อใช้ในการ (1) ประเมินผลการใช้เทคโนโลยีสารสนเทศ (2) กำกับทิศทางนโยบายการใช้เทคโนโลยีสารสนเทศให้

บรรลุวัตถุประสงค์ระดับองค์กร (3) ติดตามผลดำเนินงานที่เกิดจริงจากการใช้เทคโนโลยีสารสนเทศต้องเป็นไปตามแผนงานและนโยบาย ตั้งอยู่บนหลักการสำคัญ 6 ประการ ได้แก่ (1) ความรับผิดชอบ (2) กลยุทธ์ (3) การจัดซื้อจัดหา (4) ผลการดำเนินงาน (5) ความสอดคล้องกัน และ (6) พฤติกรรมบุคคล เป็นต้น ซึ่งฝ่ายงานเทคโนโลยีสารสนเทศในแต่ละองค์กร จะต้องมีการปรับตัวให้มีศักยภาพความพร้อม สมรรถนะที่เพิ่มขึ้นอย่างเพียงพอที่จะรองรับงานตาม “IT Governance” ที่อิงตามมาตรฐาน ISO 38500 ซึ่งถือว่าเป็น Requirement เพิ่มเติมในระดับขององค์กร นอกเหนือจาก Requirement ในระดับฝ่ายงาน และเป็น Requirement ที่ครอบคลุมทั้งองค์กร ที่เป็นหลักการใหญ่ที่ระดับหน่วยงานจะต้องปรับตัวตาม (ไอซาก้า, 2012)

อย่างไรก็ดี สิ่งที่ทุกองค์กรควรดำเนินการในลำดับต้นๆ คือ คณะกรรมการระดับสูงต้องกำกับดูแลการพัฒนาเทคโนโลยีดิจิทัลให้มีการบริหารจัดการทรัพยากรเทคโนโลยีดิจิทัลที่เหมาะสมกับบริบทขององค์กร โดยคำนึงถึงความคุ้มค่าของการลงทุนด้านเทคโนโลยีดิจิทัลเป็นสำคัญ รวมถึงต้องมีการกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลที่ครอบคลุมถึงการบริหารจัดการโครงการด้านเทคโนโลยีดิจิทัล การรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ ภัยคุกคามทางไซเบอร์ และการเปลี่ยนแปลงทางเทคโนโลยีดิจิทัลที่มีผลกระทบกับองค์กร รวมถึงตอบสนองต่อความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสียทุกกลุ่ม เช่น หน่วยงานกำกับ ลูกค้า ประชาชนผู้ใช้บริการ เป็นต้น และอีกประการที่สำคัญคือ องค์กรต้องมีการทบทวน การปฏิบัติตาม กฎหมาย ระเบียบข้อบังคับ ที่เกี่ยวข้องกับการพัฒนาเทคโนโลยีดิจิทัลอย่างสม่ำเสมอและครอบคลุมทั้งในส่วนของประเทศไทย และต่างประเทศ เช่น พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล 2562 พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 General Data Protection Regulation (GDPR) ของ EU ข้อตกลงการค้าเสรี (FTA) ความตกลงหุ้นส่วนทางเศรษฐกิจระดับภูมิภาค (Regional Comprehensive Economic Partnership (RCEP)) องค์กรที่ได้รับผลกระทบโดยตรง เป็นต้น รวมถึงการเปลี่ยนแปลงทางเทคโนโลยีดิจิทัลที่เป็นไปอย่างรวดเร็ว และต้องทบทวนแนวทางปฏิบัติต่าง ๆ ที่เกี่ยวข้องให้เป็นปัจจุบัน

ความมั่นคงปลอดภัยไซเบอร์เป็นประเด็นที่ครอบคลุมไปยังแอพพลิเคชั่นที่เกี่ยวเนื่องกับหลากหลายอุตสาหกรรมและหลายภาคส่วน การประเมินความมั่นคงปลอดภัยทางไซเบอร์จึงพิจารณาจากปัจจัยหลักทั้งหมด 5 ด้าน ได้แก่ มาตรการทางกฎหมาย(Legal Measures) มาตรการ

ทางเทคนิค(Technical Measures) มาตรการการจัดโครงสร้างองค์กร(Organizational Measures) การพัฒนาศักยภาพบุคลากร(Capacity Building) และการสร้างความร่วมมือ(Cooperation) จากปัจจัยหลัก 5 ด้านดังกล่าว ประกอบด้วย 17 ปัจจัยย่อย ดังตารางที่ 4

ตารางที่ 4 แสดงปัจจัยหลักและปัจจัยย่อยของดัชนีชี้วัดระดับของการพัฒนาการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ปัจจัยหลัก	ปัจจัยย่อย
1. มาตรการทางกฎหมาย (Legal Measures)	1.1 กฎหมายอาญา (Criminal Legislation) ที่เกี่ยวกับการควบคุมการกระทำความผิดทางคอมพิวเตอร์ 1.2 การมีกฎระเบียบและการปฏิบัติตามกฎระเบียบ (Regulation and Compliance) หมายถึง การมีกฎที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์เฉพาะเรื่อง เช่น กฎหมายการใช้ลายเซ็นอิเล็กทรอนิกส์ เป็นต้น
2. มาตรการทางเทคนิค (Technical Measures)	2.1 การจัดตั้งหน่วยงานระดับชาติเพื่อตอบสนองเหตุการณ์ที่ละเมิดความมั่นคงปลอดภัยทางไซเบอร์ (CIRT (Computer incident Response Team), CIRT (Computer Emergency Response Team) หรือ CSIRT (Computer Security incident Response Team)) 2.2 มาตรฐาน (Standards) 2.3 การออกใบรับรอง (Certifications)
3. มาตรการด้านโครงสร้างองค์กร (Organizational Measures)	3.1 นโยบาย (Policy) 3.2 แผนด้านการกำกับดูแล (Roadmap for Governance) 3.3 หน่วยงานผู้รับผิดชอบ (Responsible Agency) 3.4 การเทียบเคียงกับหน่วยงานระดับชาติ (National Benchmarking)

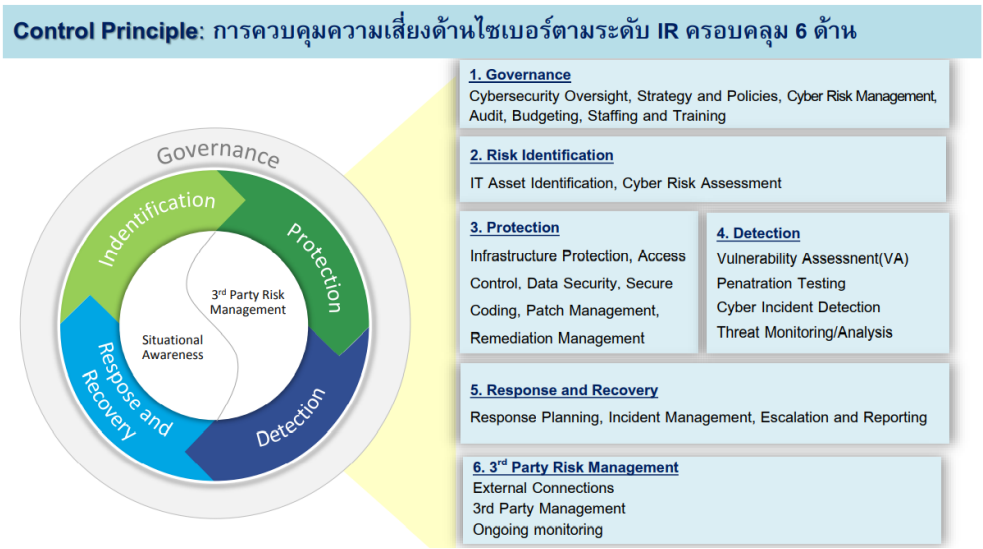
ปัจจัยหลัก	ปัจจัยย่อย
4. การพัฒนาศักยภาพบุคลากร (Capacity Building)	4.1 การกำหนดมาตรฐานในการพัฒนาบุคลากร (Standardization Development) 4.2 การพัฒนาบุคลากร (Manpower Development) 4.3 การให้การรับรองแก่ผู้เชี่ยวชาญ (Professional Certification) 4.4 การให้การรับรองหน่วยงาน (Agency Certification)
5. การสร้างความร่วมมือ (Cooperation)	5.1 การสร้างความร่วมมือระหว่างรัฐ (Intra-State Coorperation) 5.2 การสร้างความร่วมมือระหว่างหน่วยงาน (Intra-Agency Cooperation) 5.3 ความร่วมมือภาครัฐและภาคเอกชน (Public-private partnerships (PPP)) 5.4 การสร้างความร่วมมือระหว่างประเทศ (International Cooperation)

การรักษาความมั่นคงปลอดภัยไซเบอร์มีวัตถุประสงค์เพื่อการสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์(Information systems & Computer network) เพื่อให้บรรลุวัตถุประสงค์ดังกล่าวต้องใช้ทั้งมาตรการทางเทคนิค (Technical measures) มาตรการทางกฎหมาย (Statutory Regulation) รวมถึงการกำกับดูแลตนเอง (Self-Regulation) และการกำกับดูแลร่วมกัน (Co-Regulation) จากทั้งภาครัฐ ภาคเอกชน และภาคประชาสังคม ด้วยเหตุที่การโจมตีทางไซเบอร์อาจกระทำโดยผู้ไม่หวังดีที่มาจากทั้งภายในประเทศและภายนอกประเทศ ฉะนั้น หน่วยงานของรัฐ หน่วยงานภาคเอกชนและภาคประชาสังคม จะต้องมีการบูรณาการประสานความร่วมมือกันเพื่อจัดการกับปัญหาภัยคุกคามทางไซเบอร์อย่างไรก็ตามการใช้มาตรการดังกล่าวต้องคำนึงถึงสิทธิเสรีภาพของประชาชนด้วย และถึงแม้หน่วยงานต่างๆ และภาคประชาชนจะมีความตระหนักด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์แล้ว แต่ภัยคุกคามทางไซเบอร์ก็ยังมีโอกาสที่

จะก่อให้เกิดความเสี่ยงได้ตลอดเวลา ดังนั้น การกำหนดยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์จะทำให้หน่วยราชการ ภาคเอกชน และ ภาคประชาสังคม สามารถนำไปใช้เป็นมาตรฐานในการขับเคลื่อนความมั่นคงปลอดภัยไซเบอร์ในทุกระดับ และต้องทำให้เกิดการแลกเปลี่ยนข้อมูลข่าวสารระหว่างกันในทุกภาคส่วน ข้อสำคัญคือมีศูนย์ปฏิบัติการส่วนกลางที่ทำให้เกิดการวิเคราะห์งานด้านการข่าวไซเบอร์ที่สามารถประมวลผลได้ทันที (Real Times) และสามารถเชื่อมโยง แลกเปลี่ยนข้อมูลข่าวสารด้านการข่าวกรองไซเบอร์ทั้งองค์กรภายในประเทศและระหว่างประเทศได้ซึ่งความร่วมมือขององค์กรภายในประเทศและในระดับนานาชาติ จะสามารถช่วยในการติดตาม ค้นหาแหล่งที่มาของการโจมตีทางไซเบอร์ได้อย่างรวดเร็ว ทันเวลา และสามารถคาดการณ์และแจ้งเตือนแนวโน้มการโจมตีได้อีกด้วย ซึ่งในปัจจุบันคือ ศูนย์ประสานการรักษาความมั่นคงระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) สังกัดสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

2.5.5 การบริหารความเสี่ยงด้านไซเบอร์ขององค์กร

การประเมินความเสี่ยงภัยไซเบอร์ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 นั้น เป็นการประเมินความเสี่ยงด้านความปลอดภัยทางไซเบอร์ที่ช่วยให้ธุรกิจและองค์กรเข้าใจ ควบคุม และลดความเสี่ยงทางไซเบอร์ทุกรูปแบบ ที่เป็นองค์ประกอบสำคัญของการบริหารความเสี่ยงและลดความเสี่ยง หากไม่มีการประเมินความเสี่ยงการรักษาความปลอดภัยทางไซเบอร์ อาจส่งผลกระทบต่อข้อมูลและทรัพยากรสำคัญใน การดำเนินการอยู่ของธุรกิจและองค์กรได้



ภาพที่ 8 กรอบการบริหารและจัดการความเสี่ยงด้านไซเบอร์

(ธนาคารแห่งประเทศไทย, 2562)

จากภาพอธิบายได้ว่า แนวทางการบริหารจัดการความเสี่ยงและมาตรการควบคุมด้านการรักษาความปลอดภัยที่พึงมี (Maturity Level) เป็นการประเมินการบริหารจัดการและการควบคุมความเสี่ยงภัยทางไซเบอร์ว่าอยู่ในระดับที่สอดรับกับความเสี่ยงที่มี หรือมีช่องว่างในเรื่องใดบ้าง โดยประเมินใน 6 ด้านหลัก ได้แก่

(1) กรอบกำกับดูแล (Governance) เพื่อให้มีการกำกับดูแลและสนับสนุนให้องค์กรมีการบริหารความเสี่ยงด้านไซเบอร์อย่างเพียงพอเหมาะสม มีโครงสร้างและบทบาทหน้าที่ในการกำกับดูแลการดำเนินงานและการบริหารความเสี่ยงด้านไซเบอร์สอดคล้องตามหลัก 3 lines of defense อย่างมีประสิทธิภาพ เป็นส่วนหนึ่งของการบริหารตามกรอบการบริหารจัดการความเสี่ยงในภาพรวมขององค์กร (enterprise wide risk) รวมถึงมีบุคลากรที่มีความรู้และความเชี่ยวชาญเพียงพอในการปฏิบัติงานและบุคลากรทุกระดับมีความตระหนักถึงการรักษาความมั่นคงปลอดภัยไซเบอร์

(2) การระบุความเสี่ยง (Risk Identification) เพื่อให้องค์กรมีการบริหารจัดการทรัพย์สินทางด้านเทคโนโลยีที่สามารถเชื่อมโยง นำไปใช้ในการบริหารจัดการ และสามารถระบุความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ

(3) การป้องกัน (Protection) เพื่อให้องค์กรมีกระบวนการบริหารจัดการและเครื่องมือหรืออุปกรณ์ที่พร้อมสำหรับการป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจก่อให้เกิดการหยุดชะงักในการให้บริการของระบบงานที่สำคัญ

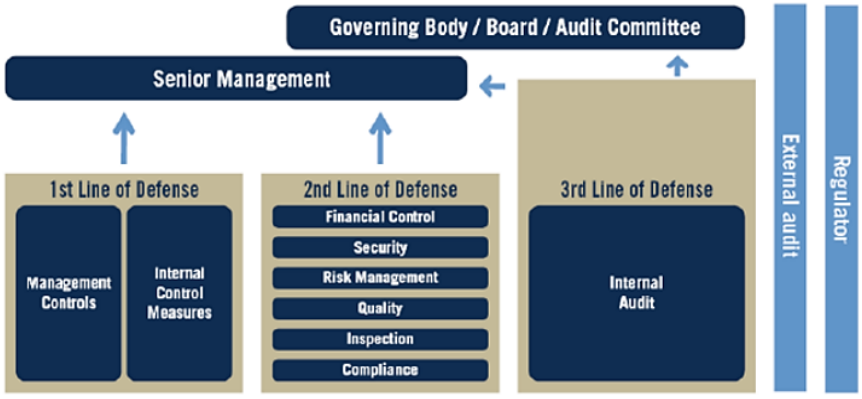
(4) การเฝ้าระวังและการตรวจจับ (Detection) เพื่อให้องค์กรมีกระบวนการบริหารจัดการและมาตรการในการตรวจหาช่องโหว่หรือจุดอ่อนของระบบงาน และให้ทราบถึงช่องโหว่ด้านการรักษาความมั่นคงปลอดภัยของระบบ รวมทั้งสามารถดำเนินการปรับปรุงแก้ไขป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้อย่างทันการณ์มีการบริหารจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Information and Event Management) เพื่อติดตามและรายงานพฤติกรรมที่ผิดปกติได้อย่างทันกาล และมีการแลกเปลี่ยนองค์ความรู้ภัยคุกคามทางไซเบอร์ภายในองค์กรและการสร้างความร่วมมือกับหน่วยงานภายนอกเพื่อประโยชน์ในการสร้างความร่วมมือกับการรับมือภัยไซเบอร์และสามารถระงับเหตุการณ์ที่อาจเกิดขึ้นได้

(5) การตอบสนองต่อเหตุการณ์และการกู้คืน (Respond and Recovery) เพื่อให้องค์กรมีแผน มาตรฐาน และระเบียบวิธีปฏิบัติในการรับมือภัยคุกคามและการตอบสนองต่อ

เหตุการณ์ผิดปกติทางไซเบอร์ที่อาจส่งผลกระทบให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบและสามารถกู้คืนระบบให้กลับคืนสู่สภาพปกติภายใต้ระยะเวลาที่ยอมรับได้

(6) การบริหารความเสี่ยงด้านภัยคุกคามที่เกิดจากหน่วยงานภายนอก (Third Party Risk Management) เพื่อให้องค์กรมีแนวทางในการบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างมีประสิทธิภาพรวมถึงมีการติดตามความเสี่ยงของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างสม่ำเสมอ (ธนาคารแห่งประเทศไทย, 2562)

ตัวอย่างการประเมินระดับความเสี่ยงด้านไซเบอร์และการบริหารความเสี่ยงด้านไซเบอร์โดยธนาคารแห่งประเทศไทย (ธปท.) ได้กำหนดหลักเกณฑ์กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยหลักเกณฑ์การกำกับดูแลระบบเทคโนโลยีสารสนเทศที่ใช้อยู่ในปัจจุบันช่วยให้ผู้ประกอบธุรกิจมีธรรมาภิบาลด้านเทคโนโลยีสารสนเทศที่ดี มีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการบริหารความเสี่ยงอย่างเหมาะสม โดยหลักเกณฑ์กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ ประกอบด้วย 2 ส่วนสำคัญ ได้แก่ (1) การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขั้นต้นที่จำเป็น (Cyber Hygiene) ซึ่งเป็นมาตรการขั้นต้นเพื่อยกระดับความมั่นคงปลอดภัยในการป้องกันและรับมือภัยคุกคามทางไซเบอร์ที่สำคัญทั้งภายในและภายนอก และ (2) การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management) ซึ่งมุ่งเน้นให้มีคุณสมบัติตามหลักเกณฑ์การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสม มีโครงสร้างองค์กร องค์ประกอบและการกำหนดบทบาทหน้าที่ของผู้ดูแล เพื่อกำหนดนโยบายในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ครอบคลุมตลอดจนกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับลักษณะการให้บริการหรือดำเนินธุรกิจในการกำกับดูแลการดำเนินงานและการบริหารความเสี่ยงด้านไซเบอร์สอดคล้องตามหลัก 3-Lines of Defense ซึ่งเป็นเครื่องมือมาตรฐานสากลมาตรการตรวจสอบ ดังภาพที่ 9



ภาพที่ 9 โมเดลของ 3-Lines of Defense (The Institute of Internal Auditors, 2013)

ซึ่งจุดประสงค์ที่สำคัญของ “Lines of Defense Model” คือหลักการควบคุมดูแลแบบเป็นลำดับขั้นให้เป็นไปตามกฎระเบียบขั้นตอน โดย 3 Lines of Defense ประกอบไปด้วยส่วนที่เป็น 1st Line of Defense , 2nd Line of Defense และ 3rd Line of Defense โดยกระบวนการในแต่ละระดับ (Line) ก่อให้เกิดกระบวนการกำกับดูแลที่ดีมีประสิทธิภาพและเป็นส่วนหนึ่งของการบริหารตามกรอบการบริหารจัดการความเสี่ยงในภาพรวมขององค์กร (Enterprise Wide Risk) รวมถึงมีบุคลากรที่มีความรู้และความเชี่ยวชาญเพียงพอในการปฏิบัติงานและบุคลากรทุกระดับมีความตระหนักถึงการรักษาความมั่นคงปลอดภัยไซเบอร์โดยคณะกรรมการสถาบันการเงินมีบทบาทและหน้าที่ความรับผิดชอบในการดูแลให้มีกลยุทธ์และนโยบายรวมทั้งดูแลให้มีกลไกในการกำกับดูแลและติดตามให้มีการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้ ธปท. ได้แบ่งระดับความเสี่ยงจากภัยคุกตามไซเบอร์ ออกเป็น 3 ระดับ ได้แก่ Baseline, Intermediate และ Advanced Maturity สอดคล้องกับระดับความเสี่ยงไซเบอร์ที่สถาบันทางการเงินมี (ธนาคารแห่งประเทศไทย, 2562) ดังนี้

ตารางที่ 5 การบริหารจัดการความเสี่ยงไซเบอร์

ระดับความเสี่ยง	การบริหารจัดการความเสี่ยงไซเบอร์
ต่ำ	สำนักงานควรปฏิบัติได้ตามมาตรการที่ ธปท. กำหนดสำหรับระดับ **Baseline Maturity**
ปานกลาง	สำนักงานควรปฏิบัติได้ตามมาตรการที่ ธปท. กำหนดสำหรับระดับ **Baseline และ Intermediate Maturity**
สูง	สำนักงานควรปฏิบัติได้ตามมาตรการที่ ธปท. กำหนดสำหรับระดับ **Baseline Intermediate และ Advanced Maturity**

ที่มา: ธนาคารแห่งประเทศไทย (2562)

ผู้วิจัยสนใจในประเด็นนี้ เนื่องจากการบริหารความเสี่ยงด้านความปลอดภัยทางไซเบอร์ เป็นแนวปฏิบัติในการจัดลำดับความสำคัญของมาตรการป้องกันความปลอดภัยทางไซเบอร์ โดยพิจารณาจากผลกระทบที่อาจเกิดขึ้นจากภัยคุกคามที่ออกแบบมาเพื่อใช้ในการโจมตีเป้าหมาย การสร้างแนวทางการบริหารความเสี่ยง เพื่อการสร้างความมั่นคงด้านความปลอดภัยทางไซเบอร์ ซึ่งธุรกิจและองค์กรที่เกิดขึ้นใหม่ อาจไม่สามารถกำจัดช่องโหว่ของระบบทั้งหมดหรือบล็อกการโจมตีทางไซเบอร์ได้ทั้งหมด ผ่านการจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์ ธุรกิจและองค์กรควรให้ความสำคัญกับข้อบกพร่องของระบบ แนวโน้มภัยคุกคามและการโจมตีที่สำคัญที่สุดต่อธุรกิจก่อน อันเป็นผลมาจากการดำเนินงานและการใช้ระบบสารสนเทศ วัตถุประสงค์หลักของการประเมินความเสี่ยงทางไซเบอร์คือ การแจ้งให้ผู้มีส่วนได้ส่วนเสียทราบและสนับสนุนการตอบสนองที่เหมาะสมต่อความเสี่ยงที่เกิดขึ้น พร้อมสามารถสรุปข้อมูลสำคัญสำหรับผู้บริหาร เพื่อช่วยผู้บริหารและกรรมการในการตัดสินใจเกี่ยวกับการรักษาความปลอดภัย

2.5.6 การสร้างความตระหนักรู้และการเตรียมความพร้อมรับมือภัยคุกคามทางไซเบอร์

2.5.6.1 การสร้างความตระหนักรู้ในองค์กร

อีกด้านหนึ่งของการป้องกันภัยคุกคามทางไซเบอร์และแก้ไขปัญหาจากการใช้อินเทอร์เน็ต จึงเป็นการสร้างการตระหนักรู้ ความเข้าใจเกี่ยวกับการใช้เทคโนโลยีสารสนเทศเพื่อให้เกิดการใช้อินเทอร์เน็ตอย่างมั่นคงปลอดภัย โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การหมาชน) หรือ สพธอ. ซึ่งพบว่าในปี พ.ศ. 2561 คนไทยมีการใช้งานอินเทอร์เน็ตเฉลี่ยสูงถึง 10.50 ชั่วโมงต่อวัน เพิ่มขึ้นจากปี พ.ศ. 2560 จำนวน 3 ชั่วโมง 41 นาที โดยพบว่าปัญหาที่เกิดขึ้นจากการใช้งานอินเทอร์เน็ตเป็นเรื่องของการถูกหลอกลวงและการละเมิดข้อมูลส่วนบุคคล การขาดความมั่นใจและความเชื่อถือจากข้อมูลที่ได้รับจากอินเทอร์เน็ต รวมทั้งปัญหาที่สำคัญจากภัยคุกคามไซเบอร์ไม่ว่าจะเป็นไวรัส มัลแวร์ จากสถานการณ์ดังกล่าว ส่งผลให้หลายหน่วยงานที่เกี่ยวข้องต้องดำเนินการเพื่อตอบสนองต่อสถานการณ์ที่เกิดขึ้น ตามภารกิจของแต่ละหน่วยงานเพื่อสร้างความเชื่อมั่นให้เกิดขึ้น (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2561) ซึ่งปัจจุบันองค์กรภาครัฐและเอกชนมีการนำเอาเทคโนโลยีสารสนเทศมาใช้ในการปฏิบัติงานกันอย่างแพร่หลายเพื่ออำนวยความสะดวกและเพิ่มขีดความสามารถในการดำเนินกิจกรรมขององค์กรไม่ว่าจะเป็นการใช้งานเครื่องคอมพิวเตอร์ภายในสำนักงาน การใช้งานเครื่องคอมพิวเตอร์แม่ข่ายเพื่อการประมวลผล รวมไปถึงการเชื่อมต่อระบบคอมพิวเตอร์เข้ากับระบบเครือข่ายเพื่อสร้างการสื่อสารทั้งภายในและภายนอกองค์กร โดยองค์กรบางแห่งอาจจะมีการพึ่งพาระบบสารสนเทศเป็นแกนหลัก เพื่อให้กิจกรรมขององค์กรสามารถดำเนินไปได้โดยการที่องค์กรจำนวนมากหันมาใช้งานเทคโนโลยีดิจิทัลในการดำเนินงานกันมากขึ้น รวมถึงการทำงานจาก

ที่บ้านได้รับความนิยมเพิ่มมากขึ้น ส่งผลให้องค์กรต่าง ๆ มีโอกาสที่จะตกเป็นเหยื่อจากการโจมตีทางไซเบอร์มากขึ้นตามไปด้วย ซึ่งการโจมตีทางไซเบอร์เป็นภัยคุกคามที่ส่งผลกระทบโดยตรงต่อความมั่นคงปลอดภัยระบบสารสนเทศขององค์กร มีโอกาสที่จะทำให้การดำเนินงานขององค์กรต้องหยุดชะงัก สร้างความเสียหายทางการเงิน ทำลายความน่าเชื่อถือและชื่อเสียงขององค์กร โดยในการศึกษาของบริษัท IBM พบว่าร้อยละ 95 ของการละเมิดทางไซเบอร์ มีสาเหตุมาจากความผิดพลาดที่เกิดจากการกระทำของบุคคลซึ่งอาจจะเกิดขึ้นได้ในหลายลักษณะ เช่น บุคลากรบางคนตั้งค่ารหัสผ่านในการเข้าใช้งานระบบที่มีความสำคัญขององค์กรในลักษณะที่ง่ายต่อการคาดเดา หรือหลงเชื่ออีเมลหลอกลวง (Phishing Email) ทำให้ถูกหลอกเอาข้อมูลที่มีความสำคัญไป เป็นต้น

จากการศึกษามาตรการของรัฐเพื่อแก้ปัญหาในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล ได้แก่ การออก พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล และมาตรการเสริมสร้างจิตสำนึกและความตระหนักรู้ ซึ่งการออกมาตรการทางกฎหมายเพื่อการคุ้มครองข้อมูลส่วนบุคคลเป็นเรื่องสำคัญ และจำเป็นในระดับนโยบายของรัฐ (National Policy) อย่างไรก็ตามมาตรการทางกฎหมายและการดำเนินการบังคับใช้กฎหมาย ยากที่จะสัมฤทธิ์ผลถ้าไม่มีการเสริมสร้างความรู้ความเข้าใจ และการสร้างความตระหนักรู้และเสริมสร้างจิตสำนึกของเจ้าหน้าที่ของรัฐและประชาชนควบคู่ไปกับการใช้มาตรการทางกฎหมาย (นครเสรีรักษ์, 2548) สอดคล้องตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ ปี 2562 มีข้อกำหนดว่าองค์กรจะต้องทำ Security Awareness ในองค์กร ดังที่ปรากฏในหมวดที่ 3 ส่วนที่ 1 นโยบายและแผน มาตรา 42 ข้อที่ 7 ว่า ต้องมีเป้าหมายและแนวทางอย่างน้อยเป็นการสร้างความตระหนักและความรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และแนวปฏิบัตินี้สอดคล้องกับ NIST-Cybersecurity ซึ่งมีแนวปฏิบัติ 5 ด้าน โดย การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) จะอยู่ในด้านของการป้องกัน (Protect) ซึ่งรายละเอียดของกรอบมาตรฐานนี้ได้กำหนดไว้ทุกกลุ่มจะต้องรับรู้หน้าที่รับผิดชอบ (Roles & Responsibilities) ของตนเองว่ามีความสำคัญและมีหน้าที่รับผิดชอบอะไรบ้าง ดังนี้ (1) ต้องมีแผนงานในการสร้างความตระหนักรู้ให้กับบุคลากรในองค์กร ได้แก่ กลุ่มพนักงานใหม่พนักงานที่ทำงานอยู่ประจำ กลุ่มผู้บริหาร กลุ่มเจ้าหน้าที่สนับสนุนโครงสร้างพื้นฐานสำคัญทางสาระสนเทศหรือทางกลุ่มแอดมิน กลุ่มผู้รับเหมาหรือ Vendor (2) ต้องตระหนักรู้ทางด้านกฎหมายเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (3) ต้องรู้เท่าทันภัยคุกคามไซเบอร์ที่จะมีผลกระทบต่อองค์กร (4) ต้องมีการทบทวนแผนในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ในทุก ๆ ปี

จากการศึกษาเรื่อง “วิศวกรรมสังคมสุดขีด - ต่อสู้กับภัยคุกคามความปลอดภัยภายใน - การฝึกความตระหนักด้านความปลอดภัย” วิเคราะห์ถึง จุดอ่อนของพฤติกรรมของมนุษย์ที่ส่งผลต่อความปลอดภัยของข้อมูลสารสนเทศและทรัพยากรระบบขององค์กร ผลเสียที่เกิดขึ้นกับองค์กรจากการที่พนักงานในองค์กรนั้นขาดความตระหนักในเรื่องความปลอดภัยของข้อมูลสารสนเทศขององค์กร พร้อมทั้งเสนอแนะวิธีการป้องกันการจารกรรมข้อมูลสารสนเทศโดยอาศัยวิธีวิศวกรรมสังคม ซึ่งไม่ได้การลงทุนไปกับเทคโนโลยีการรักษาความปลอดภัยระบบสารสนเทศชั้นสูง แต่หมายถึงการป้องกันปัญหาที่เกิดขึ้นกับคน (Bevis, J., 2007) และสอดคล้องกับงานวิจัยของ อัญรัตน์ จันทร์เจริญสุข ได้ทำการศึกษาวิจัยเรื่อง เทคนิคการจารกรรมข้อมูลสารสนเทศผ่านทางกระบวนการทางสังคม กรณีศึกษา ธนาคารพาณิชย์แห่งหนึ่ง วิธีในการรับมือและป้องกันการจารกรรมข้อมูลสารสนเทศผ่านกระบวนการทางสังคม (Social Engineering) นั้น พบว่า การมีกระบวนการหรือระเบียบวิธีในการปฏิบัติงานที่มีประสิทธิภาพและรัดกุมควบคู่กับการสร้างความตระหนักรู้เรื่องความปลอดภัยของข้อมูลสารสนเทศให้กับบุคลากรในองค์กรนั้นเป็นวิธีในการรับมือและป้องกันการจารกรรมข้อมูลสารสนเทศผ่านกระบวนการทางสังคมที่มีประสิทธิภาพมากที่สุด (อัญรัตน์ จันทร์เจริญสุข, 2552)และจากตัวอย่างงานวิจัยเรื่อง ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเตอร์เน็ตในกรุงเทพมหานคร พบว่า ในภาพรวมกลุ่มตัวอย่างมีความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์ในระดับมากเช่นเดียวกัน ทั้งนี้เป็นเพราะบริษัทเอกชนแห่งนี้ได้รับการรับรองมาตรฐานที่สำคัญหลายรายการซึ่งมีส่วนที่เกี่ยวข้องกับการบริหารจัดการระบบสารสนเทศเพื่อตอบสนองต่อความต้องการด้านมาตรฐานของคู่ค้า อีกทั้งมีกระบวนการให้ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์แก่บุคลากรเป็นระยะ ๆ ทำให้บุคลากรมีความรู้ความเข้าใจในการใช้งานเทคโนโลยีสารสนเทศเป็นอย่างดี แต่หากพิจารณาเป็นรายด้านจะพบว่ากลุ่มตัวอย่างมีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์เกี่ยวกับการหลอกลวง (Phishing Awareness) ต่ำที่สุดจากทั้งหมด 3 ด้าน ซึ่งมีสาเหตุเพราะในการโจมตีด้วยวิธีการหลอกลวง (Phishing) เป็นการโจมตีซึ่งแสวงประโยชน์จากสถาวะจิตใจและพฤติกรรมของมนุษย์ (ENISA, 2021) จึงทำให้ยากแก่การป้องกัน

ผู้วิจัยสนใจด้านการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) เนื่องด้วยปัจจุบันหลายองค์กรต้องเผชิญกับภัยคุกคามทางไซเบอร์ในรูปแบบใหม่ๆและปัญหาที่สำคัญคือ บุคลากรยังขาดความรู้ความเข้าใจในด้านกฎหมาย ประกอบกับการโจมตีทางไซเบอร์ที่หลากหลายช่องทาง โดยเฉพาะการสร้างอีเมล Phishing ที่สร้างเนื้อหาให้ตรง

กับลักษณะงานที่เหยื่อในแต่ละองค์กรสนใจอยู่ ส่งผลให้เหยื่อถูกหลอกลวงได้ง่าย ดังนั้น การปกป้องและต่อต้านภัยคุกคามทางไซเบอร์ จำเป็นที่จะต้องให้พนักงานหรือเจ้าหน้าที่ในองค์กรทุกคนตระหนักถึงเรื่อง Cybersecurity Awareness รวมถึงการทดสอบ Phishing Simulation ตลอดจน Cybersecurity Awareness Training เพื่อส่งเสริมให้พนักงานมีความรู้กับความปลอดภัยทางไซเบอร์และตระหนักถึงความสำคัญในการปรับปรุงข้อมูลภัยต่างๆ บนอินเตอร์เน็ต

2.5.6.2 การเตรียมความพร้อมขององค์กร

การเตรียมความพร้อม หมายถึงการดำเนินกิจกรรมบางอย่างเพื่อให้เกิดความสนใจและตั้งใจในการที่จะปฏิบัติกิจกรรมนั้น ๆ ให้สามารถสำเร็จลุล่วงไปได้อย่างมีประสิทธิภาพ ตลอดจนคุณสมบัติหรือสภาวะของบุคคลที่พร้อมจะทำงาน หรือกระทำกิจกรรมอย่างใดอย่างหนึ่งอย่างมีแนวโนมจะประสบผลสำเร็จตามวัตถุประสงค์ (วัชรวรรณ ดวงสะเก็ด, 2555) โดยองค์ประกอบหลักของความพร้อมมี 2 ประการ คือ ด้านความสามารถ (Ability) ประกอบด้วย ความรู้ความเข้าใจ ทักษะและประสบการณ์ส่วนอีกด้าน คือ ความเต็มใจ (Willingness) ประกอบด้วย การให้คำมั่นสัญญาหรือความผูกพัน แรงจูงใจในการทำงาน และความมั่นคง (Hersey and Blanchard, 1993) ทั้งนี้ องค์ประกอบของความพร้อมแบ่งออกได้เป็น 4 กลุ่ม ได้แก่ 1) องค์ประกอบทางกายภาพ ได้แก่ การบรรลุวุฒิภาวะทางด้านร่างกายทั่วไป เป็นต้น 2) องค์ประกอบด้านสิ่งแวดล้อม ได้แก่ ประสบการณ์ด้านสังคม และครอบครัวสภาพแวดล้อมรอบตัวที่แตกต่างกัน เป็นต้น 3) องค์ประกอบด้านอารมณ์แรงจูงใจ และบุคลิกภาพได้แก่ ความมั่นคงทางอารมณ์ และความปรารถนาที่จะเรียนรู้ เป็นต้น 4) องค์ประกอบด้านสติปัญญาได้แก่ ความพร้อมด้านความสามารถในการรับรู้ ความสามารถในการคิดอย่างมีเหตุผล เป็นต้น (Downing and Thackray, 1971)

สำหรับหน่วยงานหรือองค์กรโดยทั่วไป อาจไม่ใช่แค่ความพร้อมที่กล่าวมาแล้วในข้างต้น แต่องค์ประกอบของความพร้อมขององค์กรในการรับมือภัยคุกคามทางไซเบอร์อาจต้องพิจารณาการบริหารจัดการและการเตรียมความพร้อมให้ครอบคลุมในทุกๆด้าน ดังนี้

1) ความพร้อมของระบบองค์กร (Organization) องค์กร หมายถึงกลุ่มคนที่สร้างขึ้นเพื่อจุดมุ่งหมายที่จะดำเนินการอย่างใดอย่างหนึ่ง เพื่อให้บรรลุเป้าหมายหรือวัตถุประสงค์ที่วางไว้ระบบองค์กร หมายถึง โครงสร้างทางสังคมที่ถูกสร้างขึ้นมาเพื่อประกอบกิจกรรมของบุคคลเป็นการกำหนดนโยบายเพื่อใช้เป็นแนวทางปฏิบัติงานร่วมกัน ตลอดจนการดำเนินการจัดสรรทรัพยากรเพื่อใช้ในการดำเนินงานให้เกิดประโยชน์สูงสุด และนำไปสู่ความสำเร็จของการดำเนินการทั้งนี้ ระบบองค์กร ประกอบด้วย การวางนโยบายเพื่อกำหนดแนวทางในการปฏิบัติร่วมกันและการจัดการเพื่อ

ตัดสินใจในการใช้ทรัพยากรให้เกิดประโยชน์สูงสุด คือ บรรลุจุดมุ่งหมายขององค์กร ทั้งในด้านประสิทธิภาพ และประสิทธิผล

2) ความพร้อมของนโยบาย (Policy) หมายถึง แนวทาง ทิศทาง และกระบวนการที่จะนำไปสู่เป้าหมาย โดยมีการระบุถึงวิธีการที่จะนำไปสู่เป้าหมาย ซึ่งมีกระบวนการ ดังนี้

การวางแผน (Planning) การคิดการล่วงหน้าหรือกำหนดกิจกรรม และจะต้องทำหรือหากลวิธีที่เหมาะสมกับสถานการณ์ โดยคำนึงถึงใคร หน่วยงานใด ทำเมื่อไร ที่ไหนและจะต้องมีปัจจัยอะไรในการสนับสนุนเท่าใด จึงจะสามารถปฏิบัติงานได้ และได้ผลตามที่ต้องการ

การเตรียมการหรือเตรียมแผนปฏิบัติการ (Organizing and Preparing Operation Plan) คือ การเตรียมความพร้อมที่จะเข้าปฏิบัติงานได้ทันท่วงทีกับเวลาที่เริ่มต้นปฏิบัติเป็นเรื่องของการบริหารจัดการทำแผนสนับสนุนทรัพยากรให้แก่หน่วยปฏิบัติให้เพียงพอที่จะสร้างความสัมพันธ์ระหว่างผู้รับผิดชอบ งบประมาณ และเครื่องมือเข้าด้วยกัน หากเป็นงานประจำก็ต้องออกระเบียบปฏิบัติที่สามารถใช้เป็นเครื่องมือในการดำเนินการได้

การมีแผนงานและระเบียบปฏิบัติงาน (Direct and Supervising) คือ การนำเอกสารที่เกี่ยวข้องกับการปฏิบัติงานมาให้ผู้ร่วมงาน การออกคำสั่ง การชี้แจงและการอธิบายให้แก่ทุกคนที่รับผิดชอบ เพื่อให้สามารถทำงานได้ถูกต้องตามเจตนารมณ์ และแผนที่กำหนดไว้นอกจากนั้น นักจัดการหรือนักบริหารยังมีหน้าที่กำกับ ตรวจตรา ติดตามการปฏิบัติงานของผู้ปฏิบัติ เป็นระยะ ๆ เพื่อช่วยแก้ปัญหา ให้คำแนะนำช่วยเหลือ และให้กำลังใจแก่ผู้ปฏิบัติงาน

การประสานงาน (Coordination) คือ การแสวงหาความร่วมมือ และการทำงาน ร่วมกับหน่วยงานอื่น ทั้งภาครัฐและเอกชนที่มีวงจรเกี่ยวข้องกัน เพื่อให้หน่วยงานของตนสามารถทำงานเชื่อมโยงกับหน่วยงานอื่น หรือชุมชนได้อย่างกว้างขวาง มีประสิทธิภาพและสัมฤทธิ์ผลตามเจตนารมณ์

การประเมินผล (Evaluation) คือ การประเมินเพื่อแก้ไขปรับปรุงความสามารถในการปฏิบัติงานของตน หรือหน่วยงานของตนให้มีประสิทธิภาพมากขึ้น ซึ่งจะต้องอาศัยความรู้ เกี่ยวกับข้อเท็จจริง ผลงานของหน่วยงานปัญหา และข้อบกพร่องต่างๆ ที่เกิดขึ้นในการปฏิบัติงานสิ่งเหล่านี้จะมาจากกระบวนการรายงานย้อนกลับ (Feedback) การรายงานบางอย่างมีความซับซ้อนที่ต้องมาวิเคราะห์หาสมมติฐานที่แท้จริง ก่อนที่จะคิดหาวิธีการที่ดีกว่ามาปฏิบัติงานในโอกาสต่อไป

3) ความพร้อมของบุคลากร (Personnel) ความพร้อมของบุคลากร หมายถึง การเตรียมตัวเพื่อจะเจริญงอกงามหรือการที่จะก้าวหน้าต่อไป และมีอีกความหมายว่า ความพร้อม คือ ลักษณะทั้งหมดในตัวบุคคลที่สามารถรวบรวมขึ้นเป็นเครื่องมือ เพื่อใช้เป็นเครื่องมือในการตอบสนองสิ่งใดสิ่งหนึ่ง ด้วยวิธีการใดวิธีการหนึ่ง การจัดการที่ดีจำเป็นต้องได้บุคลากรที่มีความรู้ ความสามารถ และคุณสมบัติที่จำเป็นมาบรรจุในตำแหน่งหน้าที่ที่กำหนดไว้ การเตรียมบุคลากรให้พร้อมที่จะเข้าปฏิบัติงานได้ทันท่วงทีเรียกว่า การวางแผนกำลังคน ซึ่งหมายถึง การเตรียมบุคลากรทั้งในด้านจำนวน และคุณภาพเพื่อให้สามารถปฏิบัติงานได้บรรลุจุดประสงค์ และเป้าหมายที่วางไว้ การสร้างความพร้อมของบุคลากร ได้แก่

การฝึกอบรม (Training) หมายถึง การพัฒนาบุคลกรในองค์กรให้ได้รับความรู้ เพิ่มมากขึ้น ทั้งทางด้านสารสนเทศ และทักษะที่สามารถนำไปประยุกต์ใช้ในการทำงานอย่างได้ผลโดยผ่านกระบวนการฝึกอบรมที่จัดไว้เป็นรูปแบบมีมาตรฐาน และการประเมินผลที่เป็นที่ยอมรับ

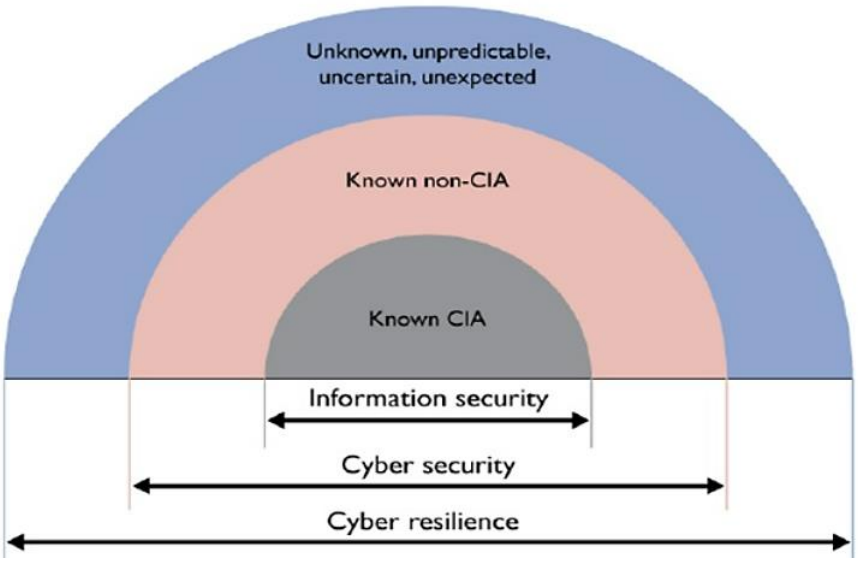
การศึกษา (Education) หมายถึง กิจกรรมที่มุ่งเน้นการเรียนรู้ที่เกี่ยวกับงานที่ได้รับมอบหมายเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน

การพัฒนา (Development) หมายถึง กระบวนการที่มุ่งจะเปลี่ยนแปลงวิธีการ ทำงาน ความรู้ความสามารถ ทักษะ และทัศนคติของบุคลากรให้เป็นไปในทางที่ดีขึ้น การวางแผนกำลังคนนี้ มีความจำเป็นต่อการเตรียมความพร้อม เพราะหากขาดบุคลากรทั้งในด้านปริมาณหรือคุณภาพ หรือขาดการพัฒนาบุคลากรก็จะทำให้การดำเนินการขององค์กรไม่บรรลุเป้าหมายตามที่กำหนดไว้ การที่บุคคลจะมีพฤติกรรมในการทำงานอย่างใดอย่างหนึ่งขึ้นอยู่กับคุณลักษณะที่บุคคลมีอยู่ในตัวเองจะสังเกตเห็นได้ และสามารถที่จะวัดได้นำมาพัฒนาได้ง่าย ได้แก่ ความรู้สาขาต่างๆ ที่ได้เรียนมา (Knowledge) และส่วนของทักษะ ได้แก่ ความเชี่ยวชาญ ความชำนาญพิเศษด้านต่าง ๆ (Skill) สำหรับคุณลักษณะอื่น ๆ (Other Characteristics) ของบุคคลนั้น ๆ เป็นส่วนที่ไม่อาจสังเกตได้ชัดเจนและวัดได้ยากกว่า และเป็นส่วนที่มีอิทธิพลต่อพฤติกรรมของบุคคลมากกว่าได้แก่ บทบาทที่แสดงออกต่อสังคม (Social Role) ภาพลักษณ์ของบุคคลที่มีต่อตนเอง (Self-Image)คุณลักษณะส่วนบุคคล (Trait) และแรงจูงใจ (Motive) ดังนั้น องค์ประกอบที่จำเป็นในการปฏิบัติงานจะประกอบด้วย ความรู้ (Knowledge) ทักษะ (Skill) ความสามารถ (Ability) และคุณลักษณะอื่น ๆ (Other Characteristics) ที่จำเป็นในการปฏิบัติงาน

4) ความพร้อมด้านทรัพยากร (Resource) ทรัพยากร หมายถึง เงิน และวัสดุอุปกรณ์ อันเป็นปัจจัยพื้นฐานในการบริหารงานของทุกกิจกรรม เงินเป็นปัจจัยสำคัญในการดำเนิน

กิจกรรมตามที่กำหนดไว้ ทั้งในด้านจำนวนและเวลาที่ถูกต้อง สอดคล้องกัน ดังนั้น การพิจารณาแหล่งเงิน การจัดสรรเพื่อเป็นค่าใช้จ่ายในการจัดกิจกรรมต่าง ๆ ต้องได้สัดส่วน การควบคุมการใช้จ่ายเงินอย่างถูกต้องตามหลักเกณฑ์ ขณะเดียวกัน ต้องสนับสนุนให้งานราบรื่นและบรรลุเป้าหมายได้ วัสดุอุปกรณ์เป็นปัจจัยสำคัญอีกประการในที่นี้รวมถึงสถานที่ปฏิบัติงาน สถานที่บริการที่เหมาะสม ทันสมัย เพียงพอและมีประสิทธิภาพที่จะสามารถช่วยให้การดำเนินงานตามหน้าที่ของหน่วยงานนั้น ๆ อย่างได้ผล

อย่างไรก็ดี นอกเหนือจากประเด็นการเตรียมความพร้อมที่กล่าวมา อีกประการหนึ่งที่มีความสำคัญคือ สภาวะที่องค์กรมีความทนทานต่อภัยคุกคามทางไซเบอร์ที่เคยพบหรือไม่เคยพบมาก่อนหรือที่เรียกกันว่า “Cyber Resilience” ซึ่งเป็นแนวทางในการเตรียมความพร้อมเพื่อตรวจจับ (Detect) และตอบสนอง (React) ต่อการถูกบุกรุกโจมตีได้อย่างรวดเร็วและมีระบบ องค์กรจำเป็นต้องปรับตัวจาก “การป้องกัน (Protective Security)” แบบดั้งเดิมที่ทำอยู่ในปัจจุบัน ไปเป็น “การเตรียมความพร้อม (Responsive Security)” ให้พร้อมรับมือต่อภัยคุกคามที่ไม่เคยพบเห็นมาก่อน



ภาพที่ 10 The Three Stage (Source: Cybersecurity Strategies by ISF)
(ธนาคารแห่งประเทศไทย, 2562)

จากภาพที่ 10 แสดงให้เห็นว่า หน่วยงาน Information Security Forum (ISF) แบ่งภัยคุกคามและวิธีรับมือออกเป็น 3 ส่วน ได้แก่

(1) Information Security หมายถึง การรับมือภัยคุกคามที่ส่งผลกระทบต่อ Confidentiality, Integrity และ Availability การรับมือกับภัยคุกคามนี้เรียกว่า Known CIA

(2) Cyber Security คือ การรับมือภัยคุกคามที่ส่งผลกระทบต่อความเสี่ยงอื่นที่นอกเหนือจาก CIA เช่น Authentication, Authorization การรับมือกับภัยคุกคามนี้เรียกว่า Known non-CIA

(3) Cyber Resilience คือ การรับมือภัยคุกคามที่ไม่เคยพบมาก่อน ไม่สามารถทำนายได้ ไม่ชัดเจน หรือไม่คาดคิดมาก่อน เช่น การโจมตีแบบ Zero-day การรับมือกับภัยคุกคามนี้เรียกว่า Unknown (ธนาคารแห่งประเทศไทย, 2562)

อนึ่ง Cyber Resilience เป็นอีกแนวทางในการเตรียมความขององค์รให้สามารถป้องกันและตรวจจับการบุกรุกโจมตีทางไซเบอร์ก่อนที่จะส่งผลเสียร้ายแรงต่อองค์กร และ ถ้าการบุกรุกโจมตีได้ก่อเกิดปัญหาขึ้นต่อการปฏิบัติงานขององค์กรแล้ว องค์กรควรจะมีความสามารถในการตอบสนองต่อการถูกโจมตีได้อย่างรวดเร็วซึ่งการที่องค์กรจะมีสภาวะ Cyber Resilience ได้นั้นจำเป็นต้องมีการเตรียมการ และ มี Incident Response Team ที่มีความเชี่ยวชาญและมีประสบการณ์มากพอสมควร จนสามารถใช้ความชำนาญ, ความสามารถและประสบการณ์ของทีมในการควบคุมภัยคุกคามไซเบอร์ที่อาจไม่เคยพบมาก่อนได้อย่างทันท่วงที กล่าวคือ องค์กรจะเกิดสภาวะ Cyber Resilience จำเป็นต้องมีการเตรียมการและเตรียมบุคลากร Incident Response Team ที่มีประสิทธิภาพ เนื่องจากการฝึกอบรมสร้างความตระหนักเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ส่วนใหญ่แล้วจะเป็นการเรียนรู้ในเชิงทฤษฎี ทำให้การฝึกอบรมไม่สามารถสร้างความตระหนักรู้และสร้างกระบวนการตอบสนองต่อภัยคุกคามทางไซเบอร์เมื่อภัยคุกคามทางไซเบอร์นั้นเกิดขึ้นจริงๆ นอกจากการฝึกอบรมในห้องแล้ว จึงจำเป็นต้องให้พนักงานและผู้บริหารได้มีโอกาสสัมผัสกับสถานการณ์ที่เกิดการโจมตีทางไซเบอร์ขึ้นจริงด้วย เรียกว่า การซ้อมหนีไฟทางไซเบอร์ หรือ “Cyber Drill” ซึ่งเป็นการจำลองสถานการณ์การโจมตีภัยคุกคามไซเบอร์ในรูปแบบต่างๆเพื่อให้พนักงานหรือผู้ที่เกี่ยวข้องในการตอบสนองต่อภัยคุกคามไซเบอร์เกิดความคุ้นเคย และยังสามารถตรวจสอบได้ว่าพนักงานคนใดมีความเสี่ยงสูงต่อการตกเป็นเหยื่อของภัยคุกคามไซเบอร์เหล่านั้นได้เช่นกัน ถัดมาคือกระบวนการ “Incident Response” คือ การตอบสนองต่อสถานการณ์ไม่พึงประสงค์และไม่คาดคิดว่าจะเกิดขึ้น เพื่อให้องค์กรสามารถควบคุมสถานการณ์และมูลค่าความเสียหายที่เกิดขึ้นให้รวดเร็วทันการณ์และลดความเสียหายให้มากที่สุด ซึ่งการจัดทำปฏิบัติการ “Cyber Drill” เป็นเครื่องมือหนึ่งในการฝึกซ้อมให้ Incident Response Team หรือเจ้าหน้าที่ที่มีหน้าที่ตอบสนองต่อสถานการณ์ไม่พึงประสงค์ที่เกิดขึ้น ผลที่ได้คือถ้า Incident Response Team สามารถความคุมสถานการณ์ได้รวดเร็วมากเท่าไร มูลค่าความเสียหายที่เกิดจากสถานการณ์นั้นจะน้อยลงมากขึ้นเท่านั้น และขั้นสุดท้ายคือ “Cyber Resilience” คือ มีความสามารถในการทนทานต่อความเสียหายที่อาจเกิดขึ้นจากภัยคุกคามเหล่านั้น การทำให้เกิดสภาวะ “Cyber Resilience” จำเป็นต้องมีการสร้างกระบวนการ Incident Response เพื่อตอบสนองต่อ

สถานการณ์ไม่พึงประสงค์และผิดปกติได้อย่างรวดเร็ว ซึ่งต้องอาศัยการฝึกฝนจากการทำ Cyber Drill อยู่เป็นประจำ หากองค์กรต้องการมีความมั่นคงปลอดภัยอย่างยั่งยืน จำเป็นต้องรักษาวินัยทางไซเบอร์ทั้งสามข้อให้คงอยู่ในวัฒนธรรมองค์กร อยู่ในความนึกคิดและความเข้าใจของผู้บริการระดับสูงอยู่เสมอ จึงจะส่งผลในทางปฏิบัติ (ปริญญา หอมอเนก, 2561)

ผู้วิจัยสนใจในแนวคิดที่เกี่ยวข้องกับการเตรียมความพร้อมของหน่วยงานและองค์กร เพื่อนำมาศึกษาและวิจัยอย่างลึกซึ้งในการหาแนวทางการเตรียมความพร้อมรับมือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะในด้านการบริหารและการกำกับดูแลองค์กร ซึ่ง ITU Development (2012) ได้นิยามไว้ว่า ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) เป็นเรื่องสำคัญของการพัฒนาเทคโนโลยีข้อมูลข่าวสาร (Information Technology) ที่เกี่ยวข้องกับบริการอินเทอร์เน็ตที่จะต้องปกป้องข้อมูลข่าวสารไม่ให้ถูกทำลาย โดยเฉพาะเครือข่ายและข้อมูลข่าวสารของโครงสร้างสาธารณูปโภคพื้นฐานที่สำคัญหรือ Critical Information Infrastructures (CII) อาทิ เครือข่ายการสื่อสารของระบบการไฟฟ้า เครือข่ายการสื่อสารของระบบส่งก๊าซธรรมชาติ เครือข่ายโทรคมนาคม เป็นต้น ซึ่งล้วนส่งผลกระทบต่อเศรษฐกิจ และความมั่นคงของชาติ หากการรักษาความปลอดภัยบกพร่อง อย่างไรก็ตามภายในหน่วยงานหรือองค์กรทั่วโลก ส่วนใหญ่ยังขาดการวางมาตรการจัดการปัญหาที่มีประสิทธิภาพเพียงพอต่อการป้องกันภัยคุกคามทางไซเบอร์ โดยเฉพาะองค์กรด้านสาธารณูปโภคที่เป็นแหล่งเก็บรวบรวมข้อมูลส่วนบุคคลของผู้บริโภค และอาจตกเป็นเป้าหมายที่สำคัญของเหล่าอาชญากรไซเบอร์ หนทางในการแก้ไขปัญหาดังกล่าวจึงจำเป็นที่จะต้องมีการเร่งจัดการมาตรการความมั่นคงปลอดภัยทางไซเบอร์ภายในองค์กรเหล่านี้ เพื่อทำการปิดช่องโหว่ทางเทคโนโลยีคอมพิวเตอร์ อีกทั้งยังเป็นการเตรียมความพร้อมรับมือภัยคุกคามทางไซเบอร์ที่กำลังสร้างความปั่นป่วนให้กับสังคมไปทั่วโลก

2.5.7 การจัดตั้งศูนย์ปฏิบัติการไซเบอร์เฝ้าระวังและตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์

ศูนย์ปฏิบัติการไซเบอร์ 911 ของภาครัฐและเอกชน

จากแนวโน้มภัยคุกคามไซเบอร์ที่สูงขึ้นอย่างต่อเนื่อง ในปัจจุบันองค์กรต่าง ๆ จึงให้ความสำคัญในด้านความมั่นคงปลอดภัยไซเบอร์มากขึ้น โดยหนึ่งในการดำเนินการหลักที่องค์กรควรพิจารณา คือ การจัดตั้งศูนย์ปฏิบัติการไซเบอร์ (Security Operations Center – SOC หรือ Cyber Security Operations Center – CSOC) เพื่อเป็นศูนย์กลางในการเฝ้าระวังและรับมือภัยคุกคามทางไซเบอร์ขององค์กร ซึ่งเป็นส่วนหนึ่งในหน้าที่ของทีม CSIRT (Computer Security Incident Response Team) หน่วยงานรับมือเหตุภัยคุกคามที่อยู่ภายใต้สถาบันวิศวกรรมซอฟต์แวร์ (Software Engineering Institute – SEI) การดำเนินงานของ CSIRT และ SOC ไม่แตกต่างกันมาก

นักเพราะมีภารกิจที่คล้ายคลึงและทับซ้อนกันอยู่มาก ในบางกรณีอาจพบ CSIRT ตั้งอยู่ใน SOC ในขณะที่ CSIRT บางแห่งก็กำหนดให้ SOC เป็นเสมือนทีมหน้าด่านในการรับมือเมื่อเกิดเหตุภัยคุกคาม (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2561) ซึ่ง Cyber Security Operations Center (CSOC) คือ ศูนย์ปฏิบัติการที่มีทีมทำหน้าที่เฝ้าระวังภัยคุกคามขององค์กร ทำหน้าที่ตรวจสอบการเข้าถึงเครือข่ายและระบบสารสนเทศต่าง ๆ ขององค์กรตลอดเวลาแบบ 24/7 นั่นหมายความว่า ศูนย์ CSOC จะต้องมีเจ้าหน้าที่ผู้เชี่ยวชาญในการเฝ้าระวังภัยคุกคามตลอด 24 ชั่วโมง เมื่อตรวจพบเหตุการณ์ต้องสงสัย เจ้าหน้าที่จะทำการวิเคราะห์ข้อมูลแวดล้อมของเหตุการณ์ ประเมินระดับความรุนแรงของเหตุกาณ์ พร้อมทั้งให้คำแนะนำเบื้องต้นในการรับมือ จัดการกับปัญหาที่เกิดขึ้น เพื่อลดผลกระทบ และลดความเสียหายที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ รวมถึงการดำเนินธุรกิจ (บริษัทโทรคมนาคมแห่งชาติ, 2565) หากพบพฤติกรรมที่ผิดปกติ เช่น พบการละเมิดข้อมูลสำคัญ ๆ ขององค์กร ก็พร้อมตอบสนองต่อเหตุการณ์อย่างรวดเร็วและสามารถหยุดการโจมตีรวมทั้งเก็บข้อมูลเพื่อตรวจหาช่องทางที่อาชญากรบุกรุกเข้ามาได้อย่างแม่นยำ SOC ที่มีประสิทธิภาพ จะช่วยให้องค์กรสามารถรับรู้ถึงสถานการณ์ภัยคุกคามต่าง ๆ ในเครือข่ายของตนได้อย่างครอบคลุม และสามารถระบุถึงเหตุการณ์ผิดปกติได้อย่างรวดเร็วและแม่นยำ รวมถึงตอบสนองต่อเหตุการณ์นั้นได้ทันท่วงที นอกจากนี้ SOC ยังสามารถทำหน้าที่อื่น เช่น การวิเคราะห์ข้อมูลเชิงลึก การตรวจสอบหาช่องโหว่ในระบบ และการสร้างความตระหนักรู้ให้กับเจ้าหน้าที่ในองค์กร เป็นต้น

ศูนย์ปฏิบัติการเฝ้าระวังรักษาความปลอดภัยทางไซเบอร์ โครงประกอบของไซเบอร์ 911 เป็นแนวคิดใหม่ที่ออกแบบมาเพื่อการเฝ้าระวังภัยคุกคามความปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพสูงสุด โดยเริ่มจากการวิเคราะห์สภาพแวดล้อม ลักษณะ และโครงสร้างการปฏิบัติงาน รวมถึงประเภทของความเสี่ยงและภัยคุกคามที่แต่ละองค์กรมีความแตกต่างกัน จากนั้นจึงพัฒนาแผนและขั้นตอนในการตอบสนองต่อภัยคุกคาม และดำเนินการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ เพื่อวิเคราะห์ภัยคุกคามที่กำลังจะเกิดขึ้นและแจ้งเตือนไปยังทีมงาน ให้สามารถจัดการภัยคุกคามได้อย่างรวดเร็วตามแผนที่วางไว้ ซึ่งศูนย์ปฏิบัติการรักษาความปลอดภัยอันล้ำสมัยของไซเบอร์ตรอน เป็นบริการที่แตกต่างจาก SOC แบบเดิม ๆ ตรงที่ดำเนินการตามกรอบการทำงานที่เป็นที่ยอมรับในระดับสากล โดยการปฏิรูปและปรับให้เหมาะสม ไม่เพียงเพื่อการตรวจจับที่รวดเร็วเท่านั้น แต่ยังตอบสนองอย่างรวดเร็วต่อทุกภัยคุกคามที่เกิดขึ้น ที่จะได้รับแจ้งเตือนและตรวจสอบโดยทีมผู้เชี่ยวชาญที่ผ่านการรับรองระดับสากล ทั้งนี้ ยังคงรักษาฟังก์ชั่นทางธุรกิจและสร้างความมั่นใจว่าจะเกิดผลกระทบน้อยที่สุด ภัยคุกคามแต่ละรายการจะได้รับการตอบสนองโดยกระบวนการที่ปรับแต่งให้เหมาะกับธุรกิจของลูกค้าแต่ละราย จากนั้นจึงดำเนินการด้านการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล และการสอบสวนโดยทีมงานที่เชี่ยวชาญเฉพาะด้าน ศึกษาการเกิดขึ้นที่ต้นเหตุ และใช้การควบคุมที่จำเป็น

ถือเป็นการสร้างความมั่นใจในความยืดหยุ่นทางไซเบอร์สำหรับการรักษาความปลอดภัยไซเบอร์ของ Cyber911 ประกอบด้วย การวิเคราะห์ผลกระทบทางธุรกิจ การประเมินช่องโหว่/การทดสอบเจาะระบบ การบริหารจัดการความเสี่ยง แผนตอบสนองเหตุการณ์ การฝึกอบรมการรับรู้ การฝึกซ้อมความตระหนักรู้ทางด้านไซเบอร์ (Cyber Drill) เป็นต้น (ไซเบอตรอน, 2565)

สำหรับในประเทศไทย กระทรวงกลาโหม เป็นอีกส่วนราชการหนึ่งที่ตระหนักถึงความสำคัญของเรื่องความมั่นคงปลอดภัยทางไซเบอร์ จึงได้กำหนดแนวทางในการเผชิญภัยคุกคามด้วยการประกาศใช้แผนแม่บทไซเบอร์เพื่อการป้องกันประเทศกระทรวงกลาโหม พ.ศ.๒๕๖๐ – ๒๕๖๔ และกำหนดแนวทางในการใช้ประโยชน์จากกำลังพลสำรองที่มีความรู้ ทักษะงานด้านไซเบอร์เป็นกำหลังสำคัญในการดำเนินการการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ และให้ความสำคัญในการรักษาความปลอดภัยด้านไซเบอร์ว่าเป็นภัยคุกคามต่อความมั่นคงของชาติในมิติต่างๆ โดยหนึ่งในสาระสำคัญคือ แผนป้องกันระบบโครงสร้างพื้นฐาน โดยเตรียมจัดตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Operation Center ; CSOC) ของแต่ละส่วนราชการขึ้นมาเพื่อรองรับภัยคุกคามด้านไซเบอร์ที่จะมาโจมตีระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งจัดทำระบบฐานข้อมูล นอกจากนี้ยังจะมีการจัดตั้ง ทีมจัดการปัญหาฉุกเฉินด้านความมั่นคงปลอดภัยทางไซเบอร์(Cyber Security Incident Response Team / Computer Security Incident Response Team ; CSIRT) เพื่อตอบสนองการแก้ไขปัญหาฉุกเฉินด้านความปลอดภัยไซเบอร์ ได้อย่างรวดเร็ว และทันเวลา (สุปรีดี ประวิตร, 2561)

อย่างไรก็ตาม องค์กรส่วนใหญ่ไม่สามารถมีศูนย์ CSOC แบบ 24/7 ได้ เพราะต้นทุนในการดำเนินงานนั้นสูง หลายองค์กรมองว่าไม่คุ้มค่ากับผลประโยชน์ที่ได้รับ จึงใช้วิธี “ยืม” พนักงานจากตำแหน่งอื่นเพื่อทำหน้าที่เฝ้าระวังภัยคุกคามแทนการสร้างทีม CSOC ขึ้นมาเอง ผลคือการตรวจจับภัยและการตอบสนองจึงล่าช้ากว่าที่ควรเป็น โดยพนักงานที่ปฏิบัติงานทีม SOC นั้นจะต้องมีความรู้ความสามารถเฉพาะทาง สามารถ Automate งานภายในศูนย์ของ CSOC ให้มากที่สุด ซึ่งการ automation จะทำให้สามารถ monitoring และตอบสนองต่อ incident ได้ทันการ เพราะในการสร้างระบบ automation จำเป็นจะต้องเรียนรู้พื้นฐาน Threat Lifecycle Management Platform ด้วย (บริษัทโทรคมนาคมแห่งชาติ, 2565)

ผู้วิจัยสนใจประเด็นการจัดตั้งศูนย์ปฏิบัติการไซเบอร์เพื่อเฝ้าระวังภัยคุกคาม เนื่องด้วยแนวโน้มภัยคุกคามไซเบอร์ที่สูงขึ้นอย่างต่อเนื่อง แต่หลายองค์กรยังมีการเตรียมความพร้อมรับมือภัยคุกคามที่ไม่ครอบคลุมทุกด้าน และต้องเผชิญภัยคุกคามในรูปแบบใหม่อยู่เสมอ แม้เป็นภัยคุกคามที่อยู่ในระดับไม่ร้ายแรง แต่ก็สร้างความปั่นป่วนให้หลายองค์กรต้องเร่งหาวิธีใหม่ๆเพื่อจัดการการ

โจมตีทางไซเบอร์ การขาดบุคลากรที่เชี่ยวชาญและความไม่เข้าใจสภาพแวดล้อมของระบบสารสนเทศ ทำให้เป็นอุปสรรคในการเตรียมความพร้อมจัดตั้งศูนย์ไซเบอร์ดังกล่าว ผู้วิจัยเห็นว่า การสร้างความตระหนักรู้สัมพันธ์กับการพัฒนาศักยภาพของบุคลากรในองค์กร เพื่อให้พร้อมในการจัดเตรียมเจ้าหน้าที่ที่จะปฏิบัติงานในศูนย์ปฏิบัติการไซเบอร์ดังกล่าว อีกทั้งตำแหน่งและหน้าที่ของเจ้าหน้าที่ SOC ต้องมีความเข้าใจอย่างถ่องแท้ในโครงสร้างและสถาปัตยกรรมระบบ แผนผังโครงสร้างเครือข่าย (Network Diagram) และมาตรการด้านความมั่นคงปลอดภัย มีการจัดทำบัญชีทรัพย์สินสารสนเทศที่ต้องเฝ้าระวังทั้งหมด เพื่อให้สามารถวิเคราะห์และหาความสัมพันธ์ของเหตุการณ์โจมตี ที่เกิดขึ้น รวมถึงตรวจสอบช่องโหว่ในระบบได้อย่างถูกต้อง นอกจากนี้ เจ้าหน้าที่ SOC ควรหมั่นตรวจสอบความถูกต้องของระบบ SIEM หรือระบบจัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่าย เพื่อให้มั่นใจได้ว่าล็อค (log) จากอุปกรณ์เครือข่ายต่าง ๆ ได้รับการบันทึกอย่างครบถ้วน องค์กรจึงจำเป็นต้องมีการกำหนดขอบเขตหน้าที่ของ SOC และเตรียมความพร้อมอย่างต่อเนื่องเพื่อป้องกันภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้นได้ในอนาคต

2.6 งานวิจัยที่เกี่ยวข้อง

การวิจัยเรื่อง **การปรับปรุงการจัดลำดับความสำคัญของช่องโหว่ตามพื้นฐานของ CVSS และการตอบสนองด้วยบริบทของข้อมูล (Improving CVSS-based Vulnerability Prioritization and Response with Context Information)** ของ C. Fruhwirth and T. Mannisto. (2552) ผลการศึกษาพบว่า การแก้ไขช่องโหว่เป็นงานที่ใช้แรงงานและค่าใช้จ่ายจำนวนมาก จึงได้นำเสนอวิธีที่ช่วยให้ผู้จัดการด้านความมั่นคงมีข้อมูลประกอบการตัดสินใจลงทุนในการจัดลำดับความสำคัญของช่องโหว่ในองค์กรให้ดีขึ้น และรายการช่องโหว่ที่นำมาคำนวณมาจากเอ็นวีดี (NVD) แต่เอ็นวีดีได้ให้คะแนนซีวีเอสเอส (CVSS) ไว้เพียงแค่กลุ่มตัววัดพื้นฐานเท่านั้น อย่างไรก็ตาม ผู้จัดการด้านความมั่นคงทราบว่า ความรุนแรงของช่องโหว่จะแตกต่างกันมากในบริบทขององค์กรที่แตกต่างกัน ดังนั้น คะแนน CVSS ที่ให้โดย NVD จึงไม่เพียงพอที่จะจัดลำดับความสำคัญของช่องโหว่ ซึ่งในงานวิจัยนี้ได้เปรียบเทียบ 2 สถานการณ์เพื่อจัดลำดับความสำคัญของช่องโหว่ในองค์กร คือ สถานการณ์แรกเป็นการประเมินผลกระทบของช่องโหว่ด้วยคะแนน CVSS โดยใช้กลุ่มตัววัดพื้นฐานเท่านั้น ส่วนอีกสถานการณ์เป็นการประเมินผลกระทบของช่องโหว่ด้วยคะแนน CVSS ทั้ง 3 กลุ่ม ซึ่งคะแนน CVSS ในส่วนของกลุ่มตัววัดตามสภาพแวดล้อมที่เกี่ยวข้องกับผลกระทบจากการสูญเสียองค์ประกอบด้านความมั่นคง ซึ่งผลกระทบที่เป็นไปได้ทั้งหมดคือ High, Medium หรือ Low ผู้วิจัยให้ระดับผลกระทบเริ่มต้นเป็น Medium หลังจากนั้นจึงไปสัมภาษณ์ผู้จัดการด้านความมั่นคงจากหลายองค์กรเพื่อให้จัดลำดับผลกระทบจากการสูญเสียการรักษาความลับ บูรณภาพ และสภาพพร้อมใช้งาน โดยให้ระบุว่าการสูญเสียด้านใดจะมีผลกระทบมากที่สุด (ระบุเป็น High) และการสูญเสียด้าน

ใดจะมีผลกระทบน้อยที่สุด (ระบุเป็น Low) จากการสัมภาษณ์จะได้ผลสรุปว่า ผลกระทบจากการสูญเสียการรักษาความลับ บูรณภาพ และสภาพพร้อมใช้งาน เป็น Medium Low และ High ตามลำดับ จากนั้นจึงนำระดับผลกระทบนี้ไปใช้คำนวณคะแนน CVSS เมื่อได้คำนวณคะแนน CVSS ของทั้งสองสถานการณ์เปรียบเทียบกันแล้ว พบว่า สถานการณ์ที่สองสะท้อนความรุนแรงที่แท้จริงของช่องโหว่จากมุมมองขององค์กรได้ดีขึ้น และผู้จัดการด้านความมั่นคงสามารถเลือกจัดการช่องโหว่ได้อย่างมีประสิทธิภาพมากขึ้น

การวิจัยเรื่อง **การวางแผนรองรับเหตุการณ์ฉุกเฉินเพื่อความมั่นคงสารสนเทศในองค์กร** ของ ณัฐวี อุตกฤษฎ์ (2555) ผลการศึกษาพบว่า การวางแผนรองรับเหตุการณ์ฉุกเฉินเพื่อความมั่นคงของสารสนเทศในองค์กร คือการเตรียมการรับเหตุการณ์ฉุกเฉินที่คุกคามต่อสารสนเทศ ซึ่งองค์กรควรให้ความสำคัญเพราะบางครั้งองค์กรอาจอยู่ในสภาวะที่ไม่สามารถรองรับและตอบสนองเหตุการณ์ดังกล่าวได้ด้วยการปฏิบัติตามแผนปกติ การวิจัยชิ้นนี้จึงมุ่งเน้นให้เห็นถึงความสำคัญของการวางแผนรองรับสำหรับเหตุการณ์ฉุกเฉินในองค์กรและอธิบายถึงขั้นตอนของการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินโดยพิจารณาตามแนวทางปฏิบัติของ NIST SP 800-34 และส่วนประกอบหลัก 4 ประการของแผนรองรับเหตุการณ์ฉุกเฉิน ได้แก่ (1) การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) (2) การวางแผนเพื่อตอบสนองต่อเหตุการณ์ที่ไม่คาดคิด (Incident Response Plan: IRP) (3) การวางแผนฟื้นฟูเหตุการณ์จากความเสียหายที่รุนแรง (Disaster Recovery Plan: DRP) และ (4) การวางแผนเพื่อดำเนินธุรกิจต่อไปได้ในสถานการณ์ฉุกเฉินที่รุนแรง (Business Continuity Plan: BCP)

การวิจัยเรื่อง **การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหม** ของ ศิวลีย์ สิริโรจน์บริรักษ์ (2558) ผลการศึกษาพบว่า (1) กรอบนโยบาย ยุทธศาสตร์ และการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหม ได้แก่ พ.ร.บ. ว่าด้วยการจัดระเบียบราชการด้านเทคโนโลยีสารสนเทศและการสื่อสารของ กห. พ.ศ. 2551, นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กห. พ.ศ. 2554, ยุทธศาสตร์ กห. อิเล็กทรอนิกส์ (e-Defence), แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของ กห. ฉบับที่ 3 พ.ศ. 2557-2561, การจัดตั้งศูนย์บัญชาการไซเบอร์ กห. (2) มาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล ได้แก่ มาตรฐาน U.S. DoD, มาตรฐาน ISO 27001: 2005, มาตรฐาน FIPS PUB 200, มาตรฐาน NIST 800-14, มาตรฐาน COBIT, และมาตรฐาน IT BPM (3) แนวทางในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กห. ให้ได้มาตรฐานในระดับสากล เชิงนโยบาย ได้แก่ ส่วนบังคับการ ต้องเปิดอัตรานายทหารสงครามข้อมูล

ข่าวสาร เพื่อดำเนินการตอบสนองต่อปัญหา/เหตุการณ์บุกรุกระบบของหน่วยขึ้นตรงได้อย่างรวดเร็ว ส่วนนโยบายและแผน ต้องมีการบรรจุข้อกำหนดในกระบวนการจัดซื้อจัดจ้าง อุปกรณ์ฮาร์ดแวร์และซอฟต์แวร์ เพื่อให้อุปกรณ์มีความปลอดภัยในระดับสากล ส่วนปฏิบัติการไซเบอร์ จะต้องมีหน่วยปฏิบัติการเชิงรับและเชิงรุก สงครามข้อมูลข่าวสาร ส่วนวิจัยและพัฒนาไซเบอร์จะต้องจัดตั้งส่วนงานวิจัยระบบสงครามข้อมูลข่าวสาร เพื่อพัฒนาระบบการรักษาความปลอดภัยของข้อมูลข่าวสารให้มีประสิทธิภาพมากยิ่งขึ้น และต้องบรรจุอัตราจเรทหารที่มีความเชี่ยวชาญเฉพาะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อดำเนินการตรวจสอบตามหลักการ ICT Audit เชิงปฏิบัติ ได้แก่ (1) ควรจัดทำหลักสูตร Cyber Training เพื่ออบรมความรู้เกี่ยวกับการใช้งานซอฟต์แวร์ และฮาร์ดแวร์ รวมทั้งการให้ทุนการศึกษาต่อในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แก่บุคลากรทุกระดับ (2) ควรมีการจัดการองค์ความรู้ด้านไซเบอร์ ในหน่วยงานและควรนำ E-Document มาใช้ในการปฏิบัติราชการมากยิ่งขึ้น

การวิจัยเรื่อง **ยุทธศาสตร์การพัฒนากำลังพลของกองทัพไทยเพื่อต่อต้านภัยคุกคามไซเบอร์ในทศวรรษหน้า** ของ ปรัชญา ฮวดปากน้ำ (2559) ผลการสึกษาพบว่า ผู้เชี่ยวชาญจากภาคเอกชน และผู้รับผิดชอบโดยตรงจากกองบัญชาการกองทัพไทย กองทัพบก กองทัพเรือ กองทัพอากาศ ได้ร่วมกันวิเคราะห์จุดอ่อน จุดแข็ง โอกาส และอุปสรรค ภายใต้สภาวะแวดล้อมปัจจุบันและอนาคตในระยะสิบปีข้างหน้าเพื่อกำหนดเป็นยุทธศาสตร์ผลการวิจัยทำให้ทราบถึง (1) ปัญหาความไม่พร้อมของหน่วยงานและกำลังพลของกองทัพไทยตลอดจนภัยคุกคามในปัจจุบันและแนวโน้มของภัยคุกคามที่จะเกิดขึ้นในอนาคตและส่งผลกระทบต่อความปลอดภัยของการใช้ข้อมูลข่าวสารในการปฏิบัติงานรักษาความมั่นคงของกองทัพไทยบนพื้นฐานของความปลอดภัยของข้อมูล หรือ Cia 3 ประการ ได้แก่ การรักษาความลับของข้อมูล การรักษาความคงสภาพของข้อมูลหรือความสมบูรณ์ของข้อมูล(Integrity) และความพร้อมใช้งานของข้อมูล (Availability) สิ่งที่จำเป็นอย่างยิ่งในการที่จะรับมือกับปัญหาหรือภัยคุกคามต่าง ๆ เหล่านี้ประการหนึ่ง คือ การสร้างความตระหนัก (Awareness) ให้แก่บุคลากรภายในองค์กร (2) การเตรียมแผนสำหรับการบูรณาการ ความรู้ความสามารถ ทักษะ เจตคติ ให้กำลังพลของกองทัพไทยมีขีดสมรรถนะเพียงพอในการปฏิบัติการต่อต้านภัยคุกคามไซเบอร์โดยการเสริมสร้างองค์ความรู้ทั้งในด้านทฤษฎี และการฝึกฝนให้เกิดความเชี่ยวชาญในการปฏิบัติการต่อต้านภัยคุกคามไซเบอร์ ทั้งการป้องกัน (Prevent) ค้นหา (Detect) และตอบสนองเหตุการณ์ (Incident Response) ตลอดจนการปรับเจตคติให้กับกำลังพลของกองทัพมีความตื่นตัวเพิ่มความระมัดระวังในการปิดช่องโหว่ต่าง ๆ ทั้งในระหว่างการปฏิบัติงานและการใช้ชีวิตประจำวัน ไม่ให้ผู้ไม่ประสงค์ดีสามารถใช้ช่องทางไซเบอร์เข้าโจมตีได้โดยง่ายตลอดจนทราบถึงความจำเป็นในการปรับปรุงโครงสร้างหน่วยงานสงครามไซเบอร์ของกองทัพ จัดเตรียมสรรหา ผลิต

และพัฒนาบุคลากรสำหรับการต่อต้านภัยคุกคามไซเบอร์และ (3) ได้ยุทธศาสตร์แนวทางพัฒนากำลังพลกองทัพไทยสำหรับต่อต้านภัยคุกคามไซเบอร์ให้มีความพร้อมรับสถานการณ์ในห้วงสิบปีข้างหน้าโดยมีรูปแบบของยุทธศาสตร์และแผนการพัฒนากำลังพลของกองทัพไทยสำหรับต่อต้านภัยคุกคามไซเบอร์

การวิจัยเรื่อง **อาชญากรรมไซเบอร์ และการกำกับดูแลเครือข่าย (Cybercrimes and Network Governance)** ของ Anna Lucia Valvo (2559) ผลการศึกษาพบว่า ปัญหาอาชญากรรมไซเบอร์จะรุนแรงมากขึ้นหากไม่มีความร่วมมือระหว่างภาครัฐและเอกชนในพื้นที่ รวมถึงการขาดความสามารถของสถาบันในการควบคุม ซึ่งคณะกรรมาธิการยุโรปได้ยอมรับความล้มเหลวของประเทศสมาชิกในการผลิตกฎหมายที่ตอบสนองต่อกิจกรรมทางอาญาใหม่ ๆ ซึ่งปัจจุบันยังไม่มีหมวดหมู่ทางกฎหมายที่ชัดเจนที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ยกเว้นอนุสัญญาบูดาเปสต์ฉบับที่ 185/2001 โดยเครื่องมือระหว่างประเทศที่สำคัญในสาขานี้คืออนุสัญญาของสภายุโรปเกี่ยวกับอาชญากรรมไซเบอร์ซึ่งมีผลบังคับใช้ในปี 2547 ระกอบด้วยคำนิยามทั่วไปของอาชญากรรมไซเบอร์ชนิดต่าง ๆ และการวางรากฐานความร่วมมือด้านการพิจารณาคดีระหว่างรัฐที่เข้าร่วม ลงนามโดยรัฐสมาชิกสหภาพยุโรปทั้งหมดและประเทศอื่น ๆ ที่ไม่ใช่ยุโรป เช่นสหรัฐอเมริกา แคนาดา ญี่ปุ่น และแอฟริกา อย่างไรก็ตาม อนุสัญญาบูดาเปสต์เมื่อวันที่ 23 พฤศจิกายน 2544 ยังคงไม่ได้รับการยอมรับจากทุกรัฐ แม้รัฐเหล่านี้จะให้สัตยาบันต่ออนุสัญญาแล้วก็ตาม แต่ก็ยังไม่ได้ให้สัตยาบันต่อระเบียบที่เพิ่มเติมเกี่ยวกับการเหยียดสีผิวหรือการทำให้หวาดกลัวโดยใช้ระบบคอมพิวเตอร์อนุสัญญาดังกล่าวได้รับการพิจารณาโดยคำนึงถึงความสมดุล

การวิจัยเรื่อง **การใช้งานสื่อสังคมออนไลน์สาธารณะมีผลกระทบต่อความมั่นคงปลอดภัยของกองทัพไทย** ของ วีรวดี ขุขันธิน (2560) ผลการศึกษาพบว่า การที่สื่อสังคมออนไลน์สาธารณะอาจทำให้เกิดช่องทางให้ผู้ประสงค์ร้ายสามารถเข้าสู่ระบบการรักษาความปลอดภัยของกองทัพได้ และอาจรอคอยโจมตีในเวลาที่เหมาะสม ทำให้เกิดภัยอันตรายต่อองค์กร ไม่ว่าจะการขโมยข้อมูลส่วนตัว ข้อมูลสำคัญต่าง ๆ ขององค์กร การปลอมตัวเป็นบุคคลอื่นในโลกสังคมออนไลน์ และการทำสงครามไซเบอร์ (Cyber Warfare) แนวทางป้องกันและแก้ไขปัญหาทำได้โดยการควบคุมการใช้งาน การให้ความรู้แก่ผู้ใช้งานทุกระดับ รวมถึงต้องปลูกฝังจิตสำนึก และค่านิยมในการใช้งานสื่อออนไลน์ที่ถูกต้องควบคู่ไปกับการบังคับใช้กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ การวางมาตรการป้องกัน กำหนดนโยบายการปฏิบัติอย่างจริงจัง โดยให้ผู้มีอำนาจลงมากำกับดูแลอย่างใกล้ชิด และการประสานความร่วมมือและเสริมสร้างเครือข่ายกับภาคเอกชน ภาควิชาการ การเสริมสร้างความร่วมมือระหว่างประเทศ

การวิจัยเรื่อง **โลกของความมั่นคงปลอดภัยไซเบอร์ และอาชญากรรมไซเบอร์ (World of Cyber Security and Cybercrime)** ของ Rachna Buch, Dhatri Ganda, Pooja Kalola, Nirala Borad (2561) ผลการศึกษาพบว่า ปัญหาอาชญากรรมไซเบอร์เป็นหนึ่งในปัญหาอาชญากรรมหลักที่กระทำโดยผู้เชี่ยวชาญด้านคอมพิวเตอร์ โดยการสร้างความก่อกวนในเครือข่าย (network) พร้อมทั้งจารกรรมข้อมูลสำคัญและข้อมูลส่วนบุคคล โดยมักจะเป็นข้อมูลบัญชีธนาคาร เพื่อโอนเงินจากบัญชีของเหยื่อไปยังบัญชีตนเอง ซึ่งอุปกรณ์อัจฉริยะใด ๆ ที่สามารถส่งผ่านข้อมูลไปยังอุปกรณ์อื่นได้ ไม่ว่าจะผ่านเครือข่ายหรือไม่ก็ตามนั้นรวมอยู่ในขอบเขตของความปลอดภัยทางไซเบอร์ ในปัจจุบัน ทุกคนควรต้องตระหนักถึงความปลอดภัยในโลกไซเบอร์เช่นเดียวกับอาชญากรรมไซเบอร์ รวมทั้งทราบถึงสาเหตุการเกิด โดยความปลอดภัยที่เกี่ยวกับกิจกรรมผ่านทางสังคมออนไลน์อาจมีความเสี่ยงเพิ่มสูงขึ้นทุกวัน เนื่องจากอาจเกิดเหตุข้อมูลสูญหาย การแก้ไขข้อมูล การลบข้อมูลที่เป็นประโยชน์ เช่น รายละเอียดส่วนบุคคล รหัสเข้าบัญชีอีเมล บัญชีสังคมออนไลน์ หรือบัญชีธนาคาร อย่างไรก็ตามคนบางคนอาจจะทราบกฎหมายที่จะต่อสู้กับอาชญากรรมไซเบอร์ หรือกฎหมายไซเบอร์และการกระทำที่จะต้องดำเนินการเพื่อต่อสู้กับอาชญากรรม

การวิจัยเรื่อง **ความเสี่ยงด้านไซเบอร์สำหรับกลุ่มการเงิน: กรอบการประเมินเชิงปริมาณ(Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment)** ของ Antoine Bouveret (2561) โดยผลการศึกษาพบว่า ทั้งธนาคารกลางและธุรกิจเทคโนโลยีการเงิน อย่างไรก็ตามข้อมูลเกี่ยวกับเหตุการณ์ไซเบอร์นั้นหายากและไม่ค่อยมีการวิเคราะห์ความเสี่ยงไซเบอร์เชิงปริมาณซึ่งการที่ข้อมูลหายาก เนื่องจากไม่มีการกำหนดมาตรฐานในการจัดเก็บข้อมูล และบริษัทไม่ได้รับแรงจูงใจให้รายงานเหตุการณ์เหล่านี้ ยิ่งไปกว่านั้น การแบ่งปันข้อมูลระหว่างประเทศที่รายงานต่อหน่วยงานกำกับดูแลท้องถิ่นนั้น นอกจากต้องคำนึงถึงความเป็นส่วนตัวและข้อจำกัดอื่น ๆ แล้วนั้น จะต้องคำนึงถึงความมั่นคงของชาติในการแบ่งปันและรายงานข้อมูลภาคการเงินมีความเสี่ยงสูงจากการโจมตีทางไซเบอร์ในทุกประเทศ ทั้งนี้กลุ่มประเทศเศรษฐกิจขั้นสูงและตลาดเกิดใหม่ส่วนใหญ่มีดัชนีความมั่นคงปลอดภัยทางไซเบอร์สูงกว่าประเทศที่มีรายได้ปานกลาง และรายได้ต่ำ ซึ่งภาคการเงินมากกว่า 50 ประเทศทั่วโลกเคยเป็นเหยื่อการโจมตีทางไซเบอร์ในช่วง 2-3 ปีที่ผ่านมา และการโจมตีส่วนใหญ่เกิดขึ้นในอเมริกา อย่างไรก็ตามการโจมตีทางไซเบอร์ไม่สัมพันธ์กับขนาดของธุรกิจ จากข้อมูลพบว่า การสูญเสียขนาดใหญ่ที่สุดเกิดขึ้นในสถาบันการเงินขนาดเล็ก เนื่องจากมีการลงทุนด้านความปลอดภัยทางไอทีน้อย การโจมตีทางไซเบอร์ต่อธนาคารกลางมักเกิดขึ้น 3 ประเภท คือ การฉ้อโกง ร้อยละ 43 การละเมิดข้อมูล ร้อยละ 34 และการทำให้ธุรกิจหยุดชะงัก ร้อยละ 23 ซึ่งการฉ้อโกงและการละเมิดข้อมูลนั้นมีแนวโน้มที่จะแพร่หลายมากขึ้น ในกรณีพื้นฐาน ผลการสูญเสียเฉลี่ยจากการโจมตีทางไซเบอร์สำหรับประเทศในกลุ่มตัวอย่าง มีมูลค่า 97 พันล้านเหรียญสหรัฐหรือร้อยละ 9 ของกำไรสุทธิของธนาคาร การสูญเสียบางครั้งนั้น

มีขนาดใหญ่เกินกว่าการประกันจะครอบคลุมได้ซึ่งเบี้ยประกันเติบโตสูงถึง 3 พันล้านเหรียญสหรัฐและคาดว่าจะสูงถึง 12-20 พันล้านเหรียญสหรัฐในอีก 10 ปีข้างหน้า อย่างไรก็ตามสถาบันการเงินส่วนใหญ่ไม่มีการทำประกันทางไซเบอร์

การวิจัยเรื่อง **ความท้าทายด้านความมั่นคงปลอดภัยไซเบอร์ และแนวโน้มที่อาจเกิดขึ้นจากเทคโนโลยีใหม่ ๆ (Cyber Security challenges and its emerging trends on latest technologies)** ของ Rajasekharaiah K.M, Chhaya S Dule, Sudarshan E. (2563) ผลการศึกษาพบว่า ปัญหาที่เกี่ยวกับอาชญากรรมไซเบอร์ที่เกิดขึ้นในประเทศมาเลเซียระหว่างเดือนมกราคมปี 2555 ถึงเดือนมิถุนายน ปี 2556 มีแนวโน้มเพิ่มสูงขึ้นอย่างมีนัยสำคัญ และเมื่อปัญหาอาชญากรรมไซเบอร์เพิ่มมากขึ้น จึงต้องมีการปรับมาตรการด้านความมั่นคงปลอดภัยทางไซเบอร์เพิ่มขึ้นตาม แนวทางการใช้คอมพิวเตอร์ในรูปแบบต่าง ๆ มีผลกระทบต่อความปลอดภัยด้านไซเบอร์ โดยรูปแบบที่ส่งผลกระทบอย่างมาก ได้แก่ Web servers, Cloud computing, Advanced Persistent Threat (APT), Mobile Networks, IPv6, Encryption of the code และในปัจจุบันที่ผู้คนใช้สื่อสังคมออนไลน์เพิ่มมากขึ้นทุกวัน ทำให้สิ่งเหล่านี้กลายเป็นรูปแบบ (Platform) หลักที่อาชญากรจะใช้ในการโจมตีขโมยข้อมูลส่วนตัวหรือข้อมูลที่สำคัญ ซึ่งผู้ใช้บริการสื่อสังคมออนไลน์มักจะส่งมอบข้อมูลส่วนตัวให้บริษัทผู้ดูแลระบบง่ายมากขึ้น

จากการศึกษาที่มาของสถานการณ์ภัยคุกคามทางไซเบอร์และการทบทวนวรรณกรรม เพื่อทำความเข้าใจถึงลักษณะและรูปแบบภัยคุกคามไซเบอร์ที่เกิดขึ้นกับหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศ ทำให้ทราบถึงสาเหตุของปัญหาของเหตุการณ์ภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยทั้งในระดับองค์กรและระดับประเทศ การศึกษาโครงสร้างการกำกับดูแล การขับเคลื่อนนโยบายและกฎหมายที่สำคัญและเกี่ยวข้องกับการป้องกันและการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงมาตรการต่างๆที่ภาครัฐนำมาบังคับใช้ การสนับสนุนข้อมูลที่ได้มาจากแนวคิด ทฤษฎีอาชญาวิทยา และข้อมูลเชิงประจักษ์จากงานวิจัยที่เกี่ยวข้อง นำไปสู่การสร้างกรอบแนวคิดในการวิจัยเพื่อศึกษากระบวนการการรับมือภัยคุกคามทางไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ เพื่อหาแนวทางการเตรียมแผนการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์และการกำกับดูแลการบริหารจัดการที่ดีด้านเทคโนโลยีดิจิทัล และความมั่นคงปลอดภัยไซเบอร์ทั้งด้านกฎหมาย ด้านองค์กร และด้านทรัพยากรทางเทคโนโลยี รวมถึงการสร้างความตระหนักรู้ของบุคลากรในองค์กร นำไปสู่มาตรการเชิงนโยบายและมาตรการเชิงปฏิบัติการ เพื่อลดความเสี่ยงและป้องกันภัยคุกคามทางไซเบอร์ในอนาคต

กรอบแนวคิดของการวิจัย

งานวิจัยนี้เป็นการวิจัยเชิงคุณภาพผ่านการวิเคราะห์ข้อมูลทั้งแบบปฐมภูมิและทุติยภูมิเพื่อสำรวจภัยสถานการณ์ภัยคุกคามไซเบอร์ตั้งแต่อดีตถึงปัจจุบันผ่านองค์กรตัวอย่าง และเสนอแนะแนวทางการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์สำหรับองค์กรทั้งภาครัฐและเอกชน เพื่อใช้ในการจัดตั้งศูนย์ปฏิบัติการไซเบอร์ในการเฝ้าระวังภัยคุกคามที่มีประสิทธิผลและประสิทธิภาพ ทั้งยังเพิ่มโอกาสในการบรรลุความสำเร็จตามยุทธศาสตร์ชาติที่เกี่ยวข้องโดยดำเนินการดังนี้

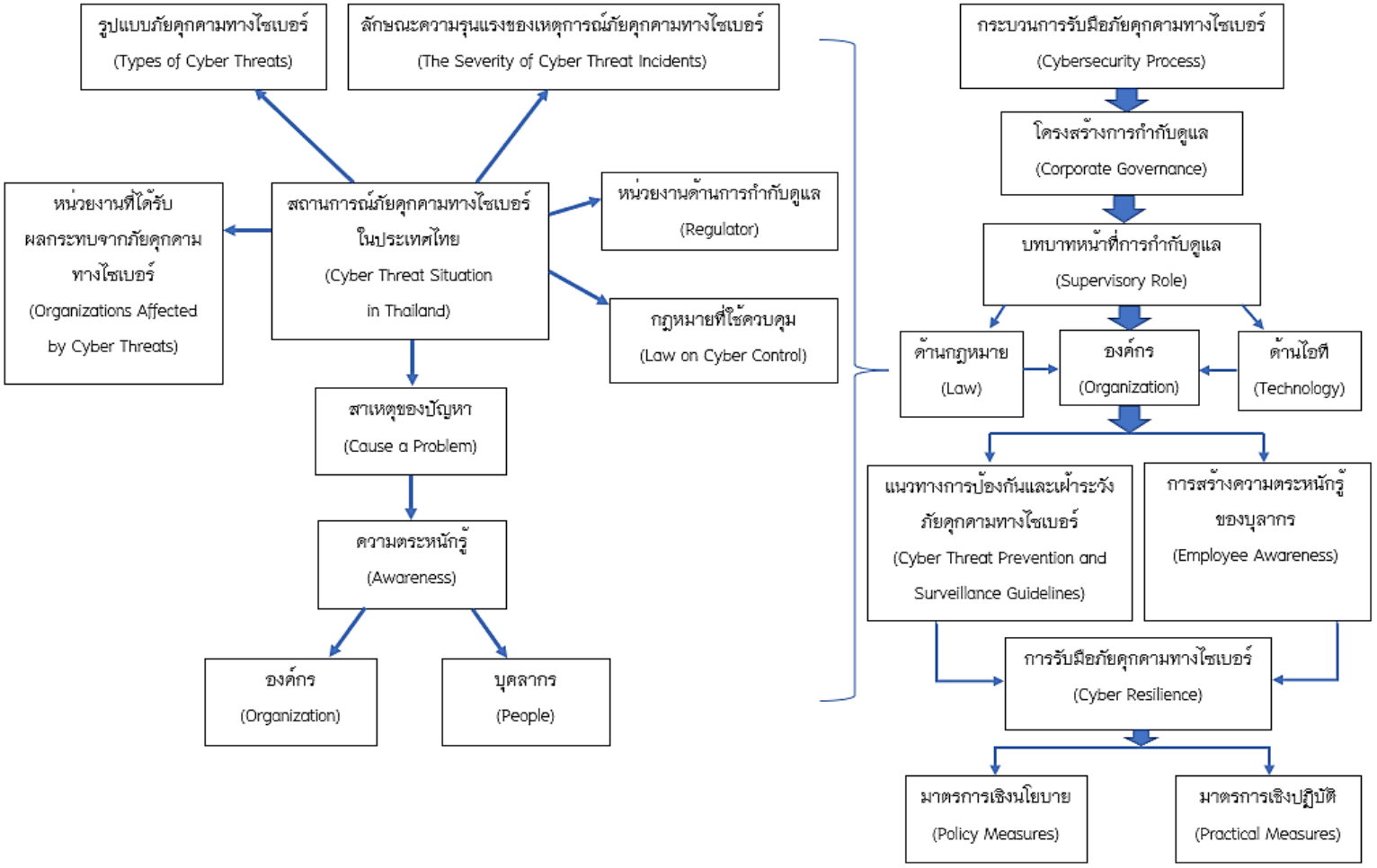
1. ศึกษาสาระและความเชื่อมโยงของ ยุทธศาสตร์ชาติ แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และกฎหมายที่เกี่ยวข้อง

2. สำรวจแนวทางในการจัดการ รวมทั้งข้อพึงปฏิบัติ และข้อจำกัดต่างๆ จากกรอบการดำเนินงาน มาตรฐาน รายงานสำรวจ และงานวิจัย ที่เกี่ยวข้อง

3. สำรวจประสิทธิผลและประสิทธิภาพ มาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์ในการเฝ้าระวังภัยคุกคามทางไซเบอร์ รวมทั้งสัมภาษณ์ความเห็นและแนวคิดจากผู้เกี่ยวข้องในระดับบริหาร

4. วิเคราะห์ข้อมูลที่ได้จากข้อ 1-3 เพื่อหาแนวทางการกำกับดูแลและแนวปฏิบัติที่ดี (Best Practice) ในการรักษาความมั่นคงปลอดภัยไซเบอร์ให้เกิดประสิทธิผลอย่างมีประสิทธิภาพ เพื่อเฝ้าระวังและเตรียมความพร้อมรับมือภัยคุกคามไซเบอร์ที่อาจจะเกิดขึ้นในอนาคตทั้งในระดับนโยบาย แนวทางปฏิบัติสำหรับองค์กรและนโยบายระดับประเทศโดยสะท้อนจากองค์กรตัวอย่าง

กรอบแนวคิดในการวิจัย



ภาพที่ 11 กรอบแนวคิดการวิจัย

บทที่ 3
ระเบียบวิธีวิจัย

ในการดำเนินตามการศึกษาวิจัยเรื่อง แนวทางการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ขององค์กรในยุคดิจิทัลนั้น โดยภาพรวมของการกำหนดระเบียบวิธีการวิจัยหรือกระบวนวิธีการวิจัย (Methodology) เป็นกระบวนวิธีการวิจัยเชิงคุณภาพ (Qualitative Research) ด้วยการศึกษาจากเอกสาร(Documentary Research) และการสัมภาษณ์เชิงลึก (In-depth Interview) จากกลุมตัวอย่างเพื่อให้การศึกษาได้ข้อมูลในเชิงลึก (In-depth Information) โดยจะไม่มีการกระทำใดต่อผู้ให้ข้อมูล (Key informant) จะเป็นการเก็บข้อมูลจากการสังเกตการสอบถาม เพื่อสกัดขอมูลสำคัญ จากนั้นผู้วิจัยจะนำข้อมูลสำคัญที่ได้รับมาทำการวิเคราะห์ (Analysis) และสังเคราะห์ (Synthesize) โดยอาศัยหลักการ แนวคิด และทฤษฎีทางอาชญาวิทยาเป็นกรอบในการวิเคราะห์เพื่ออธิบายปัจจัยและสาเหตุของปัญหาความมั่นคงปลอดภัยไซเบอร์ นำไปสู่การเสนอแนวทางการกำกับดูแลการรับมือเพื่อเฝ้าระวังภัยคุมคามความมั่นคงปลอดภัยไซเบอร์สำหรับองค์กรในยุคดิจิทัล โดยแบงออกเป็น 8 หัวขอ คือ

3.1 วิธีดำเนินการวิจัย

3.2 การกำหนดขนาดตัวอย่างการวิจัย

3.3 การกำหนดประชากรและกลุ่มตัวอย่าง

3.4 เครื่องมือที่ใชเก็บรวบรวมขอมูล

3.5 วิธีการเก็บรวบรวมขอมมูล

3.6 วิธีการวิเคราะห์และสังเคราะห์ขอมูล

3.7 วิธีการพิทักษ์สิทธิ ป้องกันความเสี่ยง และรักษาความลับของกลุ่มตัวอย่าง/ผู้มีส่วนร่วมในการวิจัย

3.8 จริยธรรมในการวิจัย

3.1 วิธีดำเนินการวิจัย

วิธีดำเนินการวิจัยเชิงคุณภาพ ผู้วิจัยได้กำหนดระเบียบวิธีการวิจัยหรือกระบวนวิธีการวิจัย (Methodology) โดยการใช้กระบวนวิธีการวิจัยเชิงคุณภาพ (Qualitative Research) โดยจะมี

การศึกษาและวิเคราะห์ข้อมูลจากเอกสารหรือการวิจัยเชิงเอกสาร (Documentary Research) และกระบวนการสัมภาษณ์เชิงลึก (In-Depth Interview)

3.1.1 การวิจัยเชิงเอกสาร (Documents)

ผู้วิจัยได้วิเคราะห์ข้อมูลจากเอกสาร (Documents) โดยการทบทวนวรรณกรรมแนวความคิด ทฤษฎี ที่เกี่ยวข้องกับการภัยคุกคามทางไซเบอร์ อาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์เพื่อมาเปรียบเทียบความเปลี่ยนแปลงที่เกิดบนโลกออนไลน์ในยุคดิจิทัล เพื่อต่อต้านภัยคุกคามไซเบอร์ในประเทศไทยและรับมือกับภัยคุกคามไซเบอร์ที่จะมีในอนาคต ทั้งนี้ในกระบวนการการศึกษายังประกอบไปด้วยการวิเคราะห์ภัยคุกคามทางไซเบอร์ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่เป็นสาเหตุของความไม่ชัดเจนในนโยบายรับมือภัยคุกคาม รวมไปถึงการศึกษายุทธศาสตร์และการมีส่วนร่วมในการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ของคณะกรรมการกำกับดูแลในระดับต่างๆทั้งภายในและภายนอกองค์กร การศึกษาจะประกอบไปด้วยการทบทวนแผนการรับมือภัยคุกคามไซเบอร์ของหน่วยงานโครงสร้างด้านสาธารณสุขและด้านสาธารณูปโภคพื้นฐานที่สำคัญและมีความเสี่ยงที่จะถูกโจมตี เป็นการศึกษาแนวความคิดเบื้องต้นที่จะนำไปต่อยอดในการวิจัยได้ต่อไป

3.1.2 การสัมภาษณ์เชิงลึก (In-Depth Interview)

การสัมภาษณ์เชิงลึก (In-Depth Interview) ที่เป็นส่วนหนึ่งของการวิจัยเชิงคุณภาพ การวิจัยในครั้งนี้ผู้วิจัยได้กำหนดรูปแบบในการสัมภาษณ์ออกเป็น 2 ส่วน คือ การสัมภาษณ์แบบกำหนดโครงสร้างของคำถาม เพื่อนำไปใช้ในการสัมภาษณ์แบบชี้นำ (Guided Interview) และการสัมภาษณ์แบบไม่มีโครงสร้างหรือเป็นการสัมภาษณ์แบบปลายเปิด มีความยืดหยุ่นและเปิดกว้างหรือมีการนำคำสำคัญ (Keywords) มาใช้ประกอบในการชี้นำคำสัมภาษณ์ การสัมภาษณ์จะเริ่มจากการใช้คำถามที่มีลักษณะปลายเปิดเริ่มต้นในการสัมภาษณ์เพื่อให้ผู้ให้ข้อมูลสามารถให้ข้อมูลให้ได้มากที่สุด ซึ่งจะทำให้ได้ข้อมูลที่มีความหลากหลายในมิติต่าง ๆ และข้อเท็จจริงในทางปฏิบัติที่มีทั้งมิติของความความลึกและมิติของความกว้างของงานวิจัย เมื่อได้คำสำคัญจากการสัมภาษณ์ผู้ให้สัมภาษณ์แต่ละคน ผู้วิจัยจะนำคำสำคัญไปกำหนดโครงสร้างของคำถาม เพื่อนำไปใช้ในการสัมภาษณ์แบบชี้นำเพื่อสามารถตีกรอบคำตอบที่ผู้วิจัยต้องการได้ ทั้งนี้ จะดำเนินการสัมภาษณ์ผู้ปฏิบัติงานระดับผู้บริหารหน่วยงานกำกับดูแลและรักษาความมั่นคงปลอดภัยไซเบอร์ หน่วยงานโครงสร้างพื้นฐานทางสารสนเทศที่สำคัญด้านสาธารณูปโภคและด้านสาธารณสุข หน่วยงานด้าน

กระบวนการยุติธรรมหรือผู้รักษากฎหมาย และผู้เชี่ยวชาญอิสระหรือที่ปรึกษาภาครัฐที่เกี่ยวข้อง ในประเด็นที่เกี่ยวกับวัตถุประสงค์ของการวิจัย คือ

(1) อภิปรายรูปแบบและลักษณะภัยคุกคามและการโจมตีทางไซเบอร์ที่เคยเกิดขึ้นกับองค์กรหรือมีความเสี่ยงที่จะการเกิดขึ้นกับองค์กร

(2) อภิปรายผลกระทบจากการเกิดสถานการณ์ภัยคุกคามทางไซเบอร์

(3) อภิปรายโครงสร้างและการขับเคลื่อนนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์

(4) อภิปรายแนวทางการกำกับดูแลด้านดิจิทัลและข้อมูลสารสนเทศ อันจะนำไปสู่การบริหารจัดการขององค์กรในการพัฒนาวิธีการเฝ้าระวังและรับมือภัยคุกคามระดับความมั่นคงปลอดภัยไซเบอร์

(5) เสนอแนะแนวทางเชิงนโยบายและเชิงปฏิบัติการและเตรียมความพร้อมรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ในอนาคต

3.2 การกำหนดขนาดตัวอย่างการวิจัย

การศึกษานี้ใช้การเลือกกลุ่มตัวอย่างแบบเจาะจง (Purposive sampling) และการสุ่มตัวอย่างแบบ Snowball โดยเข้าถึงกลุ่มตัวอย่างจากผู้ปฏิบัติงานระดับผู้บริหารในหน่วยงานเกี่ยวข้องกับปัญหาความมั่นคงไซเบอร์ การกำกับดูแล การปราบปราม ป้องกัน รับมือและแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์ ซึ่งเป็นผู้ปฏิบัติงานระดับผู้บริหารที่มีประสบการณ์การในการปฏิบัติงานไม่น้อยกว่า 3 ปี และยินดีให้คำสัมภาษณ์เชิงลึก (In-depth interview) โดยมี 4 กลุ่ม ได้แก่ (1) ผู้บริหารระดับการรับนโยบายไปปฏิบัติงานด้านกำกับดูแลเทคโนโลยีดิจิทัลและระดับเจ้าหน้าที่เฝ้าระวังและรับมือภัยคุกคามทางไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสารสนเทศ จำนวน 7 คน (2) ผู้บริหารที่มีอำนาจในการกำหนดนโยบายและยุทธศาสตร์ด้านการกำกับดูแลเทคโนโลยีดิจิทัลและด้านการควบคุมระบบความมั่นคงปลอดภัยทางไซเบอร์จากหน่วยงานภาครัฐ จำนวน 4 คน (3) ผู้บริหารด้านกระบวนการยุติธรรมหรือผู้รักษากฎหมายที่มีความรู้ความเชี่ยวชาญในด้านการบังคับใช้กฎหมายเทคโนโลยีดิจิทัลและปราบปรามอาชญากรรมทางเทคโนโลยี จำนวน 4 คน และ (4) ผู้เชี่ยวชาญอิสระ ในระดับบริหารด้านการจัดการความมั่นคงปลอดภัยทางไซเบอร์ ได้แก่ อาจารย์มหาวิทยาลัย ที่ปรึกษาด้านวิชาการ ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศและระบบเทคโนโลยีสารสนเทศ จำนวน 4 คน โดยผู้วิจัยเข้าถึงกลุ่มตัวอย่างโดยทำการติดต่อสื่อสารกับกลุ่มผู้ให้ข้อมูลโดยตรง โดยมีเอกสารนำจากต้นสังกัดแนะนำตัวและชี้แจงวัตถุประสงค์ของการวิจัยถึงผู้ให้ข้อมูลโดยมีชุดคำถามเป็นเอกสารทางการ โดยแนบคำถามวิจัยให้กับผู้ให้ข้อมูล โดยระบุวิธีการคัดเลือกกลุ่มตัวอย่าง/ผู้มีส่วนร่วมในการวิจัยที่ทำให้แน่ใจว่าเป็นความสมัครใจ ไม่ใช่การเข้าร่วมโดย

การบังคับ อีกทั้งผู้มีส่วนร่วมในการวิจัยรับทราบว่าอาจปฏิเสธที่จะเข้าร่วมโครงการวิจัย และอาจถอนตัวโดยไม่มีการลงโทษหรือเกิดผลร้าย หรือเสียผลประโยชน์ใดๆ เกณฑ์การคัดเลือกกลุ่มตัวอย่างและเกณฑ์การคัดออก ไม่มีการระบุถึงเกณฑ์คัดเข้าและเกณฑ์การคัดออก (Inclusion & Exclusion Criteria) ที่ชัดเจน ได้แก่

เกณฑ์การคัดเข้า

(1) ผู้เข้าร่วมการวิจัยจะต้องเป็นผู้ปฏิบัติงานระดับผู้บริหารที่มีประสบการณ์การในการปฏิบัติงานไม่น้อยกว่า 3 ปี

(2) ผู้เข้าร่วมการวิจัยมีโอกาสในการตัดสินใจในการเข้าร่วมด้วยความสมัครใจ

(3) ผู้เข้าร่วมการวิจัยจะต้องมีสัญชาติไทย และสามารถพูดหรือเข้าใจภาษาไทยได้

เกณฑ์การคัดออก

(1) ผู้ที่ใช้เวลาในการให้ข้อมูลมากกว่าและน้อยกว่า 3 ค่าเบี่ยงแบนมาตรฐานจะถูกคัดออก

(2) ผู้ที่ให้ข้อมูลโดยไม่ได้ให้ความใส่ใจในการตอบคำถามจะถูกคัดออก

(3) ผู้ที่ให้ข้อมูลไม่ได้ตอบคำถามครบถ้วนตามที่กำหนดจะถูกคัดออก

3.3 การกำหนดประชากรและกลุ่มตัวอย่าง

ผู้วิจัยจะใช้การเก็บข้อมูลด้วยการสัมภาษณ์เชิงลึก (In-depth Interview) จากผู้ให้ข้อมูลสำคัญ (Key Informants) ครั้งนี้คือ ผู้ปฏิบัติงานระดับผู้บริหารในหน่วยงานที่เกี่ยวข้องกับปัญหาอาชญากรรมไซเบอร์ การกำกับดูแล การปราบปราม ป้องกัน รับมือและแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์ 4 กลุ่ม ได้แก่

1) บุคลากรระดับบริหารและเจ้าหน้าที่เฝ้าระวังและรับมือภัยคุกคามทางไซเบอร์หน่วยงานโครงสร้างพื้นฐานสารสนเทศด้านสาธารณสุขและสาธารณูปโภค จำนวน 7 คน ประกอบด้วย การไฟฟ้าส่วนภูมิภาค จำนวน 1 คน การประปาส่วนภูมิภาค จำนวน 2 คน การประปานครหลวง จำนวน 1 คน ธนาคารแห่งประเทศไทย จำนวน 1 คน ธนาคารออมสิน จำนวน 1 คน และกระทรวงสาธารณสุข จำนวน 1 คน

2) บุคลากรระดับบริหารกำหนดนโยบายและยุทธศาสตร์ด้านการกำกับดูแลเทคโนโลยีดิจิทัลและความมั่นคงปลอดภัยทางไซเบอร์ จำนวน 7 คน ประกอบด้วย สำนักงาน

คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จำนวน 1 คน สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) จำนวน 1 คน สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ จำนวน 1 ท่าน กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม จำนวน 1 คน กระทรวงมหาดไทย จำนวน 1 คน สำนักงานสภาความมั่นคงแห่งชาติ จำนวน 2 คน

3) บุคลากรระดับบริหารด้านกระบวนการยุติธรรม จำนวน 4 คน ประกอบด้วย กองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี จำนวน 2 คน กระทรวงยุติธรรม จำนวน 1 คน กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี จำนวน 1 คน

4) ผู้ทรงคุณวุฒิ นักวิชาการและผู้เชี่ยวชาญ ประกอบด้วย อาจารย์มหาวิทยาลัย ที่ปรึกษาด้านวิชาการ ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศและระบบเทคโนโลยีสารสนเทศ จำนวน 4 คน

โดยข้อมูลที่ได้มาจากการสัมภาษณ์เชิงลึก จะถูกนำมาวิเคราะห์ข้อมูลด้วยวิธีการวิเคราะห์เชิงเนื้อหา (Content Analysis) เพื่อจัดกลุ่มข้อมูลตรวจสอบความถูกต้อง ความครบถ้วนของข้อมูลที่ถูกรวบรวมมาและคัดแยกประเด็นที่ไม่เกี่ยวข้องกับการวิจัยออกไป เพื่อให้ได้ข้อมูลที่มีเนื้อหาที่ตรงประเด็นกับคำถามวิจัยที่ได้ตั้งไว้

ตารางที่ 6 ผู้ให้ข้อมูลสำคัญ (Key Informants)

ผู้ให้ข้อมูลสำคัญ	**ตำแหน่ง/ความเชี่ยวชาญ**	**สังกัด**	**ประสบการณ์การทำงาน**
ผู้ให้ข้อมูลสำคัญที่ 1	ผู้ช่วยผู้ว่าการ (ดิจิทัลและสารสนเทศ)	การประปาส่วนภูมิภาค (กปภ.)	ประสบการณ์ระดับบริหารที่ครอบคลุมด้านด้านเทคโนโลยีสารสนเทศ 10 ปี
ผู้ให้ข้อมูลสำคัญที่ 2	หัวหน้างานเฝ้าระวังและควบคุมความปลอดภัย	การประปาส่วนภูมิภาค (กปภ.)	ประสบการณ์ด้านระบบเครือข่ายและสารสนเทศ 25 ปี และด้านการบริหาร 12 ปี

ผู้ให้ข้อมูลสำคัญ	ตำแหน่ง/ความเชี่ยวชาญ	สังกัด	ประสบการณ์การทำงาน
ผู้ให้ข้อมูลสำคัญที่ 3	ผู้อำนวยการกองเครือข่ายสื่อสารและความมั่นคงปลอดภัย	การประปานครหลวง (กปน.)	ประสบการณ์ด้านกำกับดูแลข้อมูล (Data governance) และด้านวิชาการระบบเครือข่าย
ผู้ให้ข้อมูลสำคัญที่ 4	รองผู้อำนวยการกองมาตรฐานและความมั่นคงปลอดภัยสารสนเทศ	การไฟฟ้าส่วนภูมิภาค (กฟภ.)	ประสบการณ์ด้าน security มากกว่า 20 ปี และด้านระบบเครือข่ายทั้งระบบ LAN และระบบ WAN ของ กฟภ. ทั่วประเทศ
ผู้ให้ข้อมูลสำคัญที่ 5	ผู้อำนวยการสำนักจัดการความมั่นคงปลอดภัย	ธนาคารแห่งประเทศไทย	ประสบการณ์ด้านเทคโนโลยีสารสนเทศ 25 ปี ,ด้าน cybersecurity 7 ปี , ดูแลระบบโอนเงินรายใหญ่ของทุกแบงก์ที่เป็นสมาชิกที่เชื่อมต่อเทคโนโลยีสารสนเทศภายใน
ผู้ให้ข้อมูลสำคัญที่ 6	ผู้อำนวยการฝ่าย Cyber Security Operation	ธนาคารออมสิน	ประสบการณ์ด้าน cybersecurity 10 ปี
ผู้ให้ข้อมูลสำคัญที่ 7	หัวหน้ากลุ่มงานธรรมาภิบาลข้อมูล	กระทรวงสาธารณสุข	ประสบการณ์ด้านนโยบายและมาตรการ

ผู้ให้ข้อมูลสำคัญ	ตำแหน่ง/ความเชี่ยวชาญ	สังกัด	ประสบการณ์การทำงาน
	(ผู้เชี่ยวชาญเฉพาะด้านเทคโนโลยีสารสนเทศสุขภาพ)		การรักษาความมั่นคงปลอดภัยไซเบอร์ 10 ปี
ผู้ให้ข้อมูลสำคัญที่ 8	ผู้อำนวยการสำนักปฏิบัติการ	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	- ประสบการณ์ด้านไซเบอร์และอาชญากรรมทางเทคโนโลยี กองกำกับการ 3 สอ.ปอท. 2 ปี - หัวหน้าศูนย์เฝ้าระวังและติดตามการใช้สื่อสังคมออนไลน์ให้กับสำนักงานตำรวจแห่งชาติ 2 ปี - ปฏิบัติงานราชการด้านอาชญากรรมและความมั่นคงทางไซเบอร์กับกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร (กอ.รมน.)

ผู้ให้ข้อมูลสำคัญ	ตำแหน่ง/ความเชี่ยวชาญ	สังกัด	ประสบการณ์การทำงาน
ผู้ให้ข้อมูลสำคัญที่ 9	ผู้อำนวยการฝ่ายความมั่นคงปลอดภัยทางไซเบอร์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)(สพร.)	ประสบการณ์ด้าน System Admin และ Security 20 ปี
ผู้ให้ข้อมูลสำคัญที่ 10	หัวหน้าทีมวิจัยความมั่นคงปลอดภัยสารสนเทศ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ	สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)	- ประสบการณ์ด้านปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ 25 ปี - หัวหน้าโครงการ ThaiCERT 2 ปี - ดำรงตำแหน่งอนุกรรมการความมั่นคงปลอดภัยภายใต้คณะกรรมการธุรกรรมอิเล็กทรอนิกส์ ปี 2552 - ปัจจุบัน
ผู้ให้ข้อมูลสำคัญที่ 11	นักวิเคราะห์นโยบายและแผนชำนาญการ	สำนักงานสภาความมั่นคงแห่งชาติ (สมช.)	ประสบการณ์ด้านความมั่นคงภัยคุกคามข้ามชาติอาชญากรรมข้ามชาติและความมั่นคงไซเบอร์ การขับเคลื่อนยุทธศาสตร์ชาติ ด้านความมั่นคงทางไซเบอร์และอาชญากรรมข้ามชาติ 20 ปี ร่วมกับ สกมช. และตำรวจขับเคลื่อนนโยบายและแผนระดับชาติว่าด้วย

ผู้ให้ข้อมูลสำคัญ	ตำแหน่ง/ความเชี่ยวชาญ	สังกัด	ประสบการณ์การทำงาน
			ความมั่นคงแห่งชาติปี 2566-2570 รวมทั้งสิ้น 10 ปีโดยประมาณ
ผู้ให้ข้อมูลสำคัญที่ 12	นักวิเคราะห์นโยบายและแผนปฏิบัติการ	สำนักงานสภาความมั่นคงแห่งชาติ (สมช.)	ประสบการณ์ด้านความมั่นคงทางไซเบอร์ 5 ปี
ผู้ให้ข้อมูลสำคัญที่ 13	นักวิชาการคอมพิเตอร์ชำนาญการพิเศษ	กระทรวงมหาดไทย	ประสบการณ์ทำงานด้านเทคโนโลยีสารสนเทศ 30 ปี
ผู้ให้ข้อมูลสำคัญที่ 14	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม	ประสบการณ์ทำงานด้านเทคโนโลยีสารสนเทศ 20 ปี
ผู้ให้ข้อมูลสำคัญที่ 15	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและสื่อสาร	กระทรวงยุติธรรม	ประสบการณ์ด้านเทคโนโลยีสารสนเทศเครือข่าย และ Security รวม 22 ปี
ผู้ให้ข้อมูลสำคัญที่ 16	รองผู้กำกับ กองกำกับการ 1	กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.)	ประสบการณ์ด้านการปราบปรามการกระทำความผิดที่มีคอมพิวเตอร์เป็นเป้าหมาย ด้านการสืบสวน จับกุม ตรวจสอบระบบ

ผู้ให้ข้อมูลสำคัญ	ตำแหน่ง/ความเชี่ยวชาญ	สังกัด	ประสบการณ์การทำงาน
			ออนไลน์ที่มีการเจาะระบบต่างๆ 5 ปี
ผู้ให้ข้อมูลสำคัญที่ 17	สารวัตรกองกำกับการ 1	กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.)	ประสบการณ์การรักษาความสงบเรียบร้อยในพื้นที่รับผิดชอบ และจับกุมตัวผู้กระทำความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติอื่นๆ 4 ปี
ผู้ให้ข้อมูลสำคัญที่ 18	รองผู้กำกับกลุ่มงานรักษาความมั่นคงปลอดภัยไซเบอร์	กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (สอท.)	ประสบการณ์การทำงานด้านเทคโนโลยีสารสนเทศ ที่ศูนย์เทคโนโลยีสารสนเทศกลางของตำรวจและด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งสิ้น 16 ปี
ผู้ให้ข้อมูลสำคัญที่ 19	- ที่ปรึกษาผู้ทรงคุณวุฒิของคณะกรรมการกำกับดูแลระบบสารสนเทศ การประปาส่วนภูมิภาค	อาจารย์เกษียณราชการ	- ประสบการณ์ เคยเป็นกรรมการจัดหาระบบคอมพิวเตอร์ในโครงการของภาครัฐที่มีงบประมาณเกิน 100 ล้าน และคณะกรรมการ

ผู้ให้ข้อมูลสำคัญ	ตำแหน่ง/ความเชี่ยวชาญ	สังกัด	ประสบการณ์การทำงาน
	- กรรมการคณะอนุกรรมการด้านเทคโนโลยีสารสนเทศ และประธานคณะทำงานเพื่อกำหนดนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมถึงเป็นประธานคณะทำงานด้านความคุ้มครองข้อมูลส่วนบุคคลของสภาวิศวกร - ที่ปรึกษาคณะกรรมการพัฒนาดิจิทัลเพื่อการตรวจเงินแผ่นดิน - ที่ปรึกษาคณะกรรมการเทคโนโลยีและการสื่อสาร สำนักงานอัยการสูงสุด		ธุรกรรมอิเล็กทรอนิกส์ภายใต้การกำกับดูแลกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม - ประธานอนุกรรมการด้านมาตรฐานและการกำกับดูแลของคณะกรรมการอิเล็กทรอนิกส์ - ผู้ทรงคุณวุฒิ ด้านพลังงานและสารสนเทศ - คณะกรรมการมูลนิธิสารสนเทศและเครือข่ายไทย - ที่ปรึกษาสมาคมความมั่นคงปลอดภัยสารสนเทศของไทย (Thailand Information Security Association) รวมประสบการณ์ 30 ปี

ผู้ให้ข้อมูลสำคัญ	ตำแหน่ง/ความเชี่ยวชาญ	สังกัด	ประสบการณ์การทำงาน
	- อาจารย์พิเศษสอนด้าน Cybersecurity		
ผู้ให้ข้อมูลสำคัญที่ 20	ผู้ทรงคุณวุฒิพิเศษ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์	มหาวิทยาลัยเกษตรศาสตร์	- ประสบการณ์ด้าน IT Innovation และ Software Engineering 16 ปี - ด้าน Advisory Committee 13 ปี - ด้าน Consultant และ Project Director 7 ปี
ผู้ให้ข้อมูลสำคัญที่ 21	กรรมการวิศวกรรมเทคโนโลยีสารสนเทศ	วิศวกรรมสถานแห่งประเทศไทย ในพระบรมราชูปถัมภ์	ประสบการณ์ด้านวิทยากรรับเชิญบรรยาย Blockchain & Crpto currency, PDPA และอาชญากรรมไซเบอร์ ในศูนย์ศึกษา Cyber crime คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัยและหลายสถาบันการศึกษา องค์กรภาครัฐและเอกชนรวม 12 ปี

ผู้ให้ข้อมูลสำคัญ	ตำแหน่ง/ความเชี่ยวชาญ	สังกัด	ประสบการณ์การทำงาน
ผู้ให้ข้อมูลสำคัญที่ 22	ผู้บริหารระดับสูง	บริษัท มอสกี้ คอร์ปอเรชั่น จำกัด	ประสบการณ์ด้านคอมพิวเตอร์และเครือข่ายบริษัทเอกชน จนได้ฉายา “หนุ่มนักฆ่าไวรัส I Love You” ในปี 2543 ประสบการณ์ 23 ปี

3.4 เครื่องมือที่ใช้เก็บรวบรวมข้อมูล

การวิจัยในครั้งนี้ใช้รูปแบบการวิจัยเชิงคุณภาพ (Qualitative research method) เป็นหลักในการดำเนินการ จึงจำเป็นต้องอาศัยความสัมพันธ์ที่ดีของผู้ทำวิจัยกับแหล่งข้อมูลที่ทำการศึกษา ดังนั้น ตัวผู้ทำการวิจัยเองจึงเป็นเครื่องมือสำคัญในการศึกษา เพื่อให้เข้าถึงแหล่งข้อมูลที่เป็นสาระสำคัญ โดยเทคนิคที่ใช้ในการเก็บข้อมูลได้แก่

3.4.1 การสัมภาษณ์แบบเจาะลึก (In-Depth Interview)เป็นการสนทนาที่ผู้ศึกษามุ่งที่จะได้คำตอบจากผู้ให้ข้อมูล (key informant) เป็นรายบุคคล ลักษณะข้อมูลที่ใช้ในการศึกษามาจากข้อคำถามเชิงลึก ดังนั้น ผู้วิจัยจะต้องตั้งคำถามที่มุ่งให้ได้คำตอบตรงกับวัตถุประสงค์ของการวิจัยให้มากที่สุด โดยแบบสัมภาษณ์ผ่านการพิจารณาจากผู้ทรงคุณวุฒิ การสัมภาษณ์กลุ่มตัวอย่างจะใช้การสอบถามเพื่อค้นหาข้อเท็จจริง และจะกระทำจนกว่าข้อมูลจะอิ่มตัวรอบด้าน และเพียงพอต่อการนำไปวิเคราะห์อธิบายผลการศึกษานี้การเก็บรวบรวมข้อมูลเป็นแบบอุปนัยโดยทยอยสะสมข้อมูล จนข้อมูลมีความชัดเจน ถูกต้อง แน่นอนครบถ้วน รอบด้าน และมีความเพียงพอต่อการทดสอบความน่าเชื่อถือ ขณะเดียวกันผู้ให้สัมภาษณ์สามารถให้ข้อมูลผู้วิจัยได้อย่างเต็มที่นอกเหนือจากประเด็นที่กำหนดไว้

3.4.2 ในการศึกษาครั้งนี้เพื่อให้ข้อมูลมีความสมบูรณ์ยิ่งขึ้น ผู้วิจัยจึงได้ทำการค้นคว้าเอกสารที่เกี่ยวข้องกับแนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ในปัจจุบันและการเตรียมความพร้อมรับมือ

ภัยคุกคามในอนาคต จากทั้งเอกสารปฐมภูมิ ได้แก่ หนังสือ บทความ งานวิจัยของนักวิชาการและหน่วยงานต่างๆ ที่มีเนื้อหาใจความสำคัญทั้งในประเทศไทยและต่างประเทศ ในรูปแบบข้อมูลทุติยภูมิ (Secondary Data) ได้แก่ บทความวิชาการหรือบทความในนิตยสารหรืออินเทอร์เน็ตที่น่าเชื่อถือ และผลสำรวจความเห็น บทสัมภาษณ์จากสื่อออนไลน์โดยตัวแทนจากสำนักงานตำรวจแห่งชาติและตำรวจสากล นักวิชาการด้านเทคโนโลยีดิจิทัล ด้านกฎหมาย และผู้เชี่ยวชาญหรือที่ปรึกษาการให้ความรู้ด้านอาชญากรรมไซเบอร์จากงานสัมมนาและการประชุมต่างๆที่เกี่ยวข้องระหว่างองค์กรทั้งภาครัฐและเอกชน ในรูปแบบ Onsite และการถ่ายทอดสดโต้ตอบแบบ Online

3.5 วิธีการเก็บรวบรวมขอมูล

ผู้วิจัยติดต่อประสานงานในเบื้องต้นผ่านโทรศัพท์ จากนั้นดำเนินการส่งหนังสือแนะนำตัวผู้วิจัยจากสาขาวิชาอาชญาวิทยาและงานยุติธรรม ภาควิชาสังคมวิทยาและมานุษยวิทยา คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ไปยังกลุ่มตัวอย่างซึ่งเป็นผู้ปฏิบัติงานระดับผู้บริหารหน่วยงานภาครัฐและเอกชน เพื่อขออนุญาตเก็บรวบรวมโดยใช้แบบสัมภาษณ์ เมื่อได้รับการอนุญาตให้เก็บรวบรวมข้อมูลแล้ว ผู้วิจัยดำเนินการสัมภาษณ์ทางโทรศัพท์อย่างเป็นทางการกับกลุ่มตัวอย่าง โดยระหว่างการสัมภาษณ์ผู้วิจัยจะทำการบันทึกข้อมูลด้วยวิธีการจดบันทึก บันทึกเสียง และถอดไฟล์บันทึกเสียง เพื่อเป็นหลักฐานเชิงยืนยัน สามารถนำไปใช้ในการวิเคราะห์รายละเอียดผลลัพธ์ที่ถูกต้องและมีคุณภาพต่องานวิจัยได้

3.6 วิธีการวิเคราะห์และสังเคราะห์ขอมูล

ผู้วิจัยจะทำการวิเคราะห์ข้อมูลโดยวิธีการวิเคราะห์เนื้อหา (Content Analysis) เพื่อนำไปประมวลผลได้ดังนี้

3.6.1 ตรวจสอบและประเมินคุณค่าของข้อมูลที่ได้จากการสัมภาษณ์เชิงลึก

3.6.2 จัดระเบียบข้อมูล เพื่อคำตอบในแต่ละประเด็นของวัตถุประสงค์ และความสมบูรณ์ของคำตอบ

3.6.3 ตรวจสอบความครบถ้วนของคำตอบแต่ละคำถามในแต่ละประเด็นและความถูกต้องของข้อเท็จจริง

3.6.4 รวบรวมข้อมูลนำไปสู่การวิเคราะห์ข้อมูลจากเอกสาร หลักฐาน การจดบันทึก และบันทึกเสียงที่ได้จากการสัมภาษณ์เชิงลึก ทำการตรวจสอบข้อมูลที่ด้วยเทคนิคการ**ตรวจสอบแบบสามเส้า (Triangulations) ซึ่งเป็นวิธีการที่เหมาะสมเพื่อหาความน่าเชื่อถือ (credibility) ความเที่ยงตรง (reliability) และ ความถูกต้อง (validity) ของการวิเคราะห์เชิงคุณภาพ** โดยการเปรียบเทียบและตรวจสอบความแน่นอนของข้อมูล (Data Triangulation) สังเกตความสัมพันธ์ของข้อมูลจากแหล่งที่มาของข้อมูล 3 กลุ่ม ได้แก่ (1) ข้อมูลที่ได้จากการสัมภาษณ์เชิงลึก นำมาวิเคราะห์ข้อมูลด้วยวิธีการวิเคราะห์เชิงเนื้อหา (Content Analysis) (2) ข้อมูลที่ได้จากการศึกษางานวิจัยที่เกี่ยวข้อง (Research Documents) และ (3) ทฤษฎี (Theory) หรือข้อมูลเชิงประจักษ์ (Empirical Material) ผลที่ได้จะทำให้รู้ว่าข้อมูลมีความถูกต้อง มีความสัมพันธ์และสอดคล้องกันหรือไม่ นำไปสู่การรายงานสรุปผลการศึกษาด้วยการบรรยาย พรรณนา ตามวัตถุประสงค์ถึงสิ่งที่ค้นพบในการศึกษาเกี่ยวกับปัญหาจากสถานการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับองค์กร สาเหตุและปัจจัยอันนำมาซึ่งการก่ออาชญากรรมจากการใช้เครือข่ายอินเตอร์เน็ต และช่องโหว่ที่เกิดจากระบบสารสนเทศของหน่วยงานในมุมมองอาชญากรรมไซเบอร์และผลกระทบจากเหตุการณ์ภัยคุกคามทางไซเบอร์ตลอดจนโครงสร้างองค์กรและการขับเคลื่อนนโยบาย กฎหมาย และมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ อันจะนำไปสู่แนวทางการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์และการกำกับดูแลที่ดีในระดับองค์กรเพื่อป้องกันภัยคุกคามทางไซเบอร์ในอนาคต

3.7 วิธีการพิทักษ์สิทธิ ป้องกันความเสี่ยง และรักษาความลับของผู้มีส่วนร่วมในการวิจัย

การทำจดหมายเพื่อชี้แจงกลุ่มตัวอย่างถึงวัตถุประสงค์ของการวิจัย การแนะนำตัวผู้วิจัย ซึ่งเป็นนิสิต คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ซึ่งผลการศึกษาจะไม่มีผลกระทบกับผู้ให้ข้อมูลสำคัญ เพื่อนำไปสู่การศึกษาสถานการณ์ภัยคุกคามไซเบอร์ที่การแฮกระบบของหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศด้านสาธารณสุข ด้านสาธารณูปโภค และด้านการเงินการธนาคาร โครงสร้างการกำกับดูแล การบังคับใช้นโยบายและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ในการบริหารจัดการ เพื่อสร้างความตระหนักและเฝ้าระวังภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ และแนวทางการเตรียมแผนการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์และการกำกับดูแลการบริหารจัดการที่ดีด้านเทคโนโลยีดิจิทัลในองค์กร เพื่อลดความเสี่ยงและป้องกันภัยคุกคามทางไซเบอร์ในอนาคต

การพิทักษ์สิทธิ ป้องกันความเสี่ยง และการรักษาความลับของกลุ่มตัวอย่าง ซึ่งเป็นผู้ให้ข้อมูลสำคัญ คือ การนำเสนอข้อมูลโดยไม่ระบุชื่อ นามสกุล อาชีพของผู้ให้ข้อมูลสำคัญ การนำเสนอข้อมูลในภาพรวม ไม่ได้เน้นกรณีศึกษาใดศึกษาหนึ่งเป็นการเฉพาะ

ผู้วิจัยจะต้องได้รับความยินยอมในการเปิดเผยชื่อหน่วยงานในบางประเด็นที่มีความเกี่ยวเนื่องทางกฎหมายจะมีการพิทักษ์สิทธิ ป้องกันความเสี่ยง และการรักษาความลับของหน่วยงานภาครัฐ หากแต่จะมีการนำเสนอข้อมูลในภาพรวม ไม่ได้เน้นกรณีศึกษาใดศึกษาหนึ่งเป็นการเฉพาะ

3.8 จริยธรรมในการวิจัย

การวิจัยเรื่อง แนวทางการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ขององค์กรในยุคดิจิทัล **ได้รับการอนุมัติโครงการวิจัยที่ 660031 ให้ผ่านการพิจารณารับรอง แบบลดขั้นตอน (Expedited Review)** โดยคณะกรรมการจริยธรรมการวิจัยในคน กลุ่มสหสถาบันชุดที่ 2 สังคมศาสตร์ มนุษยศาสตร์ และศิลปกรรมศาสตร์ แห่งจุฬาลงกรณ์มหาวิทยาลัย พิจารณาจริยธรรมการวิจัยและอนุมัติให้ดำเนินการศึกษาวิจัยเรื่องดังกล่าวได้ โดยรับรองเอกสารดังนี้

(1) เอกสารข้อมูลสำหรับกลุ่มตัวอย่างผู้มีส่วนร่วมในการวิจัย

(2) หนังสือยินยอมเข้าร่วมในการวิจัย

(3) ประวัติผู้วิจัย (CV)

(4) เครื่องมือที่ใช้ในการวิจัย

บทที่ 4
ผลการศึกษาและการอภิปรายผลการศึกษา

การวิจัยเรื่อง “แนวทางการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ขององค์กรในยุคดิจิทัล” มีวัตถุประสงค์การวิจัยอยู่ 3 ประการ คือ (1) เพื่อศึกษาสถานการณ์ภัยคุกคามทางไซเบอร์หน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศด้านสาธารณสุขและสาธารณูปโภค (2) ศึกษาโครงสร้างการกำกับดูแลด้านเทคโนโลยีดิจิทัลขององค์กรและการขับเคลื่อนด้วยนโยบายและมาตรการรักษาความปลอดภัยทางไซเบอร์ในการบริหารจัดการ เพื่อสร้างความตระหนักและเฝ้าระวังภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ และ (3) เพื่อศึกษาแนวทางการเตรียมแผนการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์และการกำกับดูแลการบริหารจัดการที่ดีด้านเทคโนโลยีดิจิทัลในองค์กร เพื่อลดความเสี่ยงและป้องกันภัยคุกคามทางไซเบอร์ในอนาคต

ผู้วิจัยดำเนินการศึกษาเชิงคุณภาพ (Qualitative Research) ด้วยการศึกษาจากเอกสาร (Documentary Research) และการสัมภาษณ์เชิงลึก (In-depth Interview) มาวิเคราะห์ (Analysis) และสังเคราะห์ (Synthesize) ถึงสถานการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศด้านสาธารณสุข สาธารณูปโภค และการเงินการธนาคาร รวมถึงหน่วยงานภาครัฐในด้านนโยบาย ด้านการกำกับดูแล ด้านกระบวนการยุติธรรม และองค์กรต่างๆที่เป็นเป้าหมายที่สำคัญของประเทศไทย เพื่อให้ทราบถึงภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยในระดับองค์กร และการตอบสนองต่อเหตุการณ์ นำไปสู่แนวทางการกำกับดูแลเพื่อรับมือภัยคุกคามและการประเมินความเสี่ยงในระดับที่องค์กรยอมรับได้ โดยอาศัยหลักการ แนวคิด และทฤษฎีทางอาชญาวิทยาที่เกี่ยวข้องมาเป็นกรอบในการศึกษา ซึ่งผู้วิจัยได้แบ่งการนำเสนอผลการศึกษาออกเป็น 5 ส่วน ดังนี้

4.1 ข้อมูลทั่วไปของผู้ให้ข้อมูลสำคัญ

4.2 สถานการณ์ภัยคุกคามทางไซเบอร์หน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ

4.3 โครงสร้างการกำกับดูแล การขับเคลื่อนนโยบายและมาตรการรักษาความปลอดภัยทางไซเบอร์ในการบริหารจัดการขององค์กร

4.4 แนวทางการรับมือภัยคุกคามทางไซเบอร์และการกำกับดูแลการบริหารจัดการที่ดีด้านเทคโนโลยีดิจิทัล

4.5 การอภิปรายผลการศึกษา

4.1 ข้อมูลทั่วไปของผู้ให้ข้อมูลสำคัญ

จากการสัมภาษณ์ผู้ให้ข้อมูลแบ่งออกเป็น 4 กลุ่ม ได้แก่ (1) กลุ่มบุคลากรระดับบริหารและเจ้าหน้าที่เฝ้าระวังและรับมือภัยคุกคามทางไซเบอร์หน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ (2) กลุ่มบุคลากรระดับบริหารกำหนดนโยบายและยุทธศาสตร์ด้านการกำกับดูแลเทคโนโลยีดิจิทัลและความมั่นคงปลอดภัยทางไซเบอร์ (3) กลุ่มบุคลากรระดับบริหารด้านกระบวนการยุติธรรม (4) กลุ่มผู้ทรงคุณวุฒิ นักวิชาการและผู้เชี่ยวชาญ จำนวนรวมทั้งสิ้น 22 คน โดยในภาพรวมมีประสบการณ์การทำงานที่เกี่ยวข้องทั้งด้านเชิงนโยบายและเชิงปฏิบัติการตั้งแต่ 3 – 25 ปี ทั้งในด้านเทคโนโลยีสารสนเทศ ด้านระบบคอมพิวเตอร์และเครือข่าย ด้านกำกับดูแลข้อมูลดิจิทัล ด้านเฝ้าระวังและรับมือภัยไซเบอร์ และด้านการป้องกันและรักษาความมั่นคงปลอดภัยทางไซเบอร์ เป็นต้น

ในส่วนของด้านวิชาการนั้น ผู้ให้ข้อมูลสำคัญมีประสบการณ์ทั้งในด้านการบริหารองค์กร การอบรมให้ความรู้ การบรรยายในสถาบันการศึกษา อาจารย์มหาวิทยาลัย วิทยากรด้านกฎหมายและไซเบอร์ รวมถึงเป็นคณะกรรมการระดับสูง ที่ปรึกษาและผู้ทรงคุณวุฒิให้กับองค์กรทั้งภาครัฐและเอกชน ซึ่งประสบการณ์ในภาพรวมตั้งแต่ 12 - 30 ปี และส่วนใหญ่มาจากสายอาชีพวิศวกร

4.2 สถานการณ์ภัยคุกคามทางไซเบอร์หน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ

4.2.1 การโจมตีทางไซเบอร์

จากการสัมภาษณ์ผู้ให้ข้อมูลสำคัญทั้ง 22 คน แสดงให้เห็นถึงการให้ข้อมูลการโจมตีทางไซเบอร์ได้กลายเป็นภัยคุกคามที่สร้างความปั่นป่วนให้กับองค์กรอย่างต่อเนื่องและหลากหลายรูปแบบมากขึ้น ทั้งในส่วนของระบบคอมพิวเตอร์ เครือข่าย อุปกรณ์ฮาร์ดแวร์และซอฟต์แวร์ และข้อมูลสารสนเทศ มักตกเป็นเป้าหมายหลักของการโจมตีเหล่านี้ โดยเฉพาะเกิดขึ้นกับหน่วยงานที่เป็นโครงสร้างพื้นฐานข้อมูลที่สำคัญทางสารสนเทศทั้งด้านสาธารณสุข สาธารณูปโภค และการเงินการธนาคาร ล้วนแล้วแต่เกี่ยวข้องกับข้อมูลที่สำคัญของประชาชนทั้งสิ้น ข้อมูลที่ได้จากกลุ่มบุคลากรระดับบริหารและเจ้าหน้าที่ปฏิบัติการด้านเฝ้าระวังและรับมือภัยคุกคามทางไซเบอร์ ด้านกำหนดนโยบายและยุทธศาสตร์การกำกับดูแลเทคโนโลยีดิจิทัล ด้านการสืบสวนสอบสวนและปราบปรามความมั่นคง

ปลอดภัยทางไซเบอร์ ผู้ทรงคุณวุฒิและผู้เชี่ยวชาญนั้น ได้กล่าวถึงลักษณะของภัยคุกคามทางไซเบอร์และการโจมตีที่องค์กรเผชิญ ดังนี้

4.2.1.1 มัลแวร์ (Malware)

Malware นั้นย่อมาจาก Malicious และ Software หมายถึง โปรแกรมประสงค์ร้ายที่ถูกเขียนขึ้นมา เพื่อทำอันตรายกับข้อมูลในระบบ เช่น ทำให้เครื่องคอมพิวเตอร์ทำงานผิดปกติ ขโมยหรือทำลายข้อมูลหรืออาจจะเปิดช่องทางให้ผู้ไม่หวังดีเข้ามาควบคุมเครื่องของเราได้ ซึ่งมัลแวร์มีหลากหลายประเภท จากผลการให้ข้อมูลของผู้มีส่วนร่วมในการวิจัย ลักษณะของมัลแวร์ที่พบ ได้แก่

(1) ไวรัสคอมพิวเตอร์ (Computer Virus) เป็นมัลแวร์ชนิดแรกๆที่บุกรุกเข้าไปทำลายคอมพิวเตอร์และสามารถแพร่กระจายจากคอมพิวเตอร์เครื่องหนึ่งไปสู่อีกเครื่องหนึ่งอย่างรวดเร็วด้วยแฟลชไดรฟ์หรืออุปกรณ์อื่นๆที่ผู้ใช้นำมาเก็บข้อมูลหรือใช้ทำงาน ซึ่งสอดคล้องกับผู้ให้ข้อมูลสำคัญดังต่อไปนี้

> *“8 ปีก่อนเคยประสบปัญหา ATM ถูกแฮก ตรวจสอบพบว่าถูกคนร้ายปล่อยโปรแกรมมัลแวร์ หรือโปรแกรมประสงค์ร้ายโจมตีเครื่องเอทีเอ็มของธนาคาร จึงระงับการใช้งานตู้เอทีเอ็มยี่ห้อดังกล่าวไว้ก่อนเพื่อตรวจสอบ”*
>
> (ผู้ให้ข้อมูลสำคัญที่ 6, สัมภาษณ์เมื่อวันที่ 28 เมษายน 2566)

> *“Malware หรือ Malicious Software โปรแกรมคอมพิวเตอร์ที่ถูกออกแบบมาเพื่อมุ่งร้ายต่อคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน โดยที่ผ่านมา ได้มีการโจมตีในรูปแบบของไวรัสคอมพิวเตอร์ ซึ่งได้มีการตรวจจับและกำหนดการเข้าถึงข้อมูลของหน่วยงานก่อนเสมอ ทั้งนี้ ทางหน่วยงานได้มีการวางระบบไว้สำหรับรองรับกับสถานการณ์ภัยคุกคามดังกล่าว เพื่อให้ระบบคอมพิวเตอร์และสารสนเทศ สามารถให้บริการได้อย่างต่อเนื่องและมีประสิทธิภาพสูงสุด”*
>
> (ผู้ให้ข้อมูลสำคัญที่ 14, สัมภาษณ์เมื่อวันที่ 18 เมษายน 2566)

“เมื่อปี 2543 ได้เกิดภัยคุกคามจากไวรัสที่ชื่อว่า ILOVEYOU ลุกลามไปทั่วโลกอย่างรวดเร็ว และภายในเวลาไม่ถึง 24 ชั่วโมงก็มีข่าวว่าไวรัสตัวนี้ทำลายคอมพิวเตอร์ถึง 45 ล้านเครื่องทั่วโลก เพราะประสิทธิภาพของไวรัสร้ายแรงกว่าไวรัสใดๆที่ผ่านมา และแพร่ระบาดง่ายจากโปรแกรมรับส่งอีเมลเอาท์ลุกเอ็กซเพรสของไมโครซอฟต์ ทั้งในสหรัฐอเมริกา รัฐสภาประเทศอังกฤษ และอีก 2 กระทรวงในนิวซีแลนด์ แต่ในประเทศไทยไม่มีรายงานความเสียหายของหน่วยงานสำคัญใดๆเกี่ยวกับไวรัสตัวนี้ เนื่องจากช่วงนั้นเป็นวันหยุดราชการ 3 วันติดต่อกัน แต่ระหว่างนั้นมีคนติดต่อให้ผมเขียนโปรแกรมเพื่อฆ่าไวรัส ILOVEYOU ผมพยายามศึกษาทดลองเขียนโปรแกรมขึ้นมาโดยใช้เวลาภายใน 24 ชั่วโมง และทดสอบว่าป้องกันได้หรือไม่ เนื่องจากเป็นไวรัสที่รุนแรงในสมัยนั้น ผลปรากฏว่าโปรแกรมที่เขียนขึ้นมาสามารถฆ่าไวรัสตัวนี้ได้จริงๆ ต่อมาโปรแกรมที่ผมเขียนขึ้นมา มีคนดาวน์โหลดไปใช้จำนวนมาก รวมถึงได้นำไปใช้ในองค์กรของเราเอง”

(ผู้ให้ข้อมูลสำคัญที่ 22, สัมภาษณ์เมื่อวันที่ 25 มีนาคม 2566)

(2) แรนซัมแวร์ (Ransomware) มีลักษณะการบุกรุกเข้ารหัสหรือล็อกไฟล์ข้อมูล ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ และทำให้ผู้ใช้งานไม่สามารถเปิดไฟล์ข้อมูลใดๆได้ ส่วนใหญ่ผู้ไม่ประสงค์ดีจะใช้วิธีนี้กับข้อมูลที่อ่อนไหว เช่น ข้อมูลส่วนบุคคล และการถูกเข้ารหัส นั่นหมายความว่าต้องใช้คีย์ในการปลดล็อกเพื่อกู้ข้อมูลคืนมา คนร้ายจึงใช้วิธีการนี้เป็นเครื่องต่อรองในการเรียกค่าไถ่ ซึ่งสอดคล้องกับผู้ให้ข้อมูลสำคัญดังต่อไปนี้

“เราโดนโจมตีด้วย Ransomware และมีการนำข้อมูลออกไปเปิดเผยสู่ภายนอก นั่นนับเป็นเหตุการณ์ใหญ่เหตุการณ์นึงที่สำคัญมาก ซึ่งเป็นจุดเปลี่ยนอะไรหลายอย่างตามมาหลังจากที่เกิดเหตุการณ์ในวันนั้น ผมเข้าใจว่าไม่ถึงกับเจาะฐานข้อมูล แต่เค้า encrypt ข้อมูลแล้วนำข้อมูลออกไปปล่อย แต่เค้ามาทางการเจาะระบบเข้ามามากกว่า และมีการ encryption ข้อมูล ซึ่งเป็น 400 servers ที่สำนักงานใหญ่ที่โดน encryption มากกว่า 1200 client ทั่วประเทศ”

(ผู้ให้ข้อมูลสำคัญที่ 4, สัมภาษณ์เมื่อวันที่ 31 มีนาคม 2566)

“ภัยคุกคามทางไซเบอร์มีหลายประเภท ถ้าในกรณีของการเจาะระบบ คือการแฮกเพื่อเข้าถึงข้อมูลและนำข้อมูลมาใช้ประโยชน์หรือนำไปขาย หรือนำไปเผยแพร่ใน Dark Web หรือเป็นข้อมูลอ่อนไหวแล้วเอาขึ้นไปเผยแพร่แล้วเกิดความเสียหาย และกรณีที่เกิดเหตุกับโรงพยาบาลสระบุรี แล้วโรงพยาบาลแจ้งให้ผู้ป่วยมาต่อคิวเพื่อรับบริการ เนื่องด้วยระบบไอทีของโรงพยาบาลหยุดชะงัก กระบวนการทำงานของบัตรผู้ป่วยไม่ปกติเนื่องจากค้นหาแล้วไม่พบชื่อผู้ป่วย จึงต้องดำเนินการแบบ manual เพราะฉะนั้นฐานข้อมูลคนไข้ก็อาจจะไม่ได้อยู่ในระบบแต่สามารถใช้วิธีจดแทนได้ เมื่อระบบคอมพิวเตอร์ต่างๆ down ลงจาก Ransomware ก็ทำอะไรไม่ได้ อันนี้จึงถือว่าเป็นคอมพิวเตอร์ด้อยประสิทธิภาพ คืออยู่ในระดับไม่ร้ายแรง แต่เนื่องด้วยสำนักปลัดกระทรวงสาธารณสุขยังไม่ได้แต่งตั้งโรงพยาบาลสระบุรีเป็นหน่วยงาน CII ภายใต้ พ.ร.บ.ไซเบอร์ ทั้งที่ควรจะเป็น แต่ไปอยู่ในฐานะหน่วยงานภาครัฐ”

(ผู้ให้ข้อมูลสำคัญที่ 8, สัมภาษณ์เมื่อวันที่ 27 มีนาคม 2566)

“ณ ตอนนี้น่าจะเป็นเรื่องของ Ransomware หรือการเรียกค่าไถ่ข้อมูลที่เกิดขึ้นกับองค์กร วิธีที่ดีที่สุดคือสอนเรื่องการป้องกันและการวิเคราะห์ความเสี่ยงก่อนว่าถ้าจ่ายค่าปรับแล้วโจรจะปลดล็อคให้หรือไม่ แต่ทั้งนี้ต้นเหตุก็มาจากคนไม่มีความตระหนักหรือ Awareness ทำให้มักจะติดไวรัส มัลแวร์ แรนซัมแวร์ หรือทำอะไรที่ไม่ถูกไม่ควร”

(ผู้ให้ข้อมูลสำคัญที่ 10, สัมภาษณ์เมื่อวันที่ 27 มีนาคม 2566)

4.2.1.2 ดีดีโอเอส (DDoS) ย่อมาจาก Distributed Denial-of-Service ซึ่งก่อนหน้านี้จะเป็นการโจมตีแบบ Denial of Service (DoS) โดย DoS และ DDoS นั้นมีลักษณะเหมือนกัน แต่จะมีความแตกต่างกันตรงที่ DoS คือ การโจมตีที่มีแหล่งที่มาเพียงแหล่งเดียว ในขณะที่ DDoS คือการโจมตีจากอุปกรณ์จำนวนมากและมีแหล่งที่มาจากหลากหลายที่ และแฮกเกอร์จะทำการส่ง Traffic หรือคำขอเข้าถึงข้อมูลจากหลากหลายที่ไปยังเว็บไซต์ที่ต้องการโจมตีพร้อม ๆ กัน ทำให้

เว็บไซต์นั้นมีปริมาณ Traffic มากเกินกว่าที่ Server จะสามารถรองรับได้ ส่งผลให้เว็บไซต์ไม่สามารถใช้งานได้ หรือที่นิยมเรียกกันว่าเว็บไซต์ล่ม เป็นภัยคุกคามที่มีกระทบต่อการปฏิเสธการให้บริการโดยเฉพาะเว็บไซต์หน่วยงานโครงสร้างพื้นฐานที่สำคัญ ซึ่งสอดคล้องกับผู้ให้ข้อมูลสำคัญดังต่อไปนี้

“ถ้าเป็นเหตุการณ์แบบทั่วไปก็จะมีคนพยายามโจมตีเรื่อย เช่น พยายามสแกนเว็บไซต์ พยายาม DDoS เว็บไซต์ ก็จะมีคนพยายามตลอด แต่ไม่เคยมีการกระทำที่ขนาดถึงขั้นทำความเสียหายให้กับองค์กร เนื่องจากมีระบบป้องกันทำให้ทราบล่วงหน้าก่อนถูกโจมตี”

(ผู้ให้ข้อมูลสำคัญที่ 5, สัมภาษณ์เมื่อวันที่ 26 เมษายน 2566)

“เรื่องการทำผมมองว่าการเจอปัญหากับเหตุการณ์ทาง cybersecurity เป็นเหมือน security incident เป็น incident response การตอบสนอง ก่อนหน้านี้น่าจะเคยได้ยินเรื่องข่าวกลุ่มทางการเมืองชักชวน user ทั่วประเทศเข้าเว็บกระทรวง ICT ณ สมัยนั้นแล้วก็ช่วยกันกด f5 เพื่อให้เกิด Denial of Service หรือ DoS เป็นการที่ทำให้ระบบหยุดให้บริการเพราะรองรับไม่พออะไร แล้วก็เหตุการณ์พวก security incident ที่เกิดในสำนักงาน เราเจอกันทุกวันอยู่แล้ว แต่ว่าโดยส่วนมากเราก็จะป้องกันไว้ได้ส่วนหนึ่ง แล้วก็ตอบสนองได้ดีพอที่จะยังไม่เกิดผลกระทบที่มีความรุนแรงสูงเท่านั้นเอง หลักๆก็คือรู้ให้ไวและตอบสนองให้ทันท่วงทีเพื่อที่จะลดความรุนแรงของผลกระทบที่เกิดขึ้น”

(ผู้ให้ข้อมูลสำคัญที่ 9, สัมภาษณ์เมื่อวันที่ 30 มีนาคม 2566)

“มีรูปแบบของ DDoS - Distributed Denial of Service การโจมตีทางไซเบอร์รูปแบบหนึ่ง โดยมีรูปแบบการโจมตีที่จะทำการส่ง Traffic มายัง Server ค่อนข้างสูงในระยะเวลาใดเวลาหนึ่ง โดยที่ผ่านมามีการพยายามโจมตีด้วยวิธีนี้มาตลอดเป็นระยะ”

(ผู้ให้ข้อมูลสำคัญที่ 14, สัมภาษณ์เมื่อวันที่ 30 มีนาคม 2566)

4.2.1.3 ช่องโหว่ (Vulnerability) เป็นการโจมตีรูปแบบใหม่ที่ผู้ไม่ประสงค์ดีสแกนหา “บั๊ก” หรือเรียกว่า ข้อบกพร่องของโค้ดที่โปรแกรมเมอร์เขียนไว้ไม่รอบคอบ หรือเป็นข้อผิดพลาดจนเกิดเป็นช่องโหว่ที่ไม่สามารถป้องกันการโจมตีได้ ซึ่งอาจส่งผลให้แฮกเกอร์สามาถเข้าไปทำลาย ขโมยข้อมูล จนทำให้เกิดการหยุดชะงัก หรือถูกนำเอาข้อมูลไปขายใน Dark Web หรือใช้ในการเรียกค่าไถ่ข้อมูล โดยผู้ให้ข้อมูลสำคัญที่มีความคิดเห็นคล้ายคลึงกันและกล่าวสอดคล้องกับประเด็นภัยคุกคามที่มาจากช่องโหว่ มีดังนี้

“เราได้ประสบปัญหาภัยคุกคามทางไซเบอร์เป็นระยะๆ ลักษณะภัยคุกคามส่วนใหญ่ที่พบเจอจะมีการโจมตีมาจากประเทศทางรัสเซีย และจีน ลักษณะการโจมตีคือ จะมีการสแกนช่องโหว่ทางช่องทางที่ กปภ. เปิดให้บริการ ซึ่งจะเป็นการบริการแบบทั่วไป เช่น port https เป็นส่วนใหญ่ และเราจะพยายามลด port ในส่วนนี้”

(ผู้ให้ข้อมูลสำคัญที่ 2, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

“ถ้าพูดถึงสำนักงานปลัดกระทรวงสาธารณสุข มีหน่วยงานภายใต้สำนักงานค่อนข้างเยอะ เนื่องจากมีโรงพยาบาล สำนักงานเขตสุขภาพ สำนักงานสาธารณสุขจังหวัด โรงพยาบาลศูนย์ โรงพยาบาลทั่วไป โรงพยาบาลชุมชน ฉะนั้น หน่วยงานที่มีขนาดใหญ่จะควบคุมกำกับดูแลจะต้องซับซ้อนกว่าหน่วยงานอื่นๆที่มีขนาดเล็ก แน่นอนว่าต้องเคยเจอกับภัยคุกคาม แต่ที่เจอบ่อยๆคือ คือ บุกรุกด้วยการเข้ามาแฝงเว็บพนันและการเปลี่ยนแปลงหน้าเว็บไซต์ต่างๆของหน่วยงาน”

(ผู้ให้ข้อมูลสำคัญที่ 7, สัมภาษณ์เมื่อวันที่ 26 พฤษภาคม 2566)

“เราเจอกับเว็บพนันบอล ทุกกรมจะเจอเหมือนกันหมด โดยการนำลิ้งก์ไปฝังไว้ในเว็บกระทรวง เช่น เมื่อมีการค้นหาในกูเกิลว่ากระทรวงยุติธรรม พนันบอล ก็จะลิ้งก์ไปหน้านั้น เมื่อตรวจสอบการ Coding ไม่ได้ปิดการเข้าถึงโฟล์เดอร์ที่สามารถนำรูปไปวางไว้ได้ แต่ไม่ได้ตรวจสอบว่าห้ามนำไฟล์อื่นๆไปวาง ซึ่งอาจเป็นช่องโหว่ที่แฮก

เกอร์ถือโอกาสนำ HTML มาวาง พอกดเข้าไปก็จะลิ้งก์ไปที่เว็บพนันบอล แต่ไม่ได้ทำให้ระบบเสียหาย และไม่เคยโดน แฮกฐานข้อมูล”

(ผู้ให้ข้อมูลสำคัญที่ 15, สัมภาษณ์เมื่อวันที่ 29 มีนาคม 2566)

“จากที่เคยศึกษาวิจัยเรื่องของหน่วยงานกองบัญชาการช่วยรบที่โคราช เป็นคลังแสงอาวุธ วิเคราะห์กระสุนเพื่อวางแผนในการรบ ปรากฏว่าคลังแสงอาวุธไม่มีระบบ Security อะไรเลย ที่เจอคือปี 2554 ระบบคลังแสงอาวุธโดนแฮก ซึ่งในขณะนั้นมีช่องโหว่ที่สามารถถูกโจมตีได้ รวมทั้งเว็บไซต์ของกระทรวง ทบวง กรม ถูกแฮกโดยผู้ไม่ประสงค์ดีเข้าไปยึดเว็บไซต์นั้นทำให้องค์กรต้องขายหน้า แต่ที่น่ากลัวกว่านั้นคือ ทำให้ทะลุเข้าไปถึงฐานข้อมูลคลังแสง ซึ่งถ้าสมมุติเกิดการทะเลาะกันระหว่างประเทศ ก็อาจจะทำให้ไทยเสียเปรียบในการรบได้ถึงขั้นโดนยึดประเทศ จึงได้เข้าไปแก้ปัญหาด้านการรักษาความปลอดภัยสารสนเทศสำหรับหน่วยงานในกองทัพไทยและพัฒนาระบบรักษาความปลอดภัยระบบส่งกำลังบำรุงอัตโนมัติ กองบัญชาการช่วยรบสมัยนั้น”

(ผู้ให้ข้อมูลสำคัญที่ 20, สัมภาษณ์เมื่อวันที่ 19 มีนาคม 2566)

“ผมมองว่าค่อนข้างยังอ่อนแออยู่ ซึ่งในมหาวิทยาลัยก็เคยโดนเมื่อไม่นานมานี้ อย่างช่องโหว่ Proxy logon เป็นช่องโหว่ในผู้ที่ใช้ Microsoft Exchange Server ที่กำลังถูกใช้โจมตีอย่างแพร่หลายในการให้บริการอีเมล เช่น @chula.ac.th หรือ @abc.co.th ซึ่ง @ ยังมีช่องโหว่ที่แฮกเกอร์ฝั่ง Web shell คือไฟล์ที่สามารถใช้เข้าถึงหรือส่งคำสั่งของระบบปฏิบัติการได้โดยตรงผ่านหน้าเว็บไซต์ ซึ่งโครงสร้างเว็บไซต์เขียนด้วย html ลูกเล่นคือ CSS กับ JavaScript ที่เชื่อมโยงกัน และจะคำนวณเป็น PHP ที่คุยกับ SQL server นั่นหมายความว่าเข้าถึงเว็บไซต์แล้วสามารถเข้าไปที่ Server ได้ แฮกเกอร์รู้จักช่องโหว่อันนี้แล้วฝั่งสคริบเล็กๆ ทำให้เปิดเผยข้อมูลออกมาได้ แต่ไม่ได้ไปทำลายหรือสร้างความเสียหายมาก เพราะเป็น web app ที่กระทบ

น้อยและแก้ไขเร็วโดยการ update patch แต่หน่วยงานในภาครัฐยังไม่ค่อยตระหนัก ซึ่งก็ยังมีข้อมูลรั่วไหลอยู่เรื่อย ๆ และควรอัพเดททุกปี”

(ผู้ให้ข้อมูลสำคัญที่ 21, สัมภาษณ์เมื่อวันที่ 25 มีนาคม 2566)

4.2.1.4 ฟิชชิ่ง (Phishing) เป็นภัยคุกคามทางไซเบอร์อีกประเภทหนึ่งที่ผู้บริหารและเจ้าหน้าที่ มักพบอยู่เสมอทั้งในการปฏิบัติงานและสภาพแวดล้อมภายนอก ซึ่งจากความคิดเห็นของผู้ให้ข้อมูลสำคัญคนที่ 2 ผู้ให้ข้อมูลสำคัญคนที่ 6 และผู้ให้ข้อมูลสำคัญคนที่ 11 มีความคล้ายคลึงกัน ในการอธิบายถึงลักษณะและวิธีการที่ผ่านมา แฮกเกอร์ (Hacker) ได้พยายามที่จะขโมยข้อมูลบัญชีผู้ใช้ เพื่อหลอกให้เหยื่อเปิดเผยข้อมูลชื่อผู้ใช้และรหัสผ่าน โดยปกติการโจมตีในลักษณะนี้จะทำการส่งข้อความหรืออีเมล บางครั้งจึงถูกเรียกว่าอีเมลฟิชชิ่ง (Phishing Emails) ที่มาพร้อมกับลิงก์ (Link) ดูผิวเผินอาจเป็นเหมือนลิงก์ของเว็บไซต์ปกติทั่วไป แต่ในความเป็นจริงคือเป็นลิงก์ของเว็บไซต์ที่ควบคุมโดยฟิชเชอร์ (Phisher)

ในขณะที่ ข้อมูลสำคัญจากผู้เชี่ยวชาญทางไซเบอร์คนที่ 21 ให้เหตุผลว่า แฮกเกอร์ได้พัฒนากลยุทธ์การฟิชชิ่งที่ชัดเจนและหลายหลายมากขึ้น จะเห็นได้จากรูปแบบของการหลอกล่อให้เหยื่อเปิดเผยข้อมูลส่วนตัวที่สำคัญ เช่น ชื่อผู้ใช้และรหัสผ่าน วันเดือนปีเกิด เลขบัตรประจำตัวประชาชน และข้อมูลทางการเงิน เป็นต้น ซึ่งปัจจุบันการฟิชชิ่ง (Phishing) ถือเป็นอาชญากรรมรูปแบบหนึ่งที่ไม่ได้ใช้เพียงเทคนิคที่ต้องอาศัยเทคโนโลยี แต่ผู้ไม่ประสงค์ดียังใช้เทคนิคที่เรียกว่าวิศวกรรมเชิงสังคม หรือ Social engineering ซึ่งเป็นการพัฒนากลวิธีในการหลอกลวงที่ซับซ้อนกว่าเมื่อก่อนมาก ยกตัวอย่างเช่น การปลอมตัวและแอบอ้างว่าเป็นเจ้าหน้าที่ของรัฐ เข้าไปในองค์กรทำทีว่าคุยกับพนักงาน และเมื่อพนักงานไม่ทันสังเกต แฮกเกอร์ได้นำ USB เสียบไปที่คอมพิวเตอร์เพื่อเข้าถึงข้อมูล จนทำให้ผู้ใช้งานระบบเครือข่ายอินเทอร์เน็ตและคอมพิวเตอร์ไม่ทันระวังตัว หรืออีกกรณี คือ การแอบอ้างและสวมรอยและใช้คำพูดที่สร้างความน่าเชื่อถือให้ประชาชนว่าเป็นเจ้าหน้าที่ของรัฐ ในพื้นที่ให้บริการของหน่วยงานเพื่อแนะนำการใช้ระบบหรือแอปพลิเคชันของภาครัฐ ทำให้ประชาชนหลงเชื่อและตกเป็นเหยื่อได้ง่าย ซึ่งมีเหตุผลสอดคล้องกับความคิดเห็นของผู้ให้ข้อมูลสำคัญ ดังนี้

“ระยะนี้ เราเจอภัยคุกคามในรูปแบบการเลียนแบบเว็บไซต์องค์กร หรือถูกปลอมแปลงเว็บไซต์องค์กรชื่อ https://pwa-co.cc/ ซึ่งจากการตรวจสอบ เว็บไซต์ดังกล่าว ไม่ใช่เว็บไซต์ขององค์กรแต่

อย่างใด ซึ่งเว็บไซต์ กปภ. คือ http://pwa.co.th/ โดยเป็นการปลอมและเลียนแบบเว็บไซต์ที่มิจฉาชีพทำขึ้นมาเท่านั้น และเราก็เพิ่งมีการเปิดตัว Application ใหม่ในการรับบริการชำระเงินค่าน้ำและบริการอื่นๆเพื่ออำนวยความสะดวกและเข้าถึงการให้บริการลูกค้าหรือผู้ใช้บริการมากขึ้น แต่จะเป็นภัยที่เกิดกับลูกค้าของ กปภ. ที่เจอผู้ไม่ประสงค์ดี อ้างว่าเป็นพนักงานของ กปภ. ทำเว็บไซต์หลอกประชาชนให้ดาวน์โหลด Application ใหม่ของ กปภ. ทำให้ลูกค้าโอนเงินไปให้มิจฉาชีพในการชำระเงินค่าน้ำประปา แต่เนื่องด้วยค่าน้ำประปาที่ลูกค้าจ่ายไปประมาณ 100-200 บาท ลูกค้าจึงไม่ได้ไปแจ้งความเพื่อดำเนินคดีกับมิจฉาชีพ อีกประเด็นคือ มิจฉาชีพนำ Application ของการประปานครหลวงมาหลอกลูกค้าการประปาส่วนภูมิภาค เนื่องจากหน้าตา Application ค่อนข้างคล้ายกันถือว่าเป็นการฟิชชิ่งแบบหนึ่ง”

(ผู้ให้ข้อมูลสำคัญที่ 1, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

“มีการปลอมแปลงเว็บไซต์ระบบตรวจสอบการฉีดวัคซีน หรือหมอพร้อม ซึ่งเป็นเว็บไซต์จัดทำโดยกระทรวงมหาดไทยร่วมกับกระทรวงสาธารณสุข เพื่อเพิ่มช่องทางตรวจสอบข้อมูลการฉีดวัคซีนให้กับประชาชน โดยที่เว็บไซต์จริง ระบบแจ้งเตือนว่า เลขประจำตัวประชาชนและเลข Laser ไม่ถูกต้อง ซึ่งเว็บไซต์นี้ใช้เฉพาะผู้ที่ฉีดวัคซีนแล้วเท่านั้น ไม่ได้เชื่อมโยงกับข้อมูลอื่น ในขณะที่เว็บปลอม ระบบจะไม่สามารถตรวจสอบความถูกต้องของเลขประจำตัวประชาชนและเลข Laser ได้”

(ผู้ให้ข้อมูลสำคัญที่ 13, สัมภาษณ์เมื่อวันที่ 25 เมษายน 2566)

“ในส่วนที่เคยได้รับแจ้งความมีในหลายรูปแบบมาก เช่น การแฮกเข้าไปเพื่อขโมยข้อมูล ออกมาขายหรือขายให้บริษัทคู่แข่งทางการค้า การแฮกเพื่อเปลี่ยนหน้าตาเว็บไซต์ การ แฮกบัญชีโซเชียลมีเดียเพื่อนำไปหลอกคนใกล้ชิดเหยื่อโอนเงิน การแฮกบัญชีโซเชียลมีเดียที่เป็นอินฟูอินเซอร์เพื่อนำช่องทางหรือแอคเคาท์นั้นๆ ไป

จำหน่าย การโจมตีเซิฟเวอร์เพื่อให้เกิดความเสียหาย การโจมตีเซิฟเวอร์ในลักษณะบูสฟอสต์เพื่อสุ่มรหัสในการแลกโค้ดหรือรางวัล”
(ผู้ให้ข้อมูลสำคัญที่ 16, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

โดยสรุปแล้วภัยคุกคามโดยส่วนใหญ่ที่เคยเกิดขึ้นกับหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ (CII) อยู่ในรูปแบบของการปล่อยมัลแวร์เพื่อทำการบุกรุกเครื่องคอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์ที่สร้างความปั่นป่วนและก่อกวนให้คอมพิวเตอร์ผิดปกติ แต่ปัจจุบันภัยคุกคามที่หน่วยงาน CII ต้องเผชิญมากขึ้น คือ การพยายามเข้าถึงระบบฐานข้อมูลของแฮกเกอร์ในระบบสารสนเทศที่สำคัญและการสแกนช่องโหว่เว็บไซต์รวมถึงแอปพลิเคชันองค์กร ทำให้เว็บไซต์ล่มและปฏิเสธการให้บริการ อีกทั้งแฮกเกอร์ได้ทำการปลอมแปลงระบบ โดยสร้างลิงก์ขึ้นมาเพื่อนำไปหลอกลวงและหาผลประโยชน์จากผู้อื่นด้วยวิธีการใหม่ๆที่หาตัวจับยากมากขึ้น

4.2.2 ผลกระทบจากสถานการณ์ภัยคุกคามทางไซเบอร์

จากปัญหาภัยคุกคามทางไซเบอร์ที่เกิดขึ้นหลากหลายรูปแบบที่กล่าวมาในข้างต้น สามารถนำไปสู่การรั่วไหลของข้อมูล การหยุดทำงานของระบบ การสูญเสียข้อมูลที่สำคัญ การสูญเสียทางการเงิน และความเสียหายต่อชื่อเสียงขององค์กร การโจมตีทางไซเบอร์ยังสามารถก่อกวนและทำลายระบบเครือข่าย ข้อมูลสารสนเทศ กระทบกระเทือนถึงการให้บริการและความมั่นคงปลอดภัยของหน่วยงานโครงสร้างพื้นฐานที่สำคัญ การปรับเปลี่ยนนโยบายและยุทธศาสตร์ด้านการกำกับดูแลและรับมือภัยไซเบอร์ขององค์กร รวมถึงด้านอื่นๆที่เกี่ยวข้อง ซึ่งนำไปสู่ผลกระทบทางเศรษฐกิจและสังคมที่สำคัญ รวมถึงระบบการปฏิบัติงานทั้งภาครัฐและเอกชน ผู้ให้ข้อมูลสำคัญได้ให้ข้อมูลในประเด็นผลกระทบจากสถานการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับองค์กรไว้ ดังนี้

4.2.2.1 ด้านระบบสารสนเทศและเครือข่าย

จากข้อมูลที่สำคัญของเหตุการณ์ภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบระบบคอมพิวเตอร์ เครือข่ายและสารสนเทศไม่ว่าจะเป็นอินเตอร์เน็ต เครื่องแม่ข่ายหรือ Server รวมถึงระบบที่สำคัญในองค์กรมีความคล้ายคลึงกันมีลักษณะการตอบสนองต่อการใช้งานที่ผิดปกติหรือมีการทำงานของระบบที่ไม่เหมือนเดิม หรือผิดเพี้ยนไปจากเดิมอย่างที่ควรจะเป็น เช่น ช้าลง หยุดชะงัก ไม่สามารถใช้งานต่อไปได้ เป็นต้น สอดคล้องกับผู้ให้ข้อมูลสำคัญ ดังนี้

“ที่เคยประสบคือ ผลกระทบภัยคุกคามทำให้ระบบไม่สามารถใช้งานได้ชั่วคราว แต่ถ้าระบบไหนมีจุดอ่อนหรือมีเหตุต้องว่าจะเกิดภัยคุกคาม เราจะต้องปิดสวิตซ์กันไปก่อน แล้วก็ต้องตรวจสอบหาสาเหตุ เพราะฉะนั้น ระบบสารสนเทศหรือเครือข่าย จะต้องหยุดให้บริการไปจนกว่าจะตรวจสอบหาสาเหตุได้จึงจะ on process ขึ้นมาใหม่ ซึ่งการใช้เวลาในการแก้ไขปัญหาขึ้นอยู่กับแต่ละกรณี แต่ที่ผ่านมาแก้ไขปัญหาได้ภายในไม่กี่ชั่วโมง”

(ผู้ให้ข้อมูลสำคัญที่ 7, สัมภาษณ์เมื่อวันที่ 26 พฤษภาคม 2566)

“ยกตัวอย่างในกรณีของโครงการ ชิมชอปใช้ เฟสที่ 2 ของภาครัฐ ที่ระบบการ ลงทะเบียนเกิดการล่ม เนื่องจาก มีผู้ใช้บางคนที่พยามใช้สคริปในการแย่งช่องทางการเข้าใช้ของประชาชนคนอื่น และใช้คำสั่งจำนวนมาก ส่งเข้ามายัง Server ของโครงการทำให้ระบบ ไม่สามารถให้บริการได้อย่างปกติ ก็ส่งผลให้ประชาชนไม่สามารถเข้าลงทะเบียนได้”

(ผู้ให้ข้อมูลสำคัญที่ 16, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

นอกจากนี้ ผู้ให้ข้อมูลสำคัญคนที่ 2 และผู้ให้ข้อมูลสำคัญคนที่ 14 เปิดเผยว่า ภัยคุกคามทางไซเบอร์ด้านระบบสารสนเทศและเครือข่ายของสำนักงานในปัจจุบันส่งผลกระกระทบในระดับต่ำ อย่างไรก็ตาม ระบบเครือข่ายเป็นช่องทางแรกที่ผู้ไม่หวังดีพยายามเข้ามาสแกนช่องโหว่ และองค์กรได้ให้ความสำคัญเพื่อลดผลกระทบในส่วนนี้โดยมีการเฝ้าระวังและติดตามภัยคุกคามทางไซเบอร์ที่เกิดขึ้นใหม่ และพยายามจำกัดช่องทางที่จะให้เข้าถึงในระบบสารสนเทศขององค์กรให้น้อยที่สุด รวมถึงการแบ่งแยกสิทธิ์ในการเข้าถึงระบบสารสนเทศของเจ้าหน้าที่กับบุคคลภายนอกออกจากกัน พร้อมจัดทำแนวทางและแผนในการเตรียมความพร้อมรับมือสถานกาณณ์ฉุกเฉิน และมีการทบทวนนโยบายและแผนที่เกี่ยวข้องให้เป็นปัจจุบันอยู่เสมอ อีกทั้งในทางเทคนิคระบบสารสนเทศและเครือข่ายยังถูกออกแบบให้มีความมั่นคงปลอดภัยครอบคลุมในทุกมิติ เช่นเดียวกับการแสดงข้อคิดเห็นและตัวอย่างที่องค์กรเผชิญจากสถานการณ์ภัยคุกคามทางไซเบอร์ที่ผ่านของผู้ให้ข้อมูลสำคัญ ดังนี้

“ทำให้เรามีแผนการบริหารจัดการที่เปลี่ยนไป เช่น ระหว่างที่เกิดโรคระบาดทำให้เราไม่สามารถเข้ามาใช้งานที่ออฟฟิตได้ ในด้าน network security เราก็จะมีวิธีการและช่องทาง ทั้งที่เป็นการรีโมทเข้ามาเป็นฮาร์ดแวร์ โทรเคน และมีการทำโครงสร้างรองรับในประเด็นนี้”

(ผู้ให้ข้อมูลสำคัญที่ 3, สัมภาษณ์เมื่อวันที่ 30 มีนาคม 2566)

“เมื่อเราเจอภัยคุกคามเราจะต้อง disconnect คือยุติการเชื่อมโยงอินเตอร์เน็ตทั้งหมด แล้วเราก็มีการทำการ recovery ระบบ และเราก็ไม่รู้ว่า hacker ฝั่งระบบอะไรไว้ ซึ่งมีการทำ back draw ในภายหลัง แต่ระบบ HR ระบบลูกค้า จะไม่โดนเนื่องจากเราแยกระบบเหล่านี้ออกจากระบบหลักขององค์กร เพราะถ้าโดนอันใดอันนึงมันจะไม่ลามไปสู่อีกอันนึง แต่ ณ ตอนนี้ระบบใหญ่ๆไม่โดนโจมตี แต่เจอระบบเล็กๆ เป็นระบบ management ระบบ HR ระบบที่เป็นเอกสารต่างๆ ระบบลูกค้า เนื่องจากเรามีการ design ระบบที่แยกออกจากกัน เพราะถ้าหากมีระบบอันใดอันนึงมันจะไม่ลามไประบบที่มันสำคัญ และเราจะมีการทำ Domain touch ดูแลระบบ 24 ชม. แต่เมื่อเกิดเหตุการณ์ภัยคุกคามเราจะหยุดระบบเพื่อตรวจสอบก่อนประมาณ 1 วัน”

(ผู้ให้ข้อมูลสำคัญที่ 4, สัมภาษณ์เมื่อวันที่ 31 มีนาคม 2566)

“ภัยคุกคามด้านไซเบอร์ที่ส่งผลกระทบต่อองค์กรในปัจจุบันอยู่ในระดับผลกระทบที่ต่ำ สืบเนื่องจากหน่วยงานมีการออกมาตรฐานกำหนดหลักเกณฑ์การรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศโดยภายรวม โดยใช้กฎหมายระเบียบ แนวนโยบายและแนวปฏิบัติที่เกี่ยวข้อง เช่น พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ แนวนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ นโยบายและแผนปฏิบัติการว่าด้วยความมั่นคงปลอดภัยไซเบอร์ เป็นมาตรฐานและแนวทางเพื่อจัดทำหลักปฏิบัติหรือวิธีปฏิบัติที่ช่วยลดความเสี่ยงจากภัยคุกคามไซเบอร์ที่เกิดขึ้นให้อยู่ในระดับที่องค์กรยอมรับได้ และส่งผลกระทบต่อระบบสารสนเทศขององค์กรน้อยที่สุด”

(ผู้ให้ข้อมูลสำคัญที่ 14, สัมภาษณ์เมื่อวันที่ 18 เมษายน 2566)

4.2.2.2 ด้านข้อมูลสารสนเทศ

ภัยคุกคามทางไซเบอร์ส่งผลกระทบอย่างมากต่อความปลอดภัยของข้อมูล ซึ่งอาจส่งผลให้เกิดการเข้าถึงโดยไม่ได้รับอนุญาต การโจรกรรม หรือการทำลายข้อมูลที่ละเอียดอ่อน รวมถึงการหยุดชะงักของการดำเนินธุรกิจที่สำคัญ และอาจส่งผลต่อการรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งานของข้อมูล จนกระทั่งนำไปสู่การส่งผลร้ายแรงต่อบุคคล องค์กร และสังคม อย่างไรก็ดี ผลกระทบด้านข้อมูลสารสนเทศจากสถานการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในใน ประเทศไทย สอดคล้องกับผู้ให้ข้อมูลสำคัญคนที่ 7 ดังนี้

> *“จากกรณีภัยคุกคามที่เกิดขึ้นกับโรงพยาบาลสระบุรีและโรงพยาบาลเพชรบูรณ์ ปัญหาที่กระทบด้านข้อมูลนั้นอาจจะไม่สามารถเรียกดูข้อมูลย้อนหลังได้ แต่มีระยะเวลาการกู้คืนข้อมูล ซึ่งขึ้นอยู่กับหลายปัจจัย อันแรกเลยก็คือ 1. มีการ backup ข้อมูล ซึ่งจริงๆแล้วโรงพยาบาลเกือบทุกแผนกมี แต่ลักษณะของการ backup ระยะมันน้อยหรือมาก อย่างเช่นที่เพชรบูรณ์กับที่สระบุรี ระยะเวลาที่ใช้ก็ประมาณวันนึงที่จะเอาข้อมูลคืนมาได้แต่ไม่หมด แต่ถามว่าผลกระทบด้านการรักษาพยาบาลไม่มีผลกระทบอะไรมาก เพราะว่าโดยส่วนใหญ่คุณหมอเขาก็จะมีการซักประวัติย้อนหลังอยู่ เพราะว่าข้อมูลรั่วไหลและข้อมูลที่ที่หลุดโดยส่วนใหญ่ก็จะเป็นข้อมูลเก่าๆหรือข้อมูลที่ยังไม่แน่ใจว่าเปิดเผยได้หรือไม่อะไรทำนองนี้ แต่เท่าที่ทราบส่วนใหญ่จะเป็นข้อมูลรายบุคคล เช่น ชื่อ สกุล ไม่ได้เป็นข้อมูลด้านสุขภาพ”*
>
> (ผู้ให้ข้อมูลสำคัญที่ 7, สัมภาษณ์เมื่อวันที่ 26 พฤษภาคม 2566)

ในขณะที่ความคิดเห็นในประเด็นผลกระทบจากภัยคุกคามทางไซเบอร์ด้านข้อมูลของผู้บริหารและผู้เชี่ยวชาญหลายองค์กรนั้น ได้อธิบายโดยมีการหยิบยก พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลมาอ้างอิงเพื่อให้เกิดความชัดเจนขึ้น และให้ข้อมูลในทิศทางเดียวกันว่าข้อมูลที่แฮกเกอร์ได้ไปนั้นไม่ได้เป็นข้อมูลที่สำคัญแต่เป็นข้อมูลทั่วไปขององค์กร ดังเช่นผู้ให้ข้อมูลสำคัญดังต่อไปนี้

> *“ไม่ส่งผลกระทบด้านสารสนเทศ แต่เราพยายามร่วมมือในส่วนของการปกป้องข้อมูลการรักษาความลับของข้อมูลของไม่ว่าจะ*

เป็นข้อมูลผู้ใช้น้ำหรือของพนักงาน เราพยายามร่วมมือกันเพื่อให้การปกป้องข้อมูลเป็นตัวอย่างตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แล้วก็ตามที่ที่องค์กรกำหนดไว้ เพราะตอนนี้การประปาส่วนภูมิภาคก็ได้มีการกำหนดแล้วและออกนโยบาย รวมถึงแนวทางปฏิบัติทางด้านการรักษาความลับของข้อมูล"

(ผู้ให้ข้อมูลสำคัญที่ 2, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

"ในปี 2554 เกิดน้ำท่วมหนักทำให้เรามีระบบ BCP หรือ Business Continuity Planเพราะฉะนั้นองค์กรใดไม่มีแผน BCP หรือแผนสำรอง ก็จะทำให้เกิดความเสียหาย ดังนั้นแผนรับมือเหตุฉุกเฉินด้าน IT ควรต้องมี และปัจจุบันก็จะมีเรื่องของข้อมูลรั่วไหล ก็เลยต้องมีการร่วมมือกันระหว่าง PDPA และ Cyber"

(ผู้ให้ข้อมูลสำคัญที่ 10, สัมภาษณ์เมื่อวันที่ 27 มีนาคม 2566)

นอกจากนี้ หน่วยงานด้านการป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีได้ให้ข้อคิดเห็นในประเด็นข้อมูลองค์กรที่ส่งผลกระทบต่อประชาชน อันเนื่องมาจากข้อมูลที่แฮกเกอร์ขโมยจากฐานข้อมูลระบบสารสนเทศขององค์กรไปนั้นคือข้อมูลส่วนบุคคลของประชาชน รวมทั้งแสดงทรรศนะในการป้องกันข้อมูลรั่วไหลในฐานะผู้ขับเคลื่อนกฎหมายที่เกี่ยวข้องโดยเฉพาะด้านความมั่นคงปลอดภัยไซเบอร์ สอดคล้องกับผู้ให้ข้อมูลสำคัญ ดังนี้

"มีหลายกรณีที่หน่วยงานโครงสร้างพื้นฐานโดนภัยคุกคามทางไซเบอร์เป็นผลกระทบขนาดใหญ่ ที่ส่งผลต่อประชาชนจำนวนมาก อย่างปฏิเสธไม่ได้ ยกตัวอย่าง 1. กรณี ของ รพ.สระบุรี ที่โดน กลุ่มคนร้าย ใช้ ransomware โจมตีเข้ารหัสพร้อมเรียกค่าไถ่ ส่งผลให้ระบบการรักษาคนไข้เกิดปัญหาด้านการเข้าถึงข้อมูลไม่ว่าจะเป็นประวัติการรักษา การนัดหมาย ร่วมถึงประวัติการใช้ยาต่างๆ และส่งผลโดยตรงกับประชาชน ทั้งนี้ หน่วยงาน ปอท. เอง เป็นผู้ที่ต้องเข้าแก้ไขปัญหา แต่ด้วยปัจจัยหลายด้าน ไม่ว่าจะเป็นการก่อเหตุอาจจะเกิดจากต่างประเทศ การโจมตีในระดับความซับซ้อน ทำให้ยากที่จะสืบสวน และการช่วยเหลือเพื่อกู้คืนข้อมูล 2. กรณีของฐานข้อมูลของประชาชน หลุดขายในโลกอินเตอร์เน็ต อันเนื่องมาจาก ข้อมูลจากหน่วยงานของรัฐ ส่งผลกระทบต่อประชาชน

เนื่องมาจากข้อมูลที่ประชาชนทั่วไปให้ไว้กับภาครัฐมักเป็นข้อมูลส่วนบุคคลที่สำคัญ และเมื่อข้อมูลต่างๆพวกนี้ หลุดไปสู่อาชญากร ในบางข้อมูลอาจจะทำให้ประชาชน ต้องเสียทรัพย์สินหรือถูกนำเอามาหลอกให้ประชาชน หลงเชื่อ ในการฉ้อโกง ได้อีกในช่องทางอื่นๆ อีกทั้งด้านข้อมูลส่วนบุคคลพื้นฐานที่ถูกขโมยออกจากหน่วยงานได้ ย่อมกระทบถึงความปลอดภัยในชีวิต หรือแม้กระทั้งการรักษาความปลอดภัยขององค์กรอีกด้วย"

(ผู้ให้ข้อมูลสำคัญที่ 16, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

"จากที่เคยประสบพบการถูกภัยคุกคามในด้านข้อมูลของเหยื่อ หรือผู้เสียหาย ยกตัวอย่าง การถูกเข้าถึงข้อมูลของเหยื่อ และนำข้อมูลนั้นไปต่อยอดการกระทำความผิด เช่น การฟิชชิ่งเหยื่อเพื่อหวังได้บัญชีโซเชียลมีเดีย และนำไปหลอกบุคคลอื่นให้เสียทรัพย์ เป็นต้น"

(ผู้ให้ข้อมูลสำคัญที่ 17, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

"ในด้านระบบบริหารจัดการความปลอดภัยของข้อมูล เรามุ่งเน้นการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยในการใช้ทรัพยากรสารสนเทศภายในองค์กร หรือ Security Awareness Training เช่น การศึกษาข้อกฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ ไม่ว่าจะเป็นเรื่องของ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และมาตรฐานด้านความปลอดภัย ISO 27001"

(ผู้ให้ข้อมูลสำคัญที่ 18, สัมภาษณ์เมื่อวันที่ 28 เมษายน 2566)

4.2.2.3 ด้านการให้บริการ

สำหรับการให้บริการด้านไอทีมีผลกระทบต่อบุคลากรทุกระดับในองค์กรไม่ว่าจะเป็นผู้มีส่วนได้เสีย ผู้จัดการ และผู้ใช้งาน หรือผู้เชี่ยวชาญที่ให้บริการที่เกี่ยวข้องกับไอทีและกระบวนการแก้ปัญหาแบบเบ็ดเสร็จให้กับธุรกิจขององค์กร นอกจากส่งผลกระทบภายในองค์กรแล้วยังส่งผลกระทบต่อลูกค้าและพันธมิตรทางธุรกิจ รวมถึงประชาชนที่รับบริการจากการใช้ระบบ

สารสนเทศของหน่วยงานโครงสร้างพื้นฐานที่สำคัญ โดยเฉพาะด้านสาธารณสุข สาธารณูปโภค รวมถึงการให้บริการประชาชนจากหน่วยงานด้านยุติธรรม ซึ่งสอดคล้องกับผู้ให้ข้อมูลสำคัญ ดังนี้

“การให้บริการ คือจะให้บริการที่เราพบเจอว่าการโจมตี ซึ่งมีมาอย่างต่อเนื่องเพียงแต่ว่าเราพยายามจะแยกเป็นส่วนของการให้บริการในส่วนของพนักงานกับส่วนของบุคคลภายนอกออกจากกัน อย่างคนภายนอกเราก็อยากให้บริการในสถานที่ที่ทางเทคนิค ตัวนี้จะเป็นโซนที่ติดต่อระหว่างระบบสารสนเทศของการประปา หน่วยงานภายนอก คือ ผ่านทางเว็บไซต์และระบบอีเมล เป็นส่วนที่มีการติดต่อกับบุคคลภายนอกไม่ว่าจะเป็นผู้ใช้น้ำหรือประชาชนทั่วไปก็จะใช้ช่องทางนี้เป็นหลัก ส่วนอีกส่วนหนึ่งก็คือเป็นส่วนของพนักงานเราจะให้บริการผ่านช่องทาง VPN เข้ามาคือพยายามแยกส่วนให้ชัดเจนยิ่งขึ้น”

(ผู้ให้ข้อมูลสำคัญที่ 2, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

“สำหรับลูกค้าภายนอก เรามีการแจ้งให้ ลูกค้ารับทราบล่วงหน้าก่อนหยุดระบบชั่วคราวเพื่อตรวจสอบ ซึ่งส่งผลกระทบกับลูกค้าประมาณ 1-2 วันในระหว่างการตรวจสอบ และก็นำระบบใหญ่ๆ ขึ้นให้บริการเนื่องจากไม่มีผลกระทบ แต่ที่กระทบอยู่บ้างคือระบบบริหารภายใน ก็เป็นเรื่องของภายใน ซึ่งเราเองก็มีระบบบริหารภายในอื่นๆทดแทน”

(ผู้ให้ข้อมูลสำคัญที่ 4, สัมภาษณ์เมื่อวันที่ 31 มีนาคม 2566)

“ถ้าเป็นหน่วยงานบริการผลกระทบจากเหตุที่ผ่านมาคือ ทางโรงพยาบาลนั้นไม่สามารถเข้าถึงข้อมูลของคนไข้ที่มีอยู่ทั้งหมดได้ ส่งผลทำให้การทำงานของโรงพยาบาลนั้นค่อนข้างลำบากขึ้น เนื่องจากกระบวนการต่าง ๆ ต้องเปลี่ยนมาทำเป็นระบบ Manual แทน และต้องซักประวัติคนไข้ใหม่ อาจจะมีการให้บริการที่ล่าช้า แต่ยังให้บริการได้”

(ผู้ให้ข้อมูลสำคัญที่ 7, สัมภาษณ์เมื่อวันที่ 26 พฤษภาคม 2566)

“เนื่องด้วยเหตุภัยคุกคามทางไซเบอร์ในปัจจุบันที่มีมากขึ้น หน่วยงานกองกำกับการ 1 กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี เดิมได้ดำเนินการรับแจ้งความร้องทุกข์กรณีอาชญากรรมคอมพิวเตอร์ แต่ปัจจุบันจะมีหน่วยงานของกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี ดำเนินการในส่วนนี้ด้วย โดยแบ่งลักษณะคดีที่จะรับร้องทุกข์ที่ต่างกันออกไป”

(ผู้ให้ข้อมูลสำคัญที่ 17, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

“ยกตัวอย่างปัญหาที่พบคือภัยคุกคามทางไซเบอร์ด้วย DDoS ที่ทำให้ความสามารถในการให้บริการของลูกค้าหรือผู้ใช้งานอ่อนด้อยลง โดยการถูกโจมตีจากผู้ไม่ประสงค์ดีทำให้บริการด้อยประสิทธิภาพลง ถึงขั้นหยุดชะงักในการให้บริการ หรือไม่สามารถให้บริการได้ ผู้ใช้บริการรอนานขึ้น”

(ผู้ให้ข้อมูลสำคัญที่ 20, สัมภาษณ์เมื่อวันที่ 19 มีนาคม 2566)

4.2.2.4 ด้านความมั่นคงปลอดภัย

จากการสัมภาษณ์ผู้ให้ข้อมูล ประเด็นผลกระทบด้านความมั่นคงปลอดภัย เหตุผลโดยส่วนมากคือ ภัยคุกคามทางไซเบอร์ที่ผ่านมาไม่ส่งผลกระทบถึงความมั่นคงปลอดภัย แต่เป็นใบเบิกทางให้หลายหน่วยงานมีการบริหารจัดการที่ดีขึ้นจากประสบการณ์การเผชิญภัยคุกคามที่ผ่านมา ทำให้เกิดการปรับปรุง เปลี่ยนแปลง วิธีการรับมือภัยคุกคามแบบเดิม ๆ เพื่อการเตรียมความพร้อมและมาตรการในการรับมือให้ครอบคลุมทุกภาคส่วนขององค์กรมากขึ้น อาทิ ภาพรวมของ แนวทางการรักษาความปลอดภัย (security safeguards guidelines), วิธีการบริหารความเสี่ยง (risk management approaches), วิธีปฏิบัติที่เป็นเลิศ (best practices) และเทคโนโลยี (technologies) ที่สามารถปกป้องสภาพแวดล้อมทางไซเบอร์ องค์กร และสินทรัพย์ของผู้ใช้งาน ได้แก่ อุปกรณ์สาหรับเชื่อมต่อคอมพิวเตอร์, ข้อมูลส่วนตัว, โครงสร้างพื้นฐาน, แอปพลิเคชัน, บริการ, ระบบสารสนเทศ และภาพรวมของการส่งผ่านหรือเก็บข้อมูลในไซเบอร์ ซึ่งสอดคล้องกับผู้ให้ข้อมูลสำคัญดังต่อไปนี้

“ไม่มีผลกระทบเนื่องด้วยมี security ค่อนข้างดี การเกิดจากช่องโหว่นั้น ถ้าคนรู้เทคนิค เวลาเกิดช่องโหว่เพียงไม่กี่ตัว ก็จะสามารถจัดการได้ ซึ่งช่วงนั้นเรามีการอัพเดต Patch แต่อาจไม่เพียงพอ ซึ่งต้องอัพเดตเวอร์ชั่น ซึ่ง Patch ที่ออกมามัน Delay กว่านั้น เพราะว่าการอัพเดต Patch กับ server เวลาออก Patch มาใหม่จะไม่มีการอัพเดตในทันที เนื่องจากต้องนำ Patch มาทำการทดสอบก่อนนำมาใช้เพื่อให้รู้ว่าจะเกิดผลกระทบกับองค์กรหรือไม่ แต่ในส่วนของ client เราจะ Patch เลย จึงไม่ค่อยกระทบในด้านนี้”

(ผู้ให้ข้อมูลสำคัญที่ 4, สัมภาษณ์เมื่อวันที่ 31 มีนาคม 2566)

“ผลกระทบจะเกิดจากการ Impact และ likelihood ในระดับความเสี่ยง แต่ว่าการโจมตีเข้ามาแล้วเราจัดการได้ สุดท้ายผลกระทบมันก็จะยังอยู่ในเกณฑ์ที่ยอมรับได้ เพราะถ้าเกิดว่าอยู่ในเกณฑ์ที่ยอมรับไม่ได้ ก็ต้องมีการแถลงข่าวมีการทำ BCP มีการทำพวก crisis เพราะว่าเหตุการณ์ที่เกิดขึ้นมีทุกวัน แต่ว่าเราก็จัดการทัน และยังไม่พบเหตุของการรั่วไหลของข้อมูลก็ยังอยู่ในเกณฑ์ที่ยอมรับได้”

(ผู้ให้ข้อมูลสำคัญที่ 9, สัมภาษณ์เมื่อวันที่ 30 มีนาคม 2566)

“ในส่วนของหน่วยงานเมื่อพบว่ามีลักษณะคดี หรือรูปแบบใดที่ประชาชนได้รับความเสียหาย ก็จะมีการประชาสัมพันธ์ถึงลักษณะคดีที่เกิดขึ้น และแนะนำแนวทางการป้องกันให้แกประชาชนได้ทราบและระมัดระวังการตกเป็นเหยื่อได้”

(ผู้ให้ข้อมูลสำคัญที่ 17, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

“ในฐานะที่สำนักงานตำรวจแห่งชาติเป็นหน่วยงานซึ่งมีหน้าที่ต้องดูแลด้านความมั่นคงของประเทศที่มีโครงสร้างพื้นฐานสำคัญ ในการจัดเก็บข้อมูลที่มีความสำคัญด้านความมั่นคง ซึ่งปัจจุบันระบบการทำงานของสำนักงานตำรวจแห่งชาติได้นำเทคโนโลยีสารสนเทศมาใช้อย่างกว้างขวาว อาทิเช่น ระบบ Polis และระบบ Crimes เป็นระบบสารสนเทศหลักที่มีความสำคัญต่อการทำงานของตำรวจ ในขณะเดียวกันก็มีความเสี่ยงต่อการถูกโจมตี รวมทั้งการโจรกรรมข้อมูล

สูง ตำรวจจึงมีความจำเป็นต้องมีมาตรการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศครบทั้ง 3 ด้าน ได้แก่ 1. ด้านบุคลากร หรือ People 2. ด้านกระบวนการปฏิบัติงาน หรือ Process และ 3. ด้านเทคโนโลยี หรือ Technology เพื่อให้ผู้ใช้งานระบบสามารถใช้งานระบบได้อย่างมีประสิทธิภาพ ปลอดภัย และเกิดประโยชน์สูงสุดแก่สำนักงานตำรวจแห่งชาติ"

(ผู้ให้ข้อมูลสำคัญที่ 18, สัมภาษณ์เมื่อวันที่ 28 เมษายน 2566)

"กรณีถ้ามีข้อมูลรั่วไหลหรือมีภัยคุกคามก็จะมีบริษัทประกันภัยรับผิดชอบให้ในส่วนนี้ ทำให้ลดความเสี่ยงองค์กร แต่ในขณะเดียวกันการตกลงทำ contract ระหว่างหน่วยงานกับบริษัทประกันภัยต้องมีการดำเนินงานตามข้อตกลงของบริษัทประกันภัยในเรื่องของมาตรฐานต่างๆที่องค์กรจำเป็นต้องมี เช่น ต้องรักษามาตรฐาน และต้องมีการสร้าง Awareness ทุกปี รวมถึงคุณสมบัติอื่นๆตามเงื่อนไขของบริษัทประกัน ทำให้ Cyber Insurance เป็นแนวทางที่ดีด้านความมั่นคงปลอดภัยไซเบอร์มากกว่านโยบายและแผนยุทธศาสตร์ ซึ่ง Cyber Insurance จะเข้ามาอุดช่องโหว่ในเรื่องนี้"

(ผู้ให้ข้อมูลสำคัญที่ 21, สัมภาษณ์เมื่อวันที่ 25 มีนาคม 2566)

ในขณะที่ ผู้ให้ข้อมูลสำคัญคนที่ 11 ได้แสดงให้เห็นถึงมุมมองในแง่ที่แตกต่างออกไปกล่าวคือ ความมั่นคงปลอดภัยของห่วงโซ่อุปทาน หรือ Supply Chain Security เป็นประเด็นความมั่นคงจากการที่จะต้องพึ่งพาเทคโนโลยีต่างชาติ ทำให้รัฐขาดศักยภาพในการบริหารจัดการไซเบอร์ภายในประเทศ ประเทศไทยต้องพึ่งพาเทคโนโลยีต่างชาติ จึงมีความเสี่ยงที่จะถูกโจมตีผ่านเทคโนโลยีต่างชาติที่ไม่มีมาตรฐานความปลอดภัย นอกจากนี้ สถานการณ์ความขัดแย้งระหว่างรัสเซียและยูเครนที่ผ่านมา พบการใช้เครื่องมือทางไซเบอร์ในการสนับสนุนปฏิบัติการทางทหารของทั้งสองฝ่ายในลักษณะ สงครามแบบผสม หรือ Hybrid Warfare ประเทศไทยต้องระมัดระวังการโดนลูกหลง หรือ spillover คือผลกระทบจากภายนอก หากภัยคุกคามและปฏิบัติการทางไซเบอร์ขยายวงกว้างมากขึ้น

4.2.2.5 ด้านการกำกับดูแล

การบริหารจัดการเฉพาะภายในองค์กรอาจไม่เพียงพอต่อการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ขององค์กร ซึ่งจากข้อมูลผู้ให้สัมภาษณ์หน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศทั้งด้านสาธารณสุข สาธารณูปโภคและด้านการเงินการธนาคาร ได้กำหนดนโยบายและแผนบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ซึ่งมีคณะกรรมการ หรือที่รู้จักในนามของ บอร์ดบริหาร (Board) ที่เป็นบุคลากรระดับบริหารทั้งภายในและภายนอก รวมทั้งผู้ทรงคุณวุฒิและที่ปรึกษา เป็นกรรมการในการกำกับดูแลโดยมีประธานบอร์ดเป็นผู้นำ มีอำนาจหน้าที่และความรับผิดชอบถูกกำหนดโดยรัฐบาล พิจารณาถึงความเสี่ยงที่เกี่ยวข้องกับการยอมรับความเสี่ยงของคณะกรรมการบริหาร รวมถึงกฎหมายและกฎระเบียบข้อบังคับที่ออกมาบังคับใช้ซึ่งเข้มข้นขึ้นและผลกระทบที่มีผู้มีส่วนได้เสียต้องการความเชื่อมั่นเพิ่มขึ้นว่า ในการดำเนินงานจริงองค์กรได้ปฏิบัติตามกฎหมายและกฎระเบียบข้อบังคับ และดำเนินการตามแนวปฏิบัติที่ดีด้านการกำกับดูแลองค์กร หากแต่มีการบริหารจัดการภายในองค์กรที่แตกต่างกันไป สอดคล้องกับผู้ให้ข้อมูลสำคัญ ดังนี้

> *“กปภ. มีผู้ว่าการ กรรมการบอร์ดและอนุกรรมการ ให้ความสำคัญในด้านการพัฒนาดิจิทัลให้ตอบโจทย์เรื่องการบริหารจัดการด้าน เงิน คน และเวลา รวมถึงความปลอดภัยให้มีการจัดทำ Pen Test ซึ่งเป็นวิธีการประเมินความเสี่ยงด้วยการทดสอบเจาะระบบเพื่อค้นหาจุดอ่อนในการเข้าถึงระบบต่างๆ โดยใช้ผู้เชี่ยวชาญด้านไซเบอร์ที่มี Certificate ด้านมาตรฐาน ช่วยในการประเมินความเสี่ยงของระบบและลูกค้าว่ามีความเสี่ยงตรงจุดใด พร้อมกับการแจ้งผลการทดสอบ และประเมินความเสี่ยงเพื่อเตรียมการป้องกันไว้ก่อน รวมทั้งมีการจัดสัมมนาให้ความรู้จากผู้บริหารระดับสูงผ่านช่องทางทั้ง Onsite และ Online ในส่วนของพนักงานก็มีแนวทางให้พนักงานทั้งองค์กรเข้าอบรมด้าน Cybersecurity Awareness ด้าน PDPA ผ่านเว็บไซต์ของ DGA และยืนยันผลการอบรมของพนักงานโดยการให้พนักงาน Upload ประกาศนียบัตรอิเล็กทรอนิกส์ที่ได้รับหลังการฝึกอบรมจาก DGA เข้าระบบจัดเก็บเอกสารอิเล็กทรอนิกส์ของหน่วยงานพัฒนาทรัพยากรบุคคลภายใน กปภ. ผ่าน Intranet ขององค์กร”*
>
> (ผู้ให้ข้อมูลสำคัญที่ 1, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

“เรามีการกำกับดูแลเริ่มตั้งแต่ผู้บริหารระดับสูง คือ บอร์ดบริหารไปจนถึงผู้ว่าการลงมา การกำกับดูแลการเฝ้าระวังหรือการรับมือจะต้องดำเนินการให้ให้มีประสิทธิภาพ ทางด้านผู้บริหารก็คือพยายามจะให้ความช่วยเหลือแล้วก็ติดตามอย่างสม่ำเสมอยกตัวอย่างเช่น เราก็จะต้องมีการรายงานนะครับเหตุการณ์ผิดปกติ ถ้าเกิดกรณีที่เป็นเหตุปกติที่ทั่วไปก็จะรายงานนะเดือนละ 1 ครั้ง แต่ถ้าเป็นเหตุผิดปกติที่มีระดับความรุนแรง เราจะต้องมีการแจ้งไปยังหน่วยงานกำกับดูแลก็คือ regulator ก่อน ในขณะเดียวกันต้องทำการแจ้ง สกมช. ให้รับทราบว่าตอนนี้เหตุการณ์ที่เกิดขึ้นเป็นเหตุการณ์ผิดปกติแล้วมีความร้ายแรงถึงขั้นร้ายแรงหรือขั้นวิกฤตภายในระยะเวลา 30 นาที”

(ผู้ให้ข้อมูลสำคัญที่ 2, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

“มีคณะกรรมการให้ทบทวนแผน และมีการกำหนดตัวชี้วัดและรายงานต่อคณะกรรมการรักษาความมั่นคงปลอดภัยตามมาตรฐาน ISO27001 แต่เนื่องด้วยปัจจุบันชื่อของคณะกรรมการฯ ของ กปน ไปอ้างอิงกับมาตรฐาน ISO27001 จึงต้องมีการปรับแก้ เป็นคณะกรรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ ของ กปน ส่วนการดำเนินการทาง กปน จะให้สอดคล้องกับ พรบ การรักษาความมั่นคงปลอดภัยไซเบอร์ 2562 โดยจัดประชุมทบทวนแผนนโยบาย และกำหนดตัวชี้วัดด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งจะมีการสั่งการให้กำกับดูแลเกี่ยวกับการควบคุมความเสี่ยงทางด้านเทคโนโลยี ให้เป็นไปตามระบบการประเมินคุณภาพรัฐวิสาหกิจ หรือ Enabler กำหนดไว้ ซึ่งจะมา audit เราเป็นระยะๆ ซึ่ง Enabler มีเจ้าภาพคือทางแผนยุทธศาสตร์ เป็นคนดำเนินการและทางเราจะตอบเฉพาะในส่วนที่เกี่ยวข้อง”

(ผู้ให้ข้อมูลสำคัญที่ 3, สัมภาษณ์เมื่อวันที่ 30 มีนาคม 2566)

“ท่านผู้บริหารการไฟฟ้าท่านจะให้ความสำคัญกับเรื่องนี้ เรามีคณะทำงาน มีระเบียบและวิธีการ ปฏิบัติกันมาหลายปีแล้ว มีการ

*กำกับตามนโยบายขององค์กรตามคณะทำงาน คปภ. ที่ประสานงานพนักงานระหว่าง OT และ IT ในการดำเนินงานร่วมกัน การ response หรือการแจ้งเหตุดำเนินการต่างๆร่วมกัน และมีการปฏิบัติตาม 24*7 หลังจากนั้นก็สามารถ control ได้ ซึ่งจากเหตุการณ์ที่เคยถูกโจมตีในปีนั้น ปีที่แล้วก็เกิด ปีนี้ก็เกิด แต่เรามี 24*7 คอยจัดการให้หมด ระบบแทบจะไม่ล่มเลย มีบ้างเล็กน้อย นี่คือข้อดีของ 24*7 และการจัดการเราคือ ระบบมีการทำงานเป็นคู่ หากตัวนึงล่ม อีกตัวนึงจะสามารถทำงานได้"*

(ผู้ให้ข้อมูลสำคัญที่ 4, สัมภาษณ์เมื่อวันที่ 31 มีนาคม 2566)

"ในด้าน cybersecurity ทางแบงก์ชาติก็ได้ให้ความสำคัญ เรามีคณะกรรมการกำกับดูแล รายงานผลการดำเนินงานให้กรรมการรับทราบ กรรมการก็มีตั้งแต่ระดับผู้ว่าการเป็นประธาน เรารายงานความก้าวหน้าให้ท่านทราบทุกๆ 3 เดือน"

(ผู้ให้ข้อมูลสำคัญที่ 5, สัมภาษณ์เมื่อวันที่ 26 เมษายน 2566)

"กรณีที่เกิดขึ้นกับโรงพยาบาลในตอนนั้น เรายังไม่มีนโยบายที่ชัดเจนนัก แต่ปัจจุบันมีการออกนโยบายในการเฝ้าระวังและมาตรการความมั่นคงปลอดภัยของโรงพยาบาลตามคำสั่งมอบหมายหน่วยงานปฏิบัติหน้าที่ควบคุมและกำกับดูแลงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสาธารณสุขและระบบสุขภาพดิจิทัล มีคณะกรรมการดิจิทัลการแพทย์ร่วมกันป้องกันความเสี่ยงด้านดิจิทัลตามมาตรฐาน Cyber Security ขั้นพื้นฐาน"

(ผู้ให้ข้อมูลสำคัญที่ 7, สัมภาษณ์เมื่อวันที่ 26 พฤษภาคม 2566)

นอกจากนี้ กลุ่มหน่วยงานที่อยู่ในระดับการกำหนดนโยบายและยุทธศาสตร์ด้านการกำกับดูแลเทคโนโลยีดิจิทัลและความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย ได้ร่วมกันปรับปรุงแผนยุทธศาสตร์ นโยบาย กฎระเบียบ ข้อบังคับและแนวปฏิบัติสำหรับองค์กรและหน่วยงานภายใต้สังกัดให้มีความชัดเจนขึ้น และคำนึงถึงผู้มีส่วนได้เสียให้สามารถดำเนินการตามแนวปฏิบัติให้ครอบคลุมทุกภาคส่วน ทั้งเชิงนโยบายและเชิงเทคนิค ซึ่งสอดคล้องกับผู้ให้ข้อมูลสำคัญ ดังนี้

“ในด้านการกำกับดูแล ผู้บริหารเน้นย้ำให้ระมัดระวังและป้องกัน เรื่องรหัส user password ของ admin และต้องมีผู้รับผิดชอบผ่าน ผู้ว่าราชการจังหวัดและผ่านหน่วยงาน NECTEC ร่วมกับ เจ้าหน้าที่ของกระทรวงมหาดไทย”

(ผู้ให้ข้อมูลสำคัญที่ 13, สัมภาษณ์เมื่อวันที่ 25 เมษายน 2566)

“สมช. มี 2 กลุ่มงานที่รับผิดชอบเรื่องภัยคุกคามทางไซเบอร์ คือ กองแผนข้ามชาติที่ดูเรื่องแผนและนโยบาย รวมถึงประสานหน่วยงานที่เกี่ยวข้องอื่นๆด้วย และมีศูนย์เทคโนโลยีสารสนเทศที่จะดูแลเรื่องระบบภายในทั้งระบบฮาร์ดแวร์และซอฟต์แวร์ และมี CIO ที่ดูแลระบบภายใน และเราเป็นหนึ่งในคณะกรรมการร่วมกับ สกมช. และหน่วยงานอื่นๆในการทำงานด้านไซเบอร์ต่างๆ ในส่วนของภาพใหญ่ สมช. เรามีสภา มช.และมีสำนักงานร้อยกองงานของ สกมช แต่ในเร็วๆนี้อาจจะมีการตั้งกรรมการชุดนึงเป็นรองเลขาฯ เป็นประธาน เพื่อที่จะติดตามในส่วนของนโยบายความมั่นคงปลอดภัยไซเบอร์ร่วมกับ สกมช. ต่อไป”

(ผู้ให้ข้อมูลสำคัญที่ 11, สัมภาษณ์เมื่อวันที่ 19 เมษายน 2566)

“ภัยคุกคามทางไซเบอร์ไม่ได้ส่งผลกระทบในการด้านการกำกับดูแล เนื่องจากสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้มีการกำกับติดตาม ดูแล และรายงานผลการดำเนินการตามแนวนโยบายและแนวปฏิบัติอย่างต่อเนื่อง เพื่อรวบรวมปัญหาและอุปสรรคที่อาจส่งผลต่อการปฏิบัติงาน พร้อมทั้งจัดทำแนวทางการแก้ไขปัญหาในสถานการณ์ดังกล่าว นอกจากนี้หน่วยงานยังได้จัดให้มีกิจกรรมสร้างความตระหนักและรู้เท่าทันภัยคุกคามทางไซเบอร์ที่เกิดขึ้นใหม่ ผ่านวิธีการและเครื่องมือในหลายรูปแบบไม่ว่าจะเป็นกิจกรรมอบรมสร้างความตระหนัก การสร้างสื่อความตระหนักรู้เช่น วีดีโอ เสียงตามสาย infographic พร้อมทั้งเผยแพร่ประชาสัมพันธ์ให้ทั้งภายในและภายนอกหน่วยงานผ่านช่องทางแพลตฟอร์มออนไลน์และอื่นๆที่เกี่ยวข้อง ทั้งนี้ก็เพื่อยกระดับความรู้ ความเข้าใจ และความ

ตระหนักอย่างเป็นระบบและต่อเนื่อง ในทุกกลุ่มเป้าหมายที่เป็นกลุ่มเสี่ยงต่อภัยไซเบอร์ที่อาจจะยังขาดความรู้ความเข้าใจเทคโนโลยีสมัยใหม่ ให้มีความพร้อมในการระวังภัยคุกคามที่ได้อาจเกิดขึ้นได้"

(ผู้ให้ข้อมูลสำคัญที่ 14, สัมภาษณ์เมื่อวันที่ 18 เมษายน 2566)

"มีการกำกับดูแลโดยให้เจ้าหน้าที่ตรวจสอบช่องโหว่กับอุปกรณ์ และ OS หากมีช่องโหว่ วิเคราะห์ว่ามีผลกระทบกับองค์กรหรือไม่ ขาดการอัพเดตหรือไม่ แผนจัดหาคอมพิวเตอร์ หรือซื้อทดแทน การกำหนดให้สิทธิ์ user เป็น user 1 คน 1 เครื่อง ไม่ว่าจะเป็น PC แต่มีการปรับให้เป็น Notebook ในช่วงโควิดให้กับพนักงาน โดยปรับนโยบายให้เปลี่ยนจาก pc เป็น NB ทุกคนในองค์กรเพื่อรองรับสถานการณ์ภัยคุกคามเช่น โควิดในอนาคต"

(ผู้ให้ข้อมูลสำคัญที่ 15, สัมภาษณ์เมื่อวันที่ 29 มีนาคม 2566)

"ในกรณีที่ได้รับแจ้งความร้องทุกข์ให้ดำเนินการติดตามหาตัวคนร้าย หรือสืบสวนกรณีมีความผิดเกิดขึ้นนั้น จะมีการกำกับการดูแลและให้ดำเนินการโดยเร็วซึ่งระบบการจัดการเร่งรัดการดำเนินการจะเป็นลักษณะการบังคับบัญชาลงมา เพื่อให้ไวต่อการแก้ปัญหาต่างๆที่ได้รับแจ้ง"

(ผู้ให้ข้อมูลสำคัญที่ 17, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

"ปฏิบัติตามประกาศคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 – 2570) สำนักงานตำรวจแห่งชาติ"

(ผู้ให้ข้อมูลสำคัญที่ 18, สัมภาษณ์เมื่อวันที่ 28 เมษายน 2566)

4.2.2.6 ด้านอื่นๆ

ผู้ให้ข้อมูลสำคัญทั้งในระดับบริหารและผู้เชี่ยวชาญได้อธิบายถึงลักษณะภัยคุกคามไซเบอร์ที่ส่งผลในแง่ของการสร้างความตระหนักให้กับบุคลากรในองค์กรทั้งพนักงานและ

ผู้บริหารระดับสูง เนื่องด้วยผลกระทบที่สำคัญเมื่อเกิดเหตุภัยคุกคามขึ้น สิ่งแรกคือชื่อเสียงขององค์กร รวมถึงความพึงพอใจของลูกค้าในการรับบริการ ซึ่งสอดคล้องกับผู้ให้ข้อมูลสำคัญ ดังนี้

“การสร้างคน พัฒนาคนในการบริการลูกค้าให้ลูกค้าพึงพอใจ และสามารถนำไปใช้ประโยชน์ได้จริง รวมทั้งการพัฒนาด้านนวัตกรรมจากหน่วยงานจากภูมิภาค รวมถึงระบบด้านความปลอดภัยต้องมีมาตรฐาน และที่สำคัญคือพนักงานต้องมีคุณธรรมจริยธรรม ปฏิบัติตาม พ.ร.บ. ด้านไซเบอร์ และการจัดซื้อจัดจ้างโครงการให้มีความโปร่งใส สร้างความตระหนักให้กับบุคลากรและให้ทำงานอย่างมีความสุข”

(ผู้ให้ข้อมูลสำคัญที่ 1, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

“ถ้าถามว่าผลกระทบก็คือว่าเป็นการที่เราจะต้องเตรียมตัวมากกว่า เตรียมตัวเพื่อเพื่อรับมือภัยคุกคามที่จะเกิดขึ้น มีการสร้างความตระหนักในส่วนของผู้ดูแลระบบและในส่วนของพนักงานให้รับทราบว่าตอนนี้การโจมตีทางไซเบอร์มีรูปแบบใดบ้าง แล้วสิ่งที่ควรปฏิบัติหรือควรรับมือในการดำเนินการจะต้องทำยังไง เราจะเน้นย้ำเพื่อรับมือในส่วนนี้เพิ่มเติม”

(ผู้ให้ข้อมูลสำคัญที่ 2, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

“จากเหตุการณ์โรงพยาบาลก็จะส่งผลกระทบในชื่อเสียงมากกว่าผลกระทบด้านอื่นๆ จะมีคำถามว่าทำไมกระทรวงสาธารณสุขไม่มีนโยบายหรือวิธีการป้องกัน ทั้ง ๆ ที่เป็นข้อมูลค่อนข้างเซนซิทีฟมากๆ รวมถึงด้านงบประมาณที่ไม่เพียงพอ โรงพยาบาลส่วนใหญ่ของกระทรวงสาธารณสุขประมาณ 70% คือโรงพยาบาลยากจน มีวิธีการป้องกันภัยคุกคามเพียงแค่ทำการ backup ข้อมูลเอาไว้เท่านั้น แต่ถามว่าจะมีการ restore ข้อมูลกลับไหม ยังไม่มีเท่าที่ทราบ ไม่มีโรงพยาบาลไหนที่ที่พยายามทำตรงนั้น เนื่องจากว่าค่อนข้างจะต้องใช้ทรัพยากรเป็นเท่าๆตัว เราก็เลยจะยังไม่มีงบประมาณขนาดนั้น เพียงแต่สิ่งที่ส่วนกลางทำได้คือ ให้โรงพยาบาลจัดหาอุปกรณ์ แต่ทางเราเองก็ไม่มีงบประมาณสนับสนุนเกี่ยวกับเรื่องของการจัดทำ ในขณะ

ที่เป็นประเด็นคำถามกับกระทรวงสาธารณสุขว่าระหว่างซื้อยากับซื้ออุปกรณ์ด้านการรักษาความมั่นคงปลอดภัย อะไรสำคัญกว่ากัน”

(ผู้ให้ข้อมูลสำคัญที่ 7, สัมภาษณ์เมื่อวันที่ 26 พฤษภาคม 2566)

“หลักๆเลยคือด้านชื่อเสียงองค์กร แต่ยกตัวอย่างกรณีของโรงพยาบาล ก็ทำให้คนตื่นตัวมากขึ้น เพราะในมุมมองของผม คนไทยจะเรียนรู้จากสื่อโซเชียลได้ดีกว่าการเรียนรู้ในห้องเรียน เพราะจริงๆ แรนซัมแวร์มีมานานแล้ว แต่พอเกิดเหตุทำให้ผู้เกี่ยวข้องตื่นตัว จึงทำให้เข้าใจว่าแรนซัมแวร์คืออะไร แล้วโรงพยาบาลสระบุรีโดนแล้วถึงเป็นข่าวดัง เพราะว่าโดนล็อคข้อมูล แล้วมีคนถามว่าล็อคข้อมูลแล้วเอาข้อมูลย้อนหลังมาดูได้หรือไม่ที่ backup ไว้ แต่มีส่วนหนึ่งที่ไม่ได้ backup ไว้เป็นปีๆ ก็เลยยิ่งทำให้ดังเข้าไปใหญ่เลย ก็เลยเป็น bad practice ที่คนนำไปเรียนรู้กันได้ แต่ถ้า advance ขึ้นมาหน่อยก็ต้องย้อนดูข้อมูล backup ว่าเมื่อไหร่ที่ข้อมูลยังไม่ติดไวรัสหรือแรนซัมแวร์ อันนี้ก็เป็นอีกสเต็ปหนึ่งที่เราต้องเรียนรู้ว่านอกจากการ backup แล้วก็ต้องมีระบบ monitor ที่ดี และทำให้เกิด mindset ใหม่คือ ภัยคุกคามเกิดขึ้นได้และอย่าตกใจ ต้องมีแผนการรับมือและแก้ไขให้กลับสู่สภาวะปกติที่ดีที่สุด เพราะถ้าเราเป็นสายป้องกันก็มักจะคิดว่าเราเก่งเสมอ แต่สมัยนี้เก่งแค่ไหนก็โดน เพราะฉะนั้นถ้าโดนปุ๊บ ต้องมีแผนสำรอง เราจะมีวิธีนำกลับคืนมายังไงมากกว่า”

(ผู้ให้ข้อมูลสำคัญที่ 10, สัมภาษณ์เมื่อวันที่ 27 มีนาคม 2566)

“สำนักงานตำรวจแห่งชาติ มีการทำ MOU กับกระทรวงศึกษา หรือมหาลัยต่างๆเพื่อยกระดับความร่วมมือ กระชับความสัมพันธ์ทางด้านวิชาการ ขยายโอกาสทางการศึกษาให้กับกำลังพลครอบคลุมทุกหน่วยงานในสังกัดสำนักงานตำรวจแห่งชาติ ตลอดจนร่วมมือกันในการแลกเปลี่ยนเสริมสร้างความรู้ ประสบการณ์และข้อมูลทางวิชาการที่เกี่ยวข้องกับการรับมือภัยคุกคามทางไซเบอร์ วิธีการโจมตีหรือการก่อภัยคุกคามทางไซเบอร์หรือในด้านอื่นๆที่เกี่ยวข้อง โดยเฉพาะกรณีภัยคุกคามทางไซเบอร์ของกลุ่มแฮกเกอร์ใน

นาม 9Near ที่สร้างความตื่นตระหนกให้สังคมและทำให้เราตื่นตัวในการป้องกันมากยิ่งขึ้น”

(ผู้ให้ข้อมูลสำคัญที่ 18, สัมภาษณ์เมื่อวันที่ 28 เมษายน 2566)

“ปัญหาที่เกิดขึ้นในเรื่องภัยไซเบอร์แบ่งออกเป็น 2 ส่วน คือ ด้านวิชาการหรือทฤษฎี และอีกด้านเป็นเรื่องของบริหารจัดการ ซึ่งถ้าเป็นด้านวิชาการ เช่น เกิดรูรั่วหรือช่องโหว่ ก็ต้องดูว่าระบบ OS มีความมั่นคงปลอดภัยแค่ไหน มีโอกาสจะถูกโจมตีได้ในลักษณะอย่างไร แต่ปัญหาส่วนใหญ่เกิดจากด้านบริหารจัดการ ยกตัวอย่างเช่น คุณได้รับ SMS ว่าถูกรางวัลที่ 1 ให้กดลิงก์ดังต่อไปนี้ และอีกตัวอย่างที่เป็นปัญหาใหญ่คือ Social Engineering หรือใช้ภาษาชาวบ้านคือ ตกทอง คือ เช่น จดหมายลูกโซ่ หรือใช้ จุดอ่อน ความกลัว ความละโมบ หรือเรื่องเงิน มาแชร์ให้กับบุคลากร เป็นการเล่นกับ Psychology ของคน ทำให้คนที่ไม่ระวังตัว ไปทำอะไรบางอย่างในสภาพการณ์ปกติที่ไม่ควรจะทำ เช่น โอนเงินไปให้คนอื่น เป็นต้น นี่คือเรื่องของบริหารจัดการไม่ใช่เรื่องเทคโนโลยีหรือวิชาการ ดังนั้น องค์กรจึงต้องให้บุคลากรจึงต้องมี Awareness เป็นเรื่องที่สำคัญ และที่สำคัญไปกว่านั้นคือการสร้างนิสัย ยกตัวอย่างเช่น กรณีใส่หมวกกันน็อค แต่บางคนไม่ใส่ ดังนั้นการบังคับใช้อาจไม่เพียงพอ และส่วนมากในเรื่องการบริหารจัดการที่เป็น Personal นั้น Awareness นั้นยังไม่พอ จึงต้องเป็นการสร้างนิสัย หรือ Habit Forming มากกว่า ยกตัวอย่างเพิ่มเติมเพื่อให้เห็นภาพยิ่งขึ้นเช่น คุณจะไม่เก็บขนมที่ตกพื้นขึ้นมากิน ซึ่งอันนี้เป็นเรื่องของนิสัยไม่ใช่เรื่องของวิชาการ เพราะเราถูกสั่งสอนมาตั้งแต่เด็กว่าของตกพื้นแล้วห้ามกิน พอหลังๆมาเรารู้ว่ามันมีเชื้อโรคแม้ว่ามองไม่เห็นเชื้อโรค แต่ถ้าเราเห็นใครหยิบของตกพื้นขึ้นมากินหรือเพื่อนหยิบใส่ปากเรา มันจะรู้สึกขยะแขยง ซึ่งความขยะแขยงนี่คือ Habit Forming คือการสร้างนิสัยให้เกิดขึ้น เพราะฉะนั้น เราจะขยะแขยงทุกครั้งที่จะกดลิงก์ใน SMS หรืออีเมล อย่างนี้เป็นต้น ซึ่งยากเพราะการสร้างนิสัยแบบนี้ต้องสร้างตั้งแต่เด็กๆ ถ้าสร้างตอนโตเรียกว่าไม้แก่ดัดยาก ดังนั้นกลุ่มคนที่เป็น Social Engineering จะรู้ว่าจะทำอย่างให้ที่จะหลอกล่อให้คนกดลิงก์ได้”

(ผู้ให้ข้อมูลสำคัญที่ 19, สัมภาษณ์เมื่อวันที่ 19 มีนาคม 2566)

สรุปได้ว่า ภัยคุกคามโดยส่วนใหญ่ที่เคยเกิดขึ้นกับหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศที่ส่งผลกระทบต่อองค์กรในปัจจุบันยังอยู่ในระดับผลกระทบที่ต่ำและระดับปานกลาง ซึ่งขึ้นอยู่กับระดับการจัดระดับความรุนแรงของแต่ละองค์กร แต่หากเป็นไปตามกรอบของ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ผู้ให้ข้อมูลสำคัญทุกท่านมีความคิดเห็นที่ตรงกันว่า ภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อองค์กรในปัจจุบันอยู่ใน ***ระดับไม่ร้ายแรง*** เนื่องด้วยหน่วยงานได้จัดเตรียมความพร้อมรับมือกับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นได้ โดยมีการกำหนดแนวทางและแผนปฏิบัติการตามมาตรการของภาครัฐในการรับมือภัยคุมคามทางไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศ (CII) นำมาใช้ในการปรับปรุงนโยบายและแนวทางในการพร้อมรับภัยคุกคามไซเบอร์ และเพื่อลดความเสี่ยงของภัยคุกคามทางไซเบอร์ที่จะเกิดขึ้นจนส่งผลกระทบต่อองค์กร

นอกจากนี้ การมีแผนรับมือเหตุการณ์ที่กำหนดไว้อย่างดีสามารถช่วยลดความรุนแรงของสถานการณ์ภัยคุกคามทางไซเบอร์ และลดผลกระทบต่อบุคคลหรือองค์กรที่ได้รับผลกระทบ แต่จากการเก็บรวบรวมข้อมูลจากผู้ให้ข้อมูลวิจัยและวิเคราะห์องค์ประกอบรวมถึงลักษณะของภัยคุกคามทางไซเบอร์ที่หลายองค์กรของประเทศไทยเจอนั้นยังคงเป็นภัยคุกคามที่ไม่รุนแรงนัก ถึงแม้จะมีเพิ่มมากขึ้นทุกวันแต่หน่วยงานภาครัฐก็สามารถรับมือได้ เพราะปฏิบัติตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ระเบียบ วิธีปฏิบัติ และมาตรการต่างๆที่เกี่ยวข้องจากภาครัฐ รวมถึงการบริหารจัดการด้วยนโยบายและแนวปฏิบัติของแต่องค์กรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทำให้แต่ละองค์กรทั้งภาคสาธารณสุข ภาคสาธารณูปโภคและภาคการเงินการธนาคาร ได้รับผลกระทบเมื่อวัดระดับตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 จึงอยู่ในระดับไม่ร้ายแรง

4.3 โครงสร้างการกำกับดูแล การขับเคลื่อนนโยบายและมาตรการรักษาความปลอดภัยทางไซเบอร์ในการบริหารจัดการขององค์กร

4.3.1 โครงสร้างการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีผลใช้บังคับเมื่อวันที่ 28 พฤษภาคม 2562 โดยมีวัตถุประสงค์เพื่อกำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานภาครัฐและภาคเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อ

ความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ โดยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ประกอบด้วยคณะกรรมการ 2 ส่วน คือ

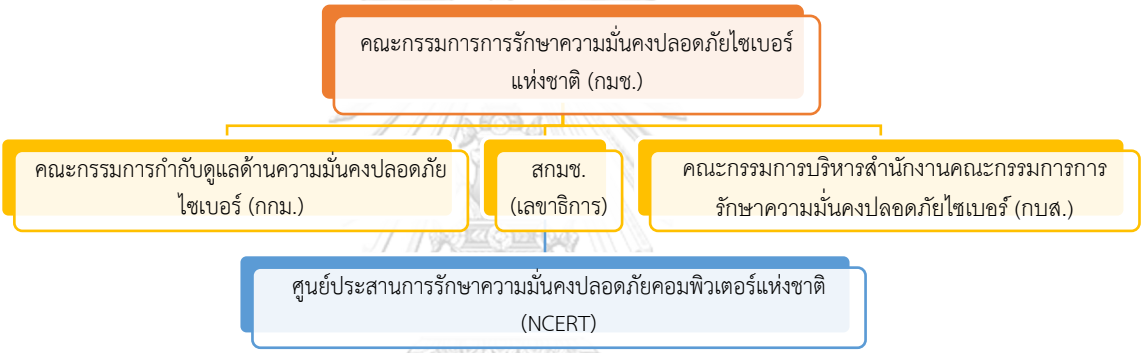
ส่วนที่ 1 มาตรา 9 กำหนดให้มี คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ กมช. ซึ่งมีนายกรัฐมนตรีเป็นประธานกรรมการ มีหน้าที่เสนอนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ กำหนดนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ (CII) จัดทำแผนปฏิบัติการ กำหนดมาตรฐาน มาตรการและแนวทางในการส่งเสริมพัฒนาระบบการให้บริการและยกระดับความรู้ความเชี่ยวชาญในการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงาน เจ้าหน้าที่หน่วยงาน CII หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชน รวมทั้งกำหนดกรอบการประสานงานความร่วมมืออื่นทั้งในประเทศและต่างประเทศ ติดตามประเมินผล และจัดทำรายงานสรุปผลการดำเนินงานตามนโยบายแลแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ 2 มาตรา 12 กำหนดให้มี คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ หรือ กกม. โดยมีรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นประธานกรรมการ มีหน้าที่ติดตามการดำเนินงานตามนโยบายและแผน ดูแลและดำเนินการรับมือภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กำกับดูแลการดำเนินงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ กำหนดแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและประสานเมื่อเผชิญเหตุได้แก่ ความมั่นคงของรัฐ บริการภาครัฐที่สำคัญ การเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม การขนส่งและโลจิสติกส์ พลังงานและสาธารณูปโภค สาธารณสุข และด้านอื่นๆ ตามที่บอร์ดกำหนดเพิ่มเติม รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือเมื่อมีเหตุภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบร้ายแรงต่อระบบสารสนเทศของประเทศ

นอกจากนี้ ตาม พ.ร.บ. ไซเบอร์ มาตรา 20 ได้กำหนดให้มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือเป็นที่รู้จักกันดีในชื่อย่อ “สกมช.” ให้เป็นหน่วยงานรัฐในฐานะนิติบุคคล ที่ไม่เป็นส่วนราชการหรือรัฐวิสาหกิจตามกฎหมาย และมาตรา 22 มีหน้าที่รับผิดชอบงานธุรการ วิชาการ การประชุม และเลขานุการของคณะกรรมการ กมช. และ กกม. และทำหน้าที่เสนอและสนับสนุนการจัดทำนโยบาย จัดทำประมวลแนวทางปฏิบัติและกรอบ

มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ประสานงานและให้ความร่วมมือในการตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ในประเทศและต่างประเทศ

ในส่วนของการบริหารงานทั่วไปของ สกมช. กำหนดให้มีคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.) ดูแลงานด้านกิจการบริหารงานทั่วไปของสำนักงานตาม มาตรา 25 รวมทั้งให้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานรับผิดชอบงานตามพระราชบัญญัติ และประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์ที่เป็นภัยต่อความมั่นคงอย่างร้ายแรง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ



ภาพที่ 12 แสดงโครงสร้างสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) (ข้อมูลจากการสัมภาษณ์)

ทั้งนี้ ตามโครงสร้างของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ได้แบ่งลักษณะหน่วยงานเป็น 2 ลักษณะใหญ่ๆ และกำหนดภารกิจที่สำคัญไว้ ดังนี้

1. หน่วยงานควบคุมหรือกำกับดูแล (Regulator) มีหน้าที่ประมวลแนวทางปฏิบัติหรือตรวจสอบการปฏิบัติงานตรวจสอบขั้นต่ำ สั่งแก้ไข จะสนับสนุนด้วย หน่วยงานเฝ้าระวัง ติดตามตรวจสอบ เผชิญเหตุ เช่น สำนักงานตำรวจแห่งชาติ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) กระทรวงมหาดไทย สำนักงานสภาความมั่นคงแห่งชาติ กระทรวงสาธารณสุข โดยจัดทำและรายงานสรุปจำนวนเหตุภัยคุกคามทางไซเบอร์ทั้งหมดที่เกิดขึ้นกับข้อมูลหรือระบบสารสนเทศของหน่วยงาน

ของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้การควบคุมหรือกำกับดูแลของตนในแต่ละปี ภายในวันที่ 31 มกราคม ของปีถัดไป ให้แก่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งการแจ้ง การรายงาน และการรายงานสรุปจะทำในรูปแบบของหนังสือหรือโดยวิธีการทางอิเล็กทรอนิกส์ก็ได้

2. หน่วยงานที่เป็นฝ่ายปฏิบัติ (Operator) มีภารกิจหรือให้บริการในด้านต่างๆเข้าลักษณะเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือลักษณะเฉพาะด้านที่ถือเป็นบริการสำคัญของชาติ หรือเกิดขึ้นตามนโยบายของรัฐและเป็นภารกิจหรือบริการหลักของหน่วยงานนั้นๆ มีหน้าที่กำหนดแผนรับมือตามมาตรฐาน COBIT หรือ ISO/IEC 27001 ให้กับหน่วยงานของตน ประเมินความเสี่ยงหรือตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง หน่วยงานตรวจประเมินความเสี่ยงระบบ (Audit) ประมวลแนวทางปฏิบัติ เช่น หน่วยงานที่มีการให้บริการด้านไฟฟ้า หน่วยงานที่ให้บริการด้านประปา หน่วยงานที่มีการให้บริการสุขภาพในโรงพยาบาล โดยอยู่ภายใต้การควบคุมหรือกำกับดูแลของหน่วยงานที่เป็น Regulator ที่ได้รับมอบหมาย ซึ่งกรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องพิจารณาส่งข้อมูลสำคัญที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับนโยบายการรักษาความลับของหน่วยงานด้วย และต้องปรับปรุงข้อมูลในรายงานเหตุภัยคุกคามทางไซเบอร์และสถานะการตอบสนองภัยคุกคามทางไซเบอร์ให้สอดคล้องกับข้อมูลอันเป็นปัจจุบันที่หน่วยงานได้สืบทราบเพิ่มมากขึ้นในระหว่างการ ดำเนินการรับมือเหตุภัยคุกคาม รวมทั้งจัดส่งรายงานปิดเหตุการณ์ภัยคุกคามดังกล่าวด้วย นอกจากนี้ ให้จัดทำและส่งรายงานเหตุภัยคุกคามทางไซเบอร์นั้นไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติภายในระยะเวลา 24 ชั่วโมงหลังจากการตรวจพบหรือเกิดเหตุภัยคุกคามทางไซเบอร์ดังกล่าวแล้ว พร้อมทั้งส่งรายงานไปยังหน่วยงานควบคุมหรือกำกับดูแลของตนภายในเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด

ภาพที่ 13 กลไกการบริหารจัดการด้านไซเบอร์ตาม พ.ร.บ.ไซเบอร์ พ.ศ.2562

ที่มา: ThaiCERT by NCSA Thailand (2023)

ข้อมูลจากการสัมภาษณ์สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ สกมช. ดังภาพที่ 13 แสดงกลไกในการบริหารจัดการและการประสานความร่วมมือกันระหว่างหน่วยงานโครงสร้างการกำกับดูแลด้านไซเบอร์ตาม พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ดังที่กล่าวมาแล้วในข้างต้น และตามประกาศคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแลนั้น ได้กำหนดหลักเกณฑ์ประกอบการพิจารณาว่าด้วยกรณีลักษณะหน่วยงานที่มีภารกิจหรือให้บริการให้อยู่ภายใต้หน่วยงานควบคุมหรือกำกับดูแลในแต่ละด้านพิจารณาตามความเหมาะสมในการกำหนดแนวทาง และให้แจ้งต่อ สกมช. เพื่อทราบต่อไป จากหลักเกณฑ์ดังกล่าวส่งผลให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสาธารณูปโภค เช่น การไฟฟ้าและการประปา พิจารณานำไปปรับใช้ให้เหมาะสมกับบริบทและภารกิจขององค์กร หลายหน่วยงานได้ปรับปรุงหรือมีแนวทางในการปรับปรุงโครงสร้างองค์กรด้านไอที ซึ่งสอดคล้องกับผู้ให้ข้อมูลสำคัญ ดังนี้

“กปภ. มีการปรับโครงสร้างในปีงบประมาณ 2566 โดยแยกจากเดิมเป็นกองคอมพิวเตอร์และเครือข่าย เราแยกระบบเครือข่ายออกมาและเพิ่มงานเฝ้าระวังและควบคุมความปลอดภัย เพื่อให้เกิดความชัดเจนยิ่งขึ้น”

(ผู้ให้ข้อมูลสำคัญที่ 2, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

“มีการบริหารภายในคือมีการจัดทำ BCM องค์กรก่อนมีสถานการณ์โควิด จึงมีการปรับโครงสร้างเพื่อรับมือ เพราะฉะนั้น BCM ขององค์กรก็จะมาจาก Value Chain แล้วหน่วยงานเราในฐานะสนับสนุนงานไอทีเพื่อให้กระบวนการต่างๆที่เป็นเป้าประสงค์ของ BCM สอดคล้องเป็นไปตามที่เค้ากำหนด และรับมาดำเนินการโครงการต่างๆที่เกี่ยวข้อง เราจึงต้องมาดำเนินการทำค่าอะไรต่างๆให้มีความยืดหยุ่นแล้วก็น้อยกว่าที่ควรจะเป็น แล้วก็ทำแผนฝึกซ้อม แผน BCP เพื่อที่จะ response ว่าทีมที่จะเข้าไปเทสตรงนี้จะใช้เวลาเท่าไหร่เพื่อทำการกู้คืนและมีกระบวนการที่จะ response และกระบวนการที่จะให้การสื่อสารให้กับพนักงานและผู้ที่เกี่ยวข้องว่าเป็นอย่างไร และก็จะมีการประกาศผู้ที่ให้ข้อมูลที่เดียวที่เป็น center”

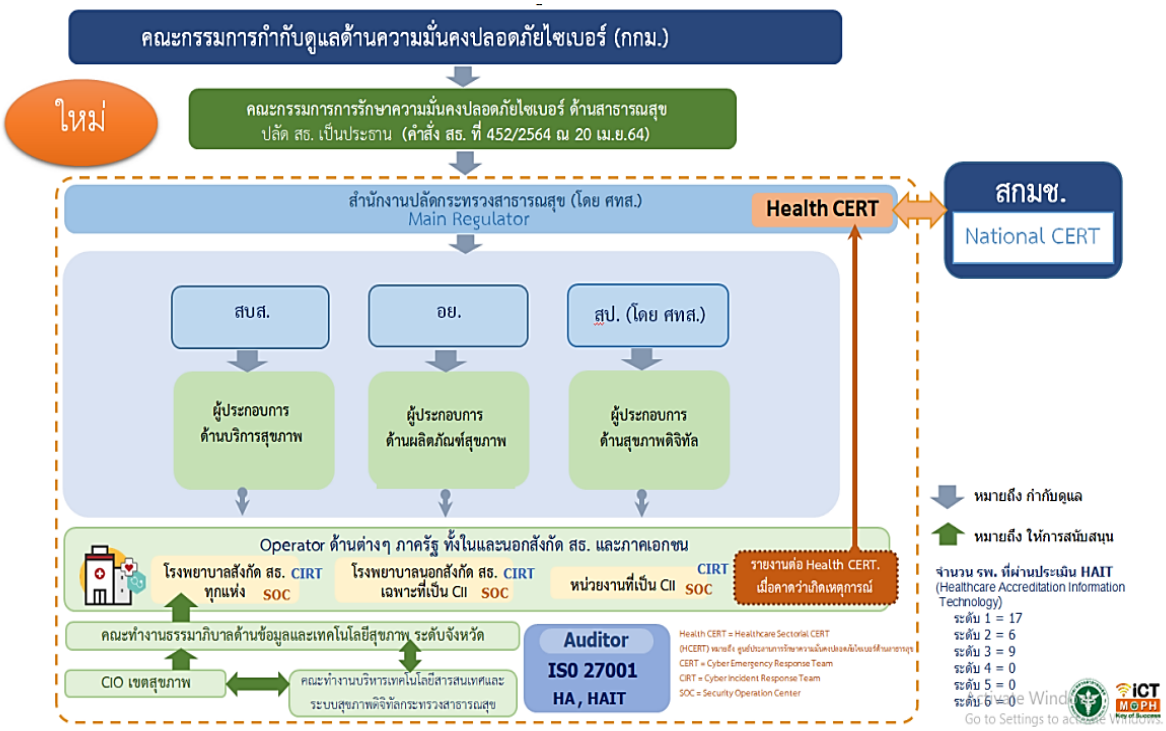
(ผู้ให้ข้อมูลสำคัญที่ 3, สัมภาษณ์เมื่อวันที่ 19 มีนาคม 2566)

“เรามีหน่วยงานยุทธศาสตร์ดิจิทัล คือเราเอายุทธศาสตร์มาวางกลยุทธ์ทางด้านดิจิทัลรวมถึงวิธีการปฏิบัติ และแยกอยู่กับทางหน่วยงานด้านไอที และขึ้นอยู่ภายใต้ ผู้ว่าการโดยตรง แต่จะมีแนวโน้มการปรับโครงสร้างใหม่ในปีหน้าซึ่งอาจมีการปรับให้ขึ้นตรงกับสายงานด้านไอทีโดยเฉพาะ”

(ผู้ให้ข้อมูลสำคัญที่ 4, สัมภาษณ์เมื่อวันที่ 31 มีนาคม 2566)

ในขณะที่ หน่วยงานด้านสาธารณสุขได้มีการแต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุขที่มีการบูรณาการเชื่อมโยงระหว่างคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์แห่งชาติ (NCERT) ภายใต้สังกัด สกมช. เพื่อให้สอดคล้องกับ พ.ร.บ. การรักษาความ

มั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และให้ครอบคลุมกับโครงสร้างองค์กรที่มีหน่วยงานภายใต้สังกัดสำนักงานปลัดกระทรวงสาธารณสุขทั่วประเทศ โดยแสดงให้เห็นดังภาพที่ 14 จากผู้ให้ข้อมูลสำคัญคนที่ 7 ดังนี้



ภาพที่ 14 โครงสร้างการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ของกระทรวงสาธารณสุข (ข้อมูลจากการสัมภาษณ์)

4.3.2 การขับเคลื่อนนโยบายและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์

การส่งเสริมนโยบายและมาตรการรักษาความปลอดภัยทางไซเบอร์ เป็นการใช้กลยุทธ์และการดำเนินการเพื่อป้องกันภัยคุกคามและการโจมตีทางไซเบอร์ ซึ่งรวมถึงการพัฒนานโยบาย ขั้นตอน และแนวปฏิบัติสำหรับการปกป้องข้อมูลที่ละเอียดอ่อนและโครงสร้างพื้นฐานที่สำคัญ ตลอดจนการให้ความรู้แก่พนักงานและผู้ใช้เกี่ยวกับแนวปฏิบัติที่ดีที่สุดสำหรับการใช้คอมพิวเตอร์อย่างปลอดภัย นอกจากนี้ การส่งเสริมมาตรการรักษาความปลอดภัยทางไซเบอร์ในทางเทคนิค เช่น ไฟร์วอลล์ ระบบตรวจจับการบุกรุก และการเข้ารหัสเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตและป้องกันการรั่วไหลของข้อมูล เป้าหมายของการส่งเสริมนโยบายและมาตรการรักษาความปลอดภัยทางไซเบอร์ คือ เพื่อให้มั่นใจถึงการรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งานของข้อมูลและระบบ ขณะเดียวกันก็ลดความ

เสี่ยงจากการโจมตีทางไซเบอร์และลดผลกระทบจากเหตุการณ์ที่เกิดขึ้น อนึ่ง ผู้ให้ข้อมูลสำคัญได้ให้ข้อมูลในประเด็นของสถานการณ์ภัยคุกคามทางไซเบอร์ไว้ ดังนี้

4.3.2.1 ความสอดคล้องของกฎหมายและนโยบายกับบริบทขององค์กร

การนำกฎหมายและนโยบายภาครัฐมาใช้ในการกำหนดนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ให้เหมาะสมกับบริบทขององค์กร ตรงตามวัตถุประสงค์และเป้าหมายขององค์กรนั้นๆ เช่น พ.ร.บ.รักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 รวมทั้งนโยบายและกฎหมายที่มีประสิทธิภาพควรปรับให้เหมาะกับพันธกิจ วัฒนธรรม และค่านิยมขององค์กร ในขณะเดียวกันต้องเป็นไปตามมาตรฐานทางกฎหมายและจริยธรรม เพื่อให้มั่นใจว่าพนักงานและผู้มีส่วนได้ส่วนเสียเข้าใจและสามารถนำไปปฏิบัติตามกฎระเบียบดังกล่าวแล้วจะส่งผลให้องค์กรมีประสิทธิภาพและประสิทธิผลมากขึ้น ซึ่งสอดคล้องกับผู้ให้ข้อมูลสำคัญด้านหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศที่แสดงให้เห็นในทิศทางที่คล้ายคลึงกัน ดังนี้

> *“เราไม่มีทางด้านกฎหมายที่ดูแลด้านรักษาความมั่นคงปลอดภัยไซเบอร์โดยตรง เพียงแต่ว่าเรามีกองนิติการที่ดูทางด้านกฎหมายทั่วไป โดยปกติคือเราจะมีการขอความร่วมมือ เป็นการจัดทำบันทึกข้อตกลงหรือ MOU ร่วมกันภายในระหว่างคอมพิวเตอร์เครือข่ายและกองนิติการเพื่อให้ทางกองนิติการแจ้งเกี่ยวกับกฎหมายที่มีมาใหม่ในแต่ละช่วงเวลาให้ทางเรารับทราบ ว่าตอนนี้มีกฎหมายอะไรบ้างและกฎหมายนั้นมีมาตราอะไรมีแนวทางปฏิบัติยังไงเพื่อจะได้ให้ทางเราสามารถที่จะดำเนินการได้อย่างถูกต้อง โดย พ.ร.บ.ไซเบอร์ 2562 ในเรื่องของมาตรา 43 ที่ออกมาทางการประปาส่วนภูมิภาคได้ดำเนินการตามมาตราที่ที่ได้มีกำหนดเอาไว้ ไม่ว่าจะเป็นกฎหมายที่เป็นกฎหมายหลัก และกฎหมายที่ออกมาล่าสุดก็คือกฎหมายลำดับรอง ประปาก็คือได้ดำเนินการในส่วนนั้นได้อย่างครบถ้วน เนื่องจากว่าเราจะต้องมีการประเมิน จากผู้ตรวจสอบภายนอกคือ มีผู้ตรวจสอบภายนอกเข้ามาตรวจว่าได้ดำเนินการตามพระราชบัญญัติ พ.ร.บ.ไซเบอร์ และมีการดำเนินการตามมาตราต่างๆ ใช้เวลาในการตรวจประมาณ 4-5 วัน ในลักษณะเข้ามาตรวจว่าทางองค์กรได้ดำเนินการได้ครบถ้วนหรือไม่ โดยมีเอกสารกลับมายืนยันว่าองค์กรได้รับ*

ตรวจสอบเรียบร้อยแล้ว ในการตรวจที่เรียกว่า critical service คือ ตรวจว่าตอนนี้ระบบที่สำคัญของการประปามีระบบไหนบ้าง มีการตรวจในส่วนงานที่เกี่ยวข้องทั้งหมด ตรงส่วนนี้เราก็จะมีเอกสารที่ทาง external audit ได้มีการประเมินแล้วส่งผลมาให้เราเป็นลักษณะของ hard copy และ soft copy ที่เป็นทางการ เมื่อเกิดเหตุการณ์โจมตีกับการประปาส่วนภูมิภาค จะมีการที่ขอความร่วมมือการฝึกอบรมหรือการปฏิบัติการ โดยการทดสอบหรือจัดทำแผนการรับมือ และจะต้องดำเนินการแจ้งทั้งหน่วยงานควบคุมดูแลหรือ regulator นั่นคือ กระทรวงมหาดไทย และแจ้งทาง สกมช. ด้วยเช่นเดียวกัน หมายความว่าจะต้องแจ้งทั้ง 2 หน่วยงานดังกล่าวรับทราบ แล้วทางกระทรวงมหาดไทยก็จะนำข้อมูลของเราทำการรวบรวม รวมถึงหน่วยงานที่อยู่ในสังกัดของมหาดไทย เพื่อส่งให้ทาง สกมช. รับทราบทุกครั้ง”

(ผู้ให้ข้อมูลสำคัญที่ 2, สัมภาษณ์เมื่อวันที่ 19 มีนาคม 2566)

“มีหน่วยงานด้านกฎหมาย แต่ในด้านการกำกับดูแล ยังมีปัญหาด้านการขับเคลื่อนด้าน PDPA ระหว่างกฎหมายและไอที ซึ่งไม่มีความชัดเจนในการรับภาระงาน และกปน. มีการแก้ปัญหาโดยตั้งคณะทำงาน DPO และมีคณะทำงาน working group มีประธานเป็นฝ่ายกฎหมายและมีไอทีเป็นเลขานุการ ซึ่งเดิมเรามีแผนที่ยังไม่สอดคล้องกับ พ.ร.บ. แต่จะมีการประชุมเพื่อจะพยายามให้สอดคล้องกับ พ.ร.บ.ไซเบอร์ 2562 และเรากำลังดำเนินการเกี่ยวกับเรื่องด้านระบบผลิต มีแผนที่จะปรับปรุงประสิทธิภาพด้าน security by decide ด้วยเช่นเดียวกันทั้งการสร้างนโยบายและวิธีแนวปฏิบัติ เราจึงได้ทำการ literature review มาจัดทำ model ที่เป็น standard ขององค์กร”

(ผู้ให้ข้อมูลสำคัญที่ 3, สัมภาษณ์เมื่อวันที่ 30 มีนาคม 2566)

“ในหน่วยงานด้านกฎหมายนอกจากดูกฎหมายทั่วไปแล้ว ก็มีเริ่มศึกษา พ.ร.บ.ไซเบอร์ พ.ร.บ. PDPA ซึ่งเราแยกออกเป็น กฎหมายหลัก กฎหมายรอง เรามีหน่วยงานที่เป็น Internal Audit ตรวจสอบภายใน เรียกว่า กองตรวจสอบระบบสารสนเทศ และหน่วยงานด้าน IT

เป็นผู้ Implementer ส่วนใหญ่ กฎหมายสองตัวที่ออกมาที่มี impact มากก็คือ พ.ร.บ ไซเบอร์ กับ พ.ร.บ. PDPA ซึ่งเราจะมีการแบ่งการทำงานกันชัดเจน ถ้ากรณีเกิดเหตุและต้องไปแจ้งความหรือการดำเนินคดี ทางหน่วยงานด้านกฎหมายจะเป็นผู้ดำเนินการ ซึ่ง กฟภ. จะมีการทำงานที่บูรณาการกัน เรามีหน่วยงาน DPO มีการจัดตั้งทีมงาน DPO ตามโครงสร้างด้านกฎหมายและยุทธศาตสตร์เป็นหลัก ซึ่งมีไอทีจะช่วยในด้าน support ทางเทคนิค ในด้านนโยบาย เรามีการจัดทำตามนโยบายมานานตั้งแต่ พรก.ว่าด้วยวิธีความมั่นคงปลอดภัยปี 2555 และวิเคราะห์ เพื่อมาดำเนินการ ออกนโยบาย ออกระเบียบ ออกแนวปฏิบัติ แต่เมื่อมี พรบ ไซเบอร์ออกมาแล้วมีการบังคับใช้ เราเองก็นำระเบียบและแนวปฏิบัติที่มีอยู่มา alignment กันว่าสิ่งที่เราทำไปแล้วว่าอะไรที่สอดคล้องกับ พ.ร.บ ไซเบอร์ ก็จะคงไว้ ซึ่งนโยบายจะเหมือนเดิม แต่มีการปรับปรุงแก้ไขแนวปฏิบัติ”

(ผู้ให้ข้อมูลสำคัญที่ 4, สัมภาษณ์เมื่อวันที่ 31 มีนาคม 2566)

“เรามีคณะทำงานธรรมาภิบาลด้านข้อมูลและเทคโนโลยีสุขภาพระดับจังหวัด ได้นำนโยบายจากส่วนกลางไปสู่การปฏิบัติและกำกับติดตามการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ หรือ Cybersecurity โดยมีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข พ.ศ. 2565 ภายใต้กฎหมายที่เกี่ยวข้อง และมีการบริหารจัดการข้อมูลส่วนบุคคลให้สอดคล้องกับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 หรือ PDPA มีการรับส่งข้อมูลตามมาตรฐานที่ตกลงร่วมกันและนำข้อมูลสุขภาพไปใช้ประโยชน์ในการให้บริการแก่ประชาชนอย่างมีธรรมาภิบาลข้อมูล หรือ Data Governance ให้สอดคล้องกับแนวทางส่วนกลาง อ้างอิงตาม พ.ร.บ.ว่าด้วนธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544”

(ผู้ให้ข้อมูลสำคัญที่ 7, สัมภาษณ์เมื่อวันที่ 26 พฤษภา 2566)

ในขณะที่ ผู้ให้ข้อมูลสำคัญจากหน่วยงานภาคการเงินการธนาคาร มีวิธีการในการนำกฎหมายและนโยบายภาครัฐมาปรับใช้กับบริบทขององค์กรที่แตกต่างไป เนื่องด้วยมีภารกิจการจัดการด้านการเงินเป็นหลัก ได้แสดงทรรศนะไว้ดังนี้

"เรามีคณะทำงานความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งไซเบอร์เป็นส่วนหนึ่งของเทคโนโลยีด้านความเสี่ยง เรามีคณะกรรมการกำกับด้านความเสี่ยง ในส่วนของด้านไอทีคือ first line จะมีคณะกรรมการคอมพิวเตอร์ ซึ่งมีผู้ว่าการเป็นประธาน มี second line อยู่ในด้านความเสี่ยงภาพรวมเข้ามาร่วมกับฝ่ายกฎหมาย ในแง่ของ compliance แล้ว ธปท. เองจะดูว่ามีกฎหมายอะไรที่เราต้องปฏิบัติตามบ้าง แล้วตรง Third line ที่เป็น Audit ภายใน เค้าก็จะตรวจสอบตาม พ.ร.บ ไซเบอร์ ด้วยว่าให้มีการตรวจสอบ ก็จะมี third line เข้ามาตรวจสอบ และดูแลให้เป็นไปตามกฎหมาย กฎหมายก็จะทำหน้าที่ Internet first ให้สอบทานประเด็นกฎหมายที่ให้ความชัดเจน ในแง่ของนโยบาย มีคณะกรรมการระดับบอร์ดที่เป็นบุคคลภายนอกเป็นกรรมการกำกับดูแล และดูเรื่อง พ.ร.บ. ไซเบอร์ เรามีนโยบายด้านไอที มีนโยบายด้านไซเบอร์ ในการปฏิบัติงานต่างๆเราก็มีระเบียบวิธีปฏิบัติต่างๆ เป็นเรื่องๆไป ในแง่ของมาตรฐานเองเราก็ดูแลระบบงานสำคัญของประเทศ ระบบพวกนี้เราก็จะมีการบริหารด้วย ISO27001 ส่วนเรื่องของการแก้ไขปัญหาของสถานการณ์ภัยคุกคาม เราจะมีแผนเรียกว่า CSIRP แผนของ ธปท. เป็นแผนเพื่อตอบสนองเวลาเกิดเหตุภัยไซเบอร์ ซักซ้อมให้กับบุคลากรในองค์กร"

(ผู้ให้ข้อมูลสำคัญที่ 5, สัมภาษณ์เมื่อวันที่ 26 เมษายน 2566)

"มีนิติการรับผิดชอบ เมื่อมีประกาศหรือระเบียบคำสั่งใดๆ ด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สอดคล้องกับ พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ หรือกฎหมายรองต่างๆ ทางนิติการจะเป็นคนมาตีความ และมาตรวจสอบก่อนที่จะมีประกาศออกไปภายในหน่วยงาน และมีความสอดคล้องในด้านนโยบายองค์กร เพราะเรานำกรอบของ พ.ร.บ.ไซเบอร์ รวมทั้งกฎหมายหลักและกฎหมายรอง และข้อกำหนดของทางแบงค์ชาติเอง มาเป็นแนวทางในการจัดเตรียม

ระเบียบ คำสั่ง ประกาศ และคู่มือปฏิบัติงานต่างๆ นอกจากนี้โดยปกติเราเป็นหนึ่งในสมาชิกของ TB-CERT คือ ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคธนาคาร โดยหน้าที่หลักๆ ก็คือเกิดขึ้นมาเพื่อเตรียมพร้อมรับมือกับภัยคุกคามไซเบอร์ทางการเงิน ซึ่งจะมีการประชุมกันระหว่างสมาชิกอย่างน้อยเดือนละ 1 ครั้ง ในส่วนของ สกมช. เมื่อมีการจัดประชุม สัมมนา หรือ event ต่างๆ ทางเราก็จะเข้าร่วมกับทาง สกมช. อยู่เสมอ ซึ่งไม่ได้นับว่าเป็นปีละ 1 ครั้งหรือไม่ โดยเราจะส่งตัวแทนเข้าไปมีส่วนร่วม เมื่อเค้ามีการจัดในเรื่องของการทดสอบในระดับประเทศ เราก็เข้าร่วมกับเค้าด้วยเช่นกัน อย่างในปีนี้ด้วยเช่นกัน เค้ามีการจัดทำเกี่ยวกับเรื่องของแผนการดำเนินการซ้อมแผนไซเบอร์ประจำปี ทางเราก็เข้าร่วม"

(ผู้ให้ข้อมูลสำคัญที่ 6, สัมภาษณ์เมื่อวันที่ 28 เมษายน 2566)

นอกจากนี้ ในส่วนของหน่วยงานด้านการกำกับดูแลจากภาครัฐเอง มีความพยายามที่จะนำ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 และกฎหมายอื่นๆมาปรับใช้กับภารกิจและบริบทขององค์กร เพื่อให้เป็นไปตามมาตรฐานการควบคุมดูแลหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ โดยสอดคล้องกับผู้ให้ข้อมูลสำคัญ ดังนี้

"สพร. มีคณะทำงาน DPO อยู่กับฝ่ายมาตรฐานที่ไม่ใช่ไอทีและกฎหมาย และเนื่องจาก สพร. เป็นหน่วยงานกำกับดูแลหรือ regulator เรามี DPO เป็นคณะทำงานในการออกระเบียบบอกมาตรฐานเพื่อสามารถนำมาบังคับใช้ในการดำเนินงานตาม พ.ร.บ. ไซเบอร์ ในเรื่องของ cybersecurity สพร. มีการออกนโยบาย cyber security policy ซึ่งเป็นไปตาม พ.ร.บ. ไซเบอร์และ พ.ร.บ.PDPA จริงๆตั้งแต่ พ.ร.บ.คอมพิวเตอร์ปี 2560 เพราะว่าสุดท้ายแล้วสิ่งที่เราทำคือ เราต้องการ Certify ISO27001 ด้วย ซึ่ง พ.ร.บ ไซเบอร์ส่วนหนึ่งในการประกาศ ก็ถอดออกมาเป็นตัว cyber security policy ภายในองค์กรด้วย มีการออก policy ให้เป็นไปตาม พ.ร.บ. คอมพิวเตอร์ พ.ร.บ.ไซเบอร์ พ.ร.บ.PDPA และ compile ตามกฎหมายต่างๆ นอกจากนี้ ตาม พ.ร.บ.ไซเบอร์ สพร. เป็น regulator

ใน sector ที่ 2 คือการบริการภาครัฐที่สำคัญ ให้ 2 หน่วยงาน คือ สำนักงานตรวจคนเข้าเมือง และกรมป้องกันและบรรเทาสาธารณะภัย และมี 4 service ซึ่ง 2 บริการเป็นของ DGA คือ Digital ID หรือการยืนยันตัวตนออนไลน์ และ Government Data Exchange ในส่วนที่เหลือก็จะเป็นทางด้านของสำนักงานตรวจคนเข้าเมือง และกรมป้องกันและบรรเทาสาธารณะภัย"

(ผู้ให้ข้อมูลสำคัญที่ 9, สัมภาษณ์เมื่อวันที่ 30 มีนาคม 2566)

"เรื่องการป้องกันไม่ใช่หน้าที่ของไอทีด้านเดียว เพราะไอทีจะไม่เข้าใจเรื่องของข้อมูลและความเสี่ยงจริงๆ มองว่าทุกฝ่ายมีส่วนเกี่ยวข้องโดยเฉพาะเจ้าของข้อมูล ส่วน DPO ก็ยังไม่มีความชัดเจนว่าต้องเป็นหน่วยงานด้านกฎหมายหรือไอที ในส่วนของนโยบาย ภาครัฐจะต้องทำนโยบายและแนวปฏิบัติที่เกี่ยวกับไซเบอร์ security ก่อนคือขั้นพื้นฐาน แต่หลายหน่วยงานก็ยังมีช่องโหว่อยู่ และไม่ได้ขับเคลื่อนสักเท่าไหร่ ทำเพื่อให้ถูกต้องตามกฎหมาย แต่ไม่ได้นำมาใช้"

(ผู้ให้ข้อมูลสำคัญที่ 10, สัมภาษณ์เมื่อวันที่ 27 มีนาคม 2566)

"พ.ร.บ. ไซเบอร์ สกมช. มอบให้ สมช. จะดูแลในส่วนของในระดับวิกฤต ซึ่งเรายังขาดในเรื่องของการเปลี่ยนผ่านการใช้กฎหมายระหว่างตัว พ.ร.บ. ไซเบอร์ มายังเป็น พ.ร.บ. สภา มช. เนื่องด้วยส่วนของกฎหมาย เราก็ยังๆมีการคุยกันอยู่ว่าเราควรจะทำยังไงหรือว่าต้องการรูปแบบในการเปลี่ยนผ่านประมาณไหน คือในเบื้องต้นถ้าเป็นในระบบของกฎหมาย สมช. อาจจะไม่ได้เป็นหน่วยงานหลักเพราะว่าเราอาจจะดูจำกัดในภาพรวมแล้วก็ส่วนของนโยบายและการใช้กฎหมายต่างๆ แต่ถ้าเป็นกฎหมายในเรื่องอื่น เช่น พ.ร.บ. คอมพิวเตอร์ หรืออาจจะเป็นในเรื่องของอาชญากรรมที่เกี่ยวกับตำรวจ สมช. มีส่วนร่วมในการดำเนินการร่วมกัน คือ ด้วยความที่เราเป็นหน่วยนโยบาย เราคงไม่สามารถที่จะไปดูรายละเอียดในแต่ละคดีได้ แต่ว่าเราสามารถที่จะทำงานร่วมกันแล้วก็ช่วยสนับสนุนว่าอะไรในกลไกทางกฎหมายที่หน่วยงานอื่นรับผิดชอบอยู่ ขาดเหลือหรือว่ามีช่องว่างตรงไหน ทาง

สมช. ก็จะช่วยอำนวยการให้ได้ ในส่วนขององค์กร เรามีกลุ่มงานด้านนิติกรที่ดูในเรื่องของกฎหมาย แต่ถ้าในส่วนของ พ.ร.บ. ไซเบอร์ ก็จะเป็นงานผมเองและมีบุคลากรที่จบด้านกฎหมายมาช่วยดู นอกจากนี้ภาครัฐจะต้องทำนโยบายและแนวปฏิบัติที่เกี่ยวกับไซเบอร์ security ก่อนคือขั้นพื้นฐาน แต่หลายหน่วยงานก็ยังมีช่องโหว่อยู่ และไม่ได้ขับเคลื่อนสักเท่าไหร่ ทำเพื่อให้ถูกต้องตามกฎหมาย แต่ไม่ได้นำมาใช้"

(ผู้ให้ข้อมูลสำคัญที่ 11, สัมภาษณ์เมื่อวันที่ 19 เมษายน 2566)

"ด้านกฎหมาย มี พ.ร.บ.ข้อมูลข่าวสารฯ 2540 มาบังคับใช้ก่อน แต่ในส่วนของ พ.ร.บ. ไซเบอร์ ยังไม่ครอบคลุมในการจัดการด้านป้องกันภัยไซเบอร์ มีให้อบรมให้ความรู้เรื่องการรักษาข้อมูลของหน่วยงานของตนเอง และใช้ พ.ร.บ.PDPA ใช้เบื้องต้นรวมถึง พ.ร.บ. คอมพิวเตอร์ 2550 มีการจัดทำแผนฉุกเฉินด้านอื่นๆ แต่ยังไม่มีแผนฉุกเฉินด้านภัยคุกคามไซเบอร์"

(ผู้ให้ข้อมูลสำคัญที่ 13, สัมภาษณ์เมื่อวันที่ 25 เมษายน 2566)

"มีนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ เพื่อเป็นส่วนหนึ่งของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ในการป้องกันภัยคุกคาม ลดความเสี่ยงจากช่องโหว่และผู้บุกรุก เพื่อให้สารสนเทศมีความปลอดภัย สามารถรักษาความลับและความถูกต้องของข้อมูล และมีความพร้อมในการให้บริการอยู่ในระดับที่ยอมรับได้ เราจึงได้กำหนดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อเป็นแนวทางเสริมสร้างความมั่นคงปลอดภัยด้านสารสนเทศให้กับสำนักงาน หรือหน่วยงานที่มีความเกี่ยวข้องในการปฏิบัติราชการกับสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยนโยบายนี้มีจุดประสงค์เพื่อการสนับสนุนการดำเนินการเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศของ สป.ดศ. โดยใช้แนวทางและกระบวนการโดยมีความสอดคล้องตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 รวมถึงกฎหมายและประกาศด้าน

เทคโนโลยีสารสนเทศอื่นๆ ที่เกี่ยวข้อง ได้แก่ พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นต้น ในเนื้อหาในเล่มนโยบายความมั่นคงปลอดภัยด้านสารสนเทศได้กำหนดองค์ประกอบที่สำคัญของการบริหารจัดการระบบเทคโนโลยีสารสนเทศให้มีความมั่นคงปลอดภัย โดยครอบคลุมทั้งด้านการควบคุมการเข้าถึง การกำหนดขั้นตอน และกระบวนการที่เหมาะสม ตามหลักมาตรฐานสากล ซึ่งมีองค์ประกอบ 14 หมวด ซึ่งได้กำหนดวัตถุประสงค์ในการดำเนินการที่เกี่ยวข้องในหมวดนั้นๆ มีรายละเอียดของมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และวิธีปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศเพื่อลดความเสียหายต่อการปฏิบัติงาน ให้เป็นหน่วยงานที่ได้รับการยอมรับจากองค์กรต่างๆ ในการปฏิบัติราชการได้อย่างมั่นคงปลอดภัยตามมาตรฐานสากล ซึ่งนโยบายความมั่นคงปลอดภัยด้านสารสนเทศนี้ถือเป็นมาตรฐานด้านความมั่นคงปลอดภัยซึ่งเจ้าหน้าที่ทุกระดับ รวมถึงบุคคลภายนอก และหน่วยงานภายนอกที่เข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรต้องรับทราบ เข้าถึง เข้าใจ และปฏิบัติตามแนวนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด ทั้งนี้ การปรับปรุงนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ จะดำเนินการปรับปรุงต่อเนื่องทุก 1 ปี ซึ่งจะนำเอานโยบาย กฎหมาย แผนปฏิบัติการ ระเบียบ ข้อบังคับ ภัยคุกคามทางไซเบอร์ที่เกิดขึ้น มาปรับปรุงแนวปฏิบัติฯ เพื่อให้เกิดความทันสมัย ครบถ้วน สอดคล้องกับการแก้ไขสถานการณ์ภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นในอนาคต”

(ผู้ให้ข้อมูลสำคัญที่ 14, สัมภาษณ์เมื่อวันที่ 18 เมษายน 2566)

“ตามประกาศคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2564 กำหนดให้สำนักงานตำรวจแห่งชาติเป็นหน่วยงานควบคุมหรือกำกับดูแล (Regulator) ในหมวด 1 ด้านความมั่นคงของรัฐ ลักษณะหน่วยงาน ข้อ 2 ที่มีภารกิจเกี่ยวข้องกับการบังคับใช้

กฎหมาย โดยมีภารกิจหรือการให้บริการ (Critical Services) ด้านการบังคับใช้กฎหมายและอำนวยความยุติธรรมทางอาญา และหมวด 5 ด้านการขนส่งและโลจิสติกส์ ลักษณะหน่วยงาน ข้อ 1 การให้บริการขนส่งทางบก โดยมีภารกิจหรือการให้บริการเกี่ยวกับการควบคุมการจราจรในพื้นที่กรุงเทพมหานคร โดยให้สำนักงานตำรวจแห่งชาติกำหนดแนวทางพิจารณาภารกิจหรือบริการของหน่วยงานที่อยู่ภายใต้การดูแลเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ"

(ผู้ให้ข้อมูลสำคัญที่ 18, สัมภาษณ์เมื่อวันที่ 28 เมษายน 2566)

ในขณะที่ผู้เชี่ยวชาญ ได้แสดงความคิดเห็นในเรื่องนี้ไว้เช่นเดียวกัน สอดคล้องกับผู้ให้ข้อมูลสำคัญคนที่ 19 และ ผู้ให้ข้อมูลสำคัญคนที่ 20 ดังนี้

"หน่วยงานด้านกฎหมายต้องขึ้นอยู่กับผู้บริหารองค์กรว่าเห็นความสำคัญของ DPO มากน้อยแค่ไหน แต่ในมุมมองของผมคือสำคัญมาก และอาจจะต้องมีการปรับโครงสร้างอะไรมากมาย ซึ่งปัจจุบันหลายองค์กรมองว่าต้องมีผู้บริหารระดับสูงด้านไซเบอร์เพิ่มเติม เช่น CSO มาจาก Chief Security Officer เพราะมีความสำคัญ"

(ผู้ให้ข้อมูลสำคัญที่ 19, สัมภาษณ์เมื่อวันที่ 19 มีนาคม 2566)

"อาจารย์เห็นว่าการออกกฎหมายถือว่าสอดคล้องและครอบคลุม แต่ในการขับเคลื่อนอาจต้องใช้เวลาเนื่องด้วยหน่วยงานภาครัฐต้องค่อยๆปฏิบัติตามและทำความเข้าใจให้ถี่ถ้วน เช่น เรื่องงบประมาณ การวางแผน การลงมือทำ ซึ่งปัจจุบันองค์กรยังปฏิบัติได้ไม่ครบถ้วนในสิ่งที่ควรปฏิบัติ ดังนั้น การวิเคราะห์สภาพปัจจุบัน หรือ As Is ด้าน Infrastructure ของเรายังมีช่องโหว่และจุดอ่อน ซึ่งแต่ละองค์กรยังไม่ทราบว่าโดนโจมตีหรือถูกแฮกมากน้อยแค่ไหน เพราะผู้โจมตีมีความรู้ความสามารถรอบด้าน แต่ก็ถือว่าเรามีกรอบในระดับประเทศที่ครอบคลุม และควรดำเนินการดังนี้ 1. หน่วยงานของภาครัฐควรปฏิบัติตาม พ.ร.บ. ของภาครัฐ คือ พ.ร.บ.ไซเบอร์ 2562 พ.ร.บ.คุ้มครองส่วนบุคคล 2562 พ.ร.บ.บริหารงานการให้บริการภาครัฐ 2562 และหน่วยงานภาครัฐจะต้องให้บริการด้าน digital

platform รวมถึงการบริการหลังบ้านต้องดำเนินงานตามกฎหมาย 2. ควรมีการกำหนดนโยบายและประกาศนโยบายทางไซเบอร์ขององค์กรให้ชัดเจน โดยเฉพาะด้าน Cybersecurity นอกจากจะต้องออกนโยบายแล้วต้องมีคู่มือแนวปฏิบัติด้วย ยกตัวอย่างเช่น คู่มือปฏิบัติ Save Internet Usages ว่าจะใช้ Internet อย่างไรถึงจะปลอดภัย เช่น จะกำหนดพาสเวิร์ดยังไงถึงจะปลอดภัย หรือใช้คอมพิวเตอร์แล้วจะลุกไปห้องน้ำหรือทำอย่างอื่น ต้อง log off หรือ ทำ screen sleep ก็เป็นแนวปฏิบัติในระดับบุคคล แนวปฏิบัติในระดับองค์กร ควรสร้างลักษณะนิสัยในการป้องกันภัยสำหรับบุคลากร"

(ผู้ให้ข้อมูลสำคัญที่ 20, สัมภาษณ์เมื่อวันที่ 19 มีนาคม 2566)

นอกจากนี้ ผู้ให้ข้อมูลสำคัญคนที่ 4 และผู้ให้ข้อมูลสำคัญคนที่ 21 แสดงความคิดเห็นในแง่มุมที่แตกต่างเพิ่มเติมว่า

"กฎหมายยังมีความไม่สอดคล้องในบางประเด็น เนื่องจากการออกกฎหมายจากคนที่เขียนแต่ไม่มีคนที่รู้จริงๆในด้านนั้นๆอยู่เป็นทีมงานด้วย ทำให้กฎหมายที่ออกมาไม่ค่อยสัมพันธ์หรือสอดคล้องกับหน่วยงาน แต่อาจจะสอดคล้องกับบางหน่วยงาน เช่น กลุ่มการเงินการธนาคาร เพราะกลุ่มนี้จะเป็น IT ล้วน ๆ แต่ไม่มีด้าน OT หรือ Operation Technology ซึ่งจริงๆแล้ว คำว่า OT อาจทำให้คนสับสนได้ ส่วนตัวมองว่าควรใช้คำว่า ICS หรือ industrial control system มากกว่า ซึ่ง ICS เองก็จะมีจาก การไฟฟ้า การประปา หน่วยงานที่เป็นพลังผลิตไฟฟ้าก็มี หรือหน่วยงานที่เป็น health care ก็มี ซึ่งกลุ่มเหล่านี้ก็จะมี ICS ทั้งหมด แต่สิ่งที่ประกาศออกมาจะเป็นฝั่ง IT ส่วนใหญ่ นี่คือความไม่สอดคล้อง แต่มองว่าเป้าหมายเค้าคืออยากไปด้าน OT คือกระบวนการ control ฝั่ง IT แต่บางอย่างด้าน IT ไม่สามารถนำไปใช้ได้กับด้าน OT หรือ ICS ได้ เนื่องจากมีข้อจำกัดค่อนข้างเยอะ เช่น วิธีการปฏิบัติและ standard ที่ใช้ไม่ค่อยเหมือนกัน แต่ผู้ที่ออกประกาศตรงนี้มาก็จะพยายามให้ครอบคลุมส่วนนี้ทั้งหมด ซึ่งในความเป็นจริงไม่มีวันที่จะ outside อยู่แล้ว"

(ผู้ให้ข้อมูลสำคัญที่ 4, สัมภาษณ์เมื่อวันที่ 31 มีนาคม 2566)

“ผมมองว่ากฎหมายยังไม่สอดคล้อง เพราะรัฐจะต้องรู้ก่อนว่าจะเกิดอะไรขึ้น ซึ่งยังไม่มีใครรู้เลยว่าตอนนี้ประเทศไทยกำลังอยู่ในสถานการณ์สงคราม และเป็น Hybrid Warfare และก็จะมี Cyber Warfare ตามมา และสถานการณ์โลก แถวหน้าคือ Economic Forum ซึ่ง Cybercrime กับการก่อการร้ายทางไซเบอร์ คือความเสี่ยงอันดับ 2 รองจาก Climate Change คือ ทรัพยากรหาย ถูกทำลาย จะเกิดการแย่งชิง เงินเฟ้อขึ้น กฎหมายต้องการให้ทุกองค์กรต้องมีการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ซึ่งทั้งหมดต้องปฏิบัติตามกฎหมายซึ่งต้องมี DPO อยู่แล้ว ส่วนใครจะไปตั้งคณะทำงานเพิ่มก็จะยิ่งดี หรือเพิ่มมาตรการด้านความมั่นคงปลอดภัยเพิ่มก็ยิ่งดี”

(ผู้ให้ข้อมูลสำคัญที่ 21, สัมภาษณ์เมื่อวันที่ 25 มีนาคม 2566)

4.3.2.2 การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร

ผู้ให้ข้อมูลสำคัญคนที่ 14 ได้เปิดเผยว่า สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนดให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นผู้กำกับดูแลด้านเทคโนโลยีดิจิทัลและด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร ซึ่งเป็นไปตามที่กำหนดไว้ในกฎกระทรวงแบ่งส่วนราชการสำนักงานปลัดกระทรวง กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ฉบับที่ 2) พ.ศ. 2565 โดยมีกลุ่มงาน ทำหน้าที่

1. ด้านกำกับดูแล โดยกำหนดทิศทางกลยุทธ์และเป้าหมาย กำกับดูแลการบริหารดำเนินงาน ผ่านผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม ของสำนักงานปลัดกระทรวง

2. ด้านการบริหารจัดการ โดยจัดการข้อมูลสารสนเทศของหน่วยงานให้เป็นไปตามมาตรฐาน ISO และติดตามตรวจสอบความถูกต้องแม่นยำ

3. ด้านการปฏิบัติการ โดยได้กำหนดขั้นตอน วิธีปฏิบัติ กรอบให้แก่เจ้าหน้าที่ในสังกัด สป.ดศ. ให้ปฏิบัติตามติดตาม ประเมินผล และรายงานความเสี่ยงต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม ของหน่วยงาน

นอกจากนี้ ดำเนินการตามแนวทางและกระบวนการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐานที่ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 กำหนดครอบคลุม Identify Protect Detect Respond และ Recovery และรวมถึงขนาด ความ

ซับซ้อนเทคโนโลยีที่ใช้ในการดำเนินงานของหน่วยงาน และประเมินความเสี่ยงที่อาจเกิดขึ้น โดยได้พิจารณาให้ครอบคลุม ได้แก่ 1. การกำหนดแนวปฏิบัติด้านการเข้ารหัสข้อมูล (cryptography) ในการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสมตามชั้นความลับ และความสำคัญของข้อมูลสารสนเทศ 2. การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสารขององค์กรและการเชื่อมต่อกับหน่วยงานภายนอก (network and communication security) 3. การกำหนดหลักเกณฑ์และกระบวนการในการจัดหาและการพัฒนาระบบของ Stakeholder (system acquisition and development) 4. การจัดจ้างผู้ให้บริการภายนอก (third party management)"

ในขณะที่ผู้ให้ข้อมูลสำคัญคนที่ 6 ให้ความคิดเห็นว่า หากมีการประกาศเกี่ยวกับ พ.ร.บ.ไซเบอร์ 2562 ใหม่ๆออกมา จะดำเนินการให้สอดคล้องกับสิ่งที่องค์กรมีอยู่ และให้ครอบคลุม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลหรือ PDPA ด้วย อย่างไรก็ตาม ผู้ให้ข้อมูลสำคัญคนที่ 10 มีความคิดเห็นที่แตกต่างออกไปว่า ความปลอดภัยด้านไอทีนั้น CIA ถือว่าเป็นเรื่องที่สำคัญ ได้แก่ ความลับ (Confidentiality) ความคงสภาพ (Integrity) และ ความพร้อมใช้ (Availability) ซึ่งบุคลากรด้านไอทีทั่วไปควรแยกกับทีม IT security เนื่องด้วยต้องมีขั้นตอนของการตรวจสอบหรือ Audit เพราะหากเป็นทีมเดียวกันอาจจะเกิด ความขัดแย้ง (Conflict) นอกจากนี้ IT security จะต้องมีการจัดทำ Penetration Test และ VA เพื่อตรวจหาช่องโหว่ ซึ่งถ้าเป็นฝ่ายเดียวกันทดสอบกันเองอย่างไรก็ผ่านการทดสอบ ดังนั้นจึงต้องมี Data Governance หรือธรรมาภิบาลกำกับดูแล

ในส่วนของผู้ให้ข้อมูลสำคัญคนที่ 9 ในฐานนะหน่วยงานควบคุมหรือกำกับดูแล (Regulator) แสดงทรรศนะไว้ว่า

> *"มองว่าทั้งสองหน่วยงานคือ ด้านกฎหมายและไอทีควรที่จะต้องแบ่งหน้าที่กัน ในลักษณะของ Check and Balance เช่น คนทำ คน implement ฝ่ายไอที และมีคนคอยตรวจสอบไม่ว่าจะเป็นฝ่าย IT audit และ internal audit หรือฝ่ายไซเบอร์เอง เป็น first teer คือ กฎหมายทำงานร่วมกับฝ่ายไอที เพื่อช่วยดูให้ IT มีความปลอดภัยมีการ implement อุปกรณ์ป้องกันต่างๆไม่ว่าจะเป็นในเรื่องของตัว process การทำงานก็ดีหรือว่าพวกเทคโนโลยีก็ดีรวมถึงการส่งเสริมการอบรมการสร้างความตระหนัก แล้วส่วนของ second line คือ IT audit เราอยู่กับฝ่าย internal audit ในส่วน Third line เราก็มีการจ้าง external audit มาคอยตรวจสอบ ซึ่งก็มองว่าต้องมีการแบ่งแยกหน้าที่ชัดเจน รวมถึงต้องเป็นนโยบายที่ชัดเจนว่าต้องมีการ*

check and balance อย่างไรก็ตาม แต่ละหน่วยงานเขาก็มีระเบียบวิธีปฏิบัติต่างกัน กฎหมายอาจจะออกได้คร่าวๆว่าจริงๆใน พรบ. ไซเบอร์รวมถึง PDPA ก็มีพูดถึงว่าแต่ละหน่วยงานจะต้องจัดให้มีการตรวจสอบ Level ที่ 1 Level ที่ 2 อะไรทำนองนี้ แต่สิ่งที่ผมมองว่ามันยังขาดเนี่ยก็อาจจะคือเรายังไม่มีเกณฑ์ว่า ระบบคุณปลอดภัยหรือยังแค่ไหนคือปลอดภัย หรือคุณทำแค่ไหนคือปลอดภัยสำหรับภาครัฐของประเทศไทย เพราะว่าการทำทุกอย่างจะสะท้อนกลับไปถึงงบประมาณแผ่นดิน เราทำแค่ไหนเราจะสร้างรั้วสูงแค่ไหนเพื่อให้ปลอดภัยเพียงพอ ซึ่งผมมองว่าอันนี้เป็นหน้าที่หลักของ regulator หน้าที่หลักของคนกำกับตั้งแต่ สกมช. อาจจะต้องออกภาพรวมของประเทศว่า แค่ไหนถึงจะปลอดภัยสำหรับประเทศไทย แล้ว สพร. เองในฐานะ regulator ที่ดูภาครัฐ เราก็นำภาพใหญ่จาก สกมช. มาถอดออกมาในมุมมองของไม้บรรทัดที่เอามาวัดหน่วยงานภาครัฐใน level เล็ก กลาง ใหญ่ หรืออื่นใด คือ ต่อไปคุณทำเท่านี้คือปลอดภัย หรือเปรียบได้ว่า คุณจะทำสูงกว่าบรรทัดไม่เป็นไร แต่ห้ามต่ำกว่าบรรทัดอะไรทำนองนี้”

(ผู้ให้ข้อมูลสำคัญที่ 9, สัมภาษณ์เมื่อวันที่ 30 มีนาคม 2566)

นอกจากนี้ ในแง่ของการบริหารความมั่นคงปลอดภัยสารสนเทศด้านกระบวนการยุติธรรม ผู้ให้ข้อมูลสำคัญคนที่ 18 แสดงความคิดเห็นไว้ว่า

“กองบังคับการตรวจสอบและวิเคราะห์อาชญากรรมทางเทคโนโลยี กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี โดยกลุ่มงานรักษาความมั่นคงปลอดภัยทางไซเบอร์ ในฐานะทำการแทนสำนักงานตำรวจแห่งชาติ ซึ่งเป็นหน่วยงานควบคุมหรือกำกับดูแล ได้กำหนดให้ 1. ศูนย์เทคโนโลยีสารสนเทศกลาง ซึ่งควบคุมดูและระบบสารสนเทศ POLIC และ CRIME 2. กองทะเบียนประวัติอาชญากร ควบคุมดูแลระบบตรวจสอบลายนิ้วมือ (AFIS) ตรวจสอบประวัติอาชญากรรม ให้เป็นหน่วยงานที่อยู่ภายใต้การดูแล โดยกำหนดให้เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในหมวด 1 ด้านความมั่นคงของรัฐ ในภารกิจด้านการบังคับใช้กฎหมายและอำนวยความยุติธรรมทางอาญา 3. กองบังคับการตำรวจ

จราจร ควบคุมดูแลระบบข้อมูลใบสั่งในเครื่องคอมพิวเตอร์ของระบบสารสนเทศกลาง เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในหมวด 5 ด้านการขนส่งและโลจิสติกส์"

(ผู้ให้ข้อมูลสำคัญที่ 18, สัมภาษณ์เมื่อวันที่ 28 เมษายน 2566)

ในขณะที่ผู้เชี่ยวชาญชี้ประเด็นจุดอ่อนของการบริหารจัดการด้านความปลอดภัยสารสนเทศของภาครัฐที่ผู้บริหารควรพิจารณาปรับปรุงไว้ ดังนี้

"1. ต้องมีเจ้าหน้าที่รองรับคอยเฝ้าระวังระบบ server 24 ชม. 2. ต้องมี Encryption database on less มีการใช้ Firewall หลายชั้น การใช้ security frontend ต้องมีเรื่อง access control เหล่านี้เป็นต้น"

(ผู้ให้ข้อมูลสำคัญที่ 20, สัมภาษณ์เมื่อวันที่ 19 มีนาคม 2566)

"หน่วยงานส่วนใหญ่ของภาครัฐที่เป็น Security Digital กล่าวได้ว่า มีการรักษาความมั่นคงปลอดภัยไซเบอร์แค่ขั้นต่ำ ยังไม่ได้เรียกว่าขั้นสูง ส่วนใหญ่ภาครัฐยังมี compliance ที่ไม่ครอบคลุม"

(ผู้ให้ข้อมูลสำคัญที่ 21, สัมภาษณ์เมื่อวันที่ 25 มีนาคม 2566)

4.3.2.3 ด้านการบูรณาการเชื่อมโยงระหว่างหน่วยงาน

ปัจจุบันภาครัฐของไทยยกระดับสู่การเป็นรัฐบาลดิจิทัล ที่มีการบูรณาการระหว่างหน่วยงาน มีการดำเนินงานแบบอัจฉริยะ ให้บริการโดยมีประชาชนเป็นศูนย์กลาง และขับเคลื่อนให้เกิดการเปลี่ยนแปลงได้อย่างแท้จริง มีการกำหนดข้อมูลขององค์กรที่สามารถเปิดเผยข้อมูลสารสนเทศขององค์กรและแลกเปลี่ยนข้อมูลกับหน่วยงานอื่น การกำหนดนโยบายและแนวทางส่งเสริมการทำงานร่วมกันระหว่างหน่วยงาน พัฒนาระบบการทำงานร่วมกันระหว่างหน่วยงานภาครัฐ วางแผนบูรณาการการทำงานร่วมกัน โดยกำหนดเป็นแผนปฏิบัติการขององค์กรที่ชัดเจนเป็นรูปธรรม สอดคล้องกับผู้ให้ข้อมูลสำคัญ ดังนี้

“ประสานงานกับหน่วยงานที่ควบคุมดูแลคือกระทรวงมหาดไทยและ สกมช. เพื่อรับทราบข่าวสารเกี่ยวกับการโจมตีว่ามีการโจมตีประเภทไหนเกิดขึ้นบ้างและการแก้ไขการป้องกันจะดำเนินการยังไง ผ่านช่องทางไม่ว่าจะเป็น ทางอีเมล ทางโทรศัพท์หรือทางไลน์ เพื่อให้ได้รับทราบข่าวสารได้เร็วที่สุด นอกจากนี้ยังมีการทำบันทึกข้อตกลงหรือ MOU ร่วมกันกับการไฟฟ้าส่วนภูมิภาคในการแลกเปลี่ยนและสื่อสารข้อมูลด้าน Cyber Attack เพื่อเรียนรู้และรับมือภัยคุกคามทางไซเบอร์ สำหรับต่างประเทศนั้นเราไม่มีไม่มีการทำสัญญาหรืออะไรโดยตรง เพียงแต่ว่าเราอาศัยเป็นช่องทางในการรับทราบข้อมูลเกี่ยวกับการโจมตีและเหตุการณ์ผิดปกติหรือช่องโหว่ที่เกิดขึ้นของผลิตภัณฑ์ต่างๆ ผ่านช่องทางเว็บไซต์ต่างๆ”

(ผู้ให้ข้อมูลสำคัญที่ 2, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

“ทาง DGA ที่ประสานมา มีการประสานงานคุยงานร่วมกันด้าน detect และ checklist ชื่อ กับทางด้านสำนักงานมาตรฐานสากล หากใช่ก็จะทำการบล็อกภัยคุกคามยกตัวอย่างที่เห็นได้ชัดคือ ransomware ซึ่งเวลาตัว ransomware เวลาทำงาน มันจะเป็น site ที่อยู่ใน list ของกระบวนการจัดการ โดยจะเข้าไป detect ชื่อนั้นและจะดำเนินการ resolve คือ SOAR ย่อมาจากคำว่า Security Orchestration, Automation และ Response เป็นกระบวนการสร้างเพย์บุคขึ้นมาทำงานร่วมกันกับทางสากลที่เรียกว่า threat intelligence เพื่อที่จะ detection และ response ด้านการจัดการกระบวนการรักษาความปลอดภัย ซึ่งกระบวนการทั้งหมดนี้เป็นฟังก์ชันนึงของศูนย์ SOC ซึ่งก็เป็น outsource ที่ทำงานร่วมกับ กปน.”

(ผู้ให้ข้อมูลสำคัญที่ 3, สัมภาษณ์เมื่อวันที่ 30 มีนาคม 2566)

“มีการประสานงานในประเทศกับหน่วยงานภายนอก เช่น สกมช. และทำ MOU ร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างการไฟฟ้า 3 แห่งเมื่อวันที่ 14 กุมภาพันธ์ 2566 ที่ผ่านมาระหว่าง PEA การไฟฟ้าส่วนภูมิภาค MEA การไฟฟ้านครหลวง และ EGAT การไฟฟ้าฝ่ายผลิต เพื่อรับข้อมูลข่าวสารและรับมือภัยคุกคาม นอกจากนี้

ได้มีแชร์ข้อมูลข่าวสารด้าน Cyber Attack ระหว่าง PEA กฟภ. และ PWA กปภ. ผ่านระบบอีเมลหน่วยงาน"

(ผู้ให้ข้อมูลสำคัญที่ 4, สัมภาษณ์เมื่อวันที่ 31 มีนาคม 2566)

"ของเรามีทั้งภายในและภายนอกประเทศ สำหรับภายในประเทศ หลักๆก็จะมี สกมช. ในส่วนของระดับ sector และเรามีการทำ MOU ในด้าน sector การเงิน ซึ่งในประเทศไทยจะมี regulator อยู่ 3 ราย คือ แบงก์ชาติ ก.ล.ต. กำกับดูแลในเรื่องของหลักทรัพย์ คปภ. ที่กำกับดูแลในเรื่อง Insurance ด้านประกันภัย เพราะฉะนั้น เราก็จะมีการประชุมในระดับ sector ร่วมกัน 3 องค์กรเป็นความร่วมมือภาคการเงิน สำหรับในภาคการธนาคาร ในประเทศไทยเราจะมี TB-CERT เป็นกลุ่ม community ของแบงก์พาณิชย์ในไทยทุกแบงก์รวมถึงแบงก์ต่างชาติบางแบงก์ด้วย เป็นสมาชิกอยู่และมีการประชุมทุกเดือน เป็นการแลกเปลี่ยนข้อมูล ถ้าใครมีเคสอะไรก็จะแลกเปลี่ยนข้อมูลกัน สำหรับภายนอก ในส่วนต่างประเทศก็จะมีลักษณะคล้ายๆกัน ในส่วนของแบงก์ชาติก็จะเป็น center bank และก็จะมีความร่วมมือของกลุ่ม community ของ center bank เอง และแบงก์ชาติเป็นสมาชิกเข้าร่วมกลุ่ม BIS เพื่อแชร์ข้อมูล ร่วมใน working group เขียน paper ต่างๆ ด้าน security ระดับย่อยลงมาอีกคือ แบงก์ที่อยู่ในยุโรปก็ดี แอฟริกาก็ดี ย่อยลงมาอีกคือ ระดับอาเซียนเองก็จะมี commercial bank security ที่แชร์ข้อมูลด้าน security เรียกว่ากลุ่ม CRISP เป็นกลุ่มที่แบงก์ชาติ 10 ประเทศในอาเซียนเป็นสมาชิกอยู่ มีการประชุมปีละ 2 ครั้ง เพื่อแชร์ข้อมูล ความรู้ ประสบการณ์ ด้านความปลอดภัยไซเบอร์"

(ผู้ให้ข้อมูลสำคัญที่ 5, สัมภาษณ์เมื่อวันที่ 26 เมษายน 2566)

"เรามีการประสานงานในประเทศ เราเป็นสมาชิกของ TB-CERT ซึ่งจะมีการแชร์ข้อมูลกันระหว่างธนาคารสมาชิก และมีการจัดตั้ง CISO เอง เพื่อเป็นผู้ประสานงานกับทางหน่วยงานที่เป็น regulator ทั้ง สกมช. แบงก์ชาติ และ ก.ล.ต."

(ผู้ให้ข้อมูลสำคัญที่ 6, สัมภาษณ์เมื่อวันที่ 28 เมษายน 2566)

“สำนักปลัดกระทรวงสาธารณสุขเป็นศูนย์กลางในการประสานงานเพื่อดำเนินการตามนโยบายโดยมีคณะทำงานธรรมาภิบาลด้านข้อมูลและเทคโนโลยีสุขภาพระดับจังหวัด สื่อสารไปยัง Operator ด้านต่างๆของภาครัฐ ทั้งในและนอกสังกัด สธ. รวมถึงภาคเอกชน เพื่อรายงานต่อ Health CIRT เมื่อคาดว่าจะเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ และหากอยู่ในระดับวิกฤต Health CIRT จะทำหน้าที่รายงานต่อ NCERT และ สกมช.”

(ผู้ให้ข้อมูลสำคัญที่ 7, สัมภาษณ์เมื่อวันที่ 26 พฤษภาคม 2566)

“มีการกำกับดูแลตาม พ.ร.บ. วิธีปฏิบัติการทางอิเล็กทรอนิกส์ ซึ่งเป็นการส่งเสริมในการป้องกันภัยให้ภาครัฐเป็นรัฐบาลดิจิทัล และการร่วมมือกับหน่วยงานต่างประเทศ ไม่ว่าจะเป็นต่างประเทศที่เราพยายามไปดูต้นแบบในการที่เขาให้บริการประชาชนด้วยระบบดิจิทัล อย่างเช่น เอสโตเนีย สิงค์โปร์ ไต้หวัน”

(ผู้ให้ข้อมูลสำคัญที่ 9, สัมภาษณ์เมื่อวันที่ 30 มีนาคม 2566)

“ต้องเป็นหน่วยงาน DPO ในการประสานงานทุกทิศทาง และต้องอิสระจากผู้บริหารครอบงำ เช่น การจ้าง outsource และห้ามไล่ DPO ออก DPO ควรมีทุกองค์กร ต้องหาหน่วยงานรับมือจะดีกว่าป้องกันหรือเพียงแค่จัดทำแผน และมีหน่วยงานด้านการประสานงานและให้คำปรึกษาได้”

(ผู้ให้ข้อมูลสำคัญที่ 10, สัมภาษณ์เมื่อวันที่ 27 มีนาคม 2566)

“เราประสานงานในเชิงนโยบายและประสานงานเรื่องกรอบความร่วมมือต่างๆในระดับเวทีทั้งในระดับภูมิภาคและระดับโลก อย่างเช่น ARS กรอบอาเซียน เช่น สิงค์โปร์ เป็นหลักหรือไม่ก็ UN และ AFC หรือว่าจะเป็นในเรื่องของกรอบ WinTech กลุ่มประเด็นความมั่นคงโดยรวมอยู่แล้ว เช่น อินเดีย ภูฏาน ศรีลังกา พม่า เป็นต้น แต่ถ้าเกี่ยวข้องกับความมั่นคงทางไซเบอร์ เราก็จะเข้าไปร่วมด้วย แล้วแต่ว่า

วาระการประชุมมีอะไรบ้าง ในส่วนเรื่องของความมั่นคงทางไซเบอร์ในเรื่องของโครงสร้างพื้นฐานหรือว่าหน่วยงาน CII จะเป็น สกมช ที่รับผิดชอบโดยตรง เพราะว่าตัว พ.ร.บ. ไซเบอร์ จะต้องมีการที่จะขับเคลื่อนร่วมกัน และจะให้เร่งรัดการจัดทำ MOU คอยประสานงานร่วมกับ สกมช กับหน่วยงานอื่นเพราะว่า สกมช เป็นหน่วย National CERT และ พ.ร.บ. ไซเบอร์ เป็นประเด็นใหญ่และค่อนข้างเฉพาะทางมาก แต่เรื่อง Cybercrime ก็ยังไม่แล้วเสร็จ จึงต้องมีความร่วมมือที่ให้การ endorse ไปโดยตรง และเนื่องจาก สมช ไม่ได้เป็นหน่วยงานด้านการปฏิบัติโดยตรง เราจึงให้ สกมช ประสานงานเป็นหลักกับหน่วยงาน POC ต่างๆ แต่ สมช. ก็จะมีการทำ MOU ร่วมในด้านอาชญากรรมความมั่นคงทางไซเบอร์ การฟอกเงิน ก่อการร้ายที่จะดูในภาพรวมร่วมกัน และถ้าหากในการประชุมนั้นมีเรื่องความมั่นคงทางไซเบอร์เราก็จะเข้าร่วมประชุมด้วย”

(ผู้ให้ข้อมูลสำคัญที่ 11, สัมภาษณ์เมื่อวันที่ 19 เมษายน 2566)

“ดำเนินการติดต่อและประสานการดำเนินงานในด้านต่าง ๆ เช่น ข้อมูล เหตุการณ์ภัยคุกคามทางไซเบอร์ แนวปฏิบัติต่าง ๆ ร่วมกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติอย่างใกล้ชิด”

(ผู้ให้ข้อมูลสำคัญที่ 14, สัมภาษณ์เมื่อวันที่ 18 เมษายน 2566)

“มีการประสานงานหน่วยงานภายในกระทรวงและภายนอก คือ สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และยังไม่มีหน่วยไหนเป็น regulator”

(ผู้ให้ข้อมูลสำคัญที่ 15, สัมภาษณ์เมื่อวันที่ 29 มีนาคม 2566)

“ในระดับประเทศ สำนักงานตำรวจแห่งชาติได้จัดการประชุมอาชญากรรมไซเบอร์สำหรับหน่วยงานบังคับใช้กฎหมายและหุ้นส่วนระหว่าง ผู้แทนจากประเทศสมาชิกอาเซียน 8 ประเทศ มีผู้เข้าร่วมประชุมกว่า 100 คน ณ จังหวัดภูเก็ต เมื่อวันที่ 16 – 19 พ.ค. พ.ศ.

2565 ที่ผ่านมา โดยเร่งปราบปรามอาชญากรรมทางออนไลน์เร่งด่วนและจริงจัง รวมทั้งสร้างภูมิคุ้มกันให้กับประชาชนไม่ให้ตกเป็นเหยื่อ ทั้งนี้ อาชญากรรมทางออนไลน์ มีการกระทำความผิดในลักษณะเป็นกลุ่มองค์กร กระจายกันอยู่ทั้งในประเทศและต่างประเทศ จำเป็นอย่างยิ่งที่จะต้องได้รับความร่วมมือจากประเทศภาคีเครือข่าย ในการแลกเปลี่ยนข้อมูลอันเป็นประโยชน์ระหว่างกัน การแลกเปลี่ยนมุมมอง ข้อคิดเห็นและประสบการณ์ของประเทศต่างๆ โดยเฉพาะอย่างยิ่งในด้านการข่าวและการแบ่งปันข้อมูลระหว่างกัน รวมถึงการยกระดับความร่วมมือระหว่างหน่วยงานบังคับใช้กฎหมายในอาเซียน ซึ่งจะทำให้การป้องกันและปราบปรามการกระทำความผิดทางไซเบอร์ของไทยมีประสิทธิภาพดียิ่งขึ้น สำหรับในประเทศไทย มีการทำ MOU กับหลายฝ่ายทั้งภาครัฐและเอกชน เช่น EGA DSI สกมช. กสทช. เครือข่ายโทรศัพท์ต่างๆ ล่าสุดจัดทำบันทึกข้อตกลงหรือ MOU กับสมาคมธนาคารไทย เพื่อยกระดับสกัดกระบวนการถ่ายโอนเงินระหว่างบัญชีม้า ซึ่งหลายฝ่ายได้พยายามหากลไกเข้ามาจัดการ แต่ในภาคของกฎหมายยังตามหลังอยู่”

(ผู้ให้ข้อมูลสำคัญที่ 18, สัมภาษณ์เมื่อวันที่ 28 เมษายน 2566)

สรุปได้ว่า โครงสร้างการกำกับดูแล การขับเคลื่อนการบังคับใช้นโยบายและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ในการบริหารจัดการความเสี่ยง เพื่อสร้างความตระหนักและเฝ้าระวังภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ มีข้อค้นพบว่า หลายองค์กรในประเทศไทยทั้งหน่วยงาน CII หน่วยงานด้านการกำกับดูแล และหน่วยงานด้านกระบวนการยุติธรรม ได้ดำเนินงานตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ในการปรับปรุงโครงสร้างองค์กรเพื่อเพิ่มหน่วยงานเฉพาะที่เกี่ยวข้องด้านการเฝ้าระวังและรับมือภัยคุกคามทางไซเบอร์ และหน่วยงานที่คอยประสานงานและรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์ร่วมกับ สกมช. เพื่อให้สามารถแก้ไขปัญหาได้ทันท่วงที รวมถึงหน่วยงานด้าน Data Protection Officer (DPO) หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ในการดูแลรักษาข้อมูลส่วนบุคคลทั้งหมดขององค์กร ไม่ว่าจะเป็นข้อมูลภายในหรือภายนอกองค์กรก็ตาม โดยเจ้าหน้าที่ DPO นั้นจะทำหน้าที่ให้คำปรึกษา ตรวจสอบ กำกับดูแลการใช้ข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมายคุ้มครอง

ข้อมูลส่วนบุคคล ซึ่งองค์กรจะไม่สามารถห้ามไม่ให้ DPO ทำหน้าที่ตามที่กฎหมายกำหนด หรือไล่ DPO ออกได้ อีกทั้งได้นำกฎหมายรองดังกล่าว พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560 มาพิจารณาจัดทำนโยบายความมั่นคงปลอดภัยด้านสารสนเทศได้กำหนดองค์ประกอบที่สำคัญของการบริหารจัดการระบบเทคโนโลยีสารสนเทศให้มีความมั่นคงปลอดภัย โดยครอบคลุมทั้งด้านการควบคุมการเข้าถึง การกำหนดขั้นตอนและกระบวนการที่เหมาะสม ตามหลักมาตรฐานสากล

นอกจากนี้ หน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ หรือ CII ได้นำกฎหมายรองเหล่านี้ ไปใช้ในการประเมินความเสี่ยงด้านความปลอดภัยทางไซเบอร์ที่ช่วยให้ธุรกิจและองค์กรเข้าใจ ควบคุม และลดความเสี่ยงทางไซเบอร์ทุกรูปแบบ ที่เป็นองค์ประกอบสำคัญของการบริหารความเสี่ยงและลดความเสี่ยง หากไม่มีการประเมินความเสี่ยงการรักษาความปลอดภัยทางไซเบอร์ อาจส่งผลกระทบต่อข้อมูลและทรัพยากรสำคัญใน การดำเนินการอยู่ของธุรกิจและองค์กรได้ ทั้งการประเมินในด้าน กรอบกำกับดูแล (Governance) การระบุความเสี่ยง (Risk Identification) การป้องกัน (Protection) การเฝ้าระวังและการตรวจจับ (Detection) และมาตรการในการตรวจหาช่องโหว่หรือจุดอ่อนของระบบงาน รวมทั้งสามารถดำเนินการปรับปรุงแก้ไขป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้อย่างทันการณ์มี การตอบสนองต่อเหตุการณ์และการกู้คืน (Respond and Recovery) เพื่อให้องค์กรมีแผนและระเบียบวิธีปฏิบัติในการรับมือภัยคุกคามและการตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ที่อาจส่งผลกระทบให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ และสามารถกู้คืนระบบให้กลับคืนสู่สภาพปกติภายใต้ระยะเวลาที่ยอมรับได้ ตลอดจนการบริหารความเสี่ยงด้านภัยคุกคามที่เกิดจากผู้มีส่วนได้ส่วนเสีย (Stakeholders) หรือหน่วยงานภายนอก (Third Party Risk Management) เพื่อให้องค์กรมีแนวทางในการบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างมีประสิทธิภาพ อีกทั้งพฤติกรรมการป้องกันอาชญากรรมไซเบอร์ในองค์กรโดยส่วนมาก ได้รับอิทธิพลจากปัจจัยส่วนบุคคล และประสบการณ์ในอดีต รวมทั้งปัจจัยด้านสภาพแวดล้อม ได้แก่ การสร้างจิตสำนึกในการรับรู้คุณค่าข้อมูล ความรู้ด้านความปลอดภัย การลงทุนด้านการป้องกันภัย โดยส่งผ่านการรับรู้ต่อสภาวะคุกคามการรับรู้ความสามารถในการจัดการกับภัยคุกคามและแรงจูงใจในการป้องกัน เพื่อสร้างความตระหนักรู้ของผู้ใช้เทคโนโลยีและข้อมูลสารสนเทศ

4.4 แนวทางการรับมือภัยคุกคามทางไซเบอร์และการกำกับดูแลการบริหารจัดการที่ดีด้านความมั่นคงปลอดภัยไซเบอร์

4.4.1 การรับมือภัยคุกคามทางไซเบอร์

การรับมือภัยคุกคามทางไซเบอร์ เป็นการตอบสนองต่อภัยคุกคามทางไซเบอร์ นั่นหมายถึงกระบวนการตอบสนองและบรรเทาผลกระทบจากการโจมตีทางไซเบอร์หรือการละเมิดความปลอดภัย โดยเกี่ยวข้องกับการระบุแหล่งที่มาและลักษณะของภัยคุกคาม การแพร่กระจาย และการกู้คืนระบบและข้อมูลที่ได้รับผลกระทบให้อยู่ในสถานะที่ปลอดภัย กระบวนการนี้อาจรวมถึงการใช้แพตช์ (Patch) ความปลอดภัย การอัปเดตซอฟต์แวร์ การวิเคราะห์ทางนิติวิทยาศาสตร์ และการสื่อสารกับผู้มีส่วนได้ส่วนเสียเกี่ยวกับเหตุการณ์ดังกล่าว เป้าหมายของการตอบสนองต่อภัยคุกคามทางไซเบอร์ เพื่อลดความเสียหายและป้องกันไม่ให้เกิดการโจมตีหรือถูกโจมตีในอนาคต โดยผลการศึกษาการรับมือภัยคุกคามทางไซเบอร์ในงานวิจัยนี้ สามารถอธิบายแนวทางการรับมือได้เป็น 4 หน่วยงาน ได้แก่ การรับมือของหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ การรับมือของหน่วยงานด้านการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ การรับมือของหน่วยงานด้านการป้องกันและปราบปราม และการรับมือของบุคลากรผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ อีกทั้งข้อมูลจากการสัมภาษณ์แสดงให้เห็นถึงกระบวนการที่สำคัญในการเตรียมความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ ประกอบด้วย (1) การกำกับดูแลและบริหารความเสี่ยง (2) มาตรฐานและมาตรการเฝ้าระวังภัยไซเบอร์ (3) การประสานความร่วมมือและถ่ายทอดสื่อสารให้แก่ผู้มีส่วนได้ส่วนเสีย และ (4) การติดตามและประเมินผลลัพธ์

4.4.1.1 การรับมือของหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ

(1) การกำกับดูแลและการบริหารความเสี่ยง

การกำกับดูแลและบริหารความเสี่ยงสำหรับหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศหรือ CII หรือที่รู้จักในนิยามของ GRC ประกอบด้วย การกำกับดูแล (Governance) การบริหารความเสี่ยง (Risk) และการปฏิบัติตามข้อกำหนด (Compliance) ที่ผสมผสานการดำเนินงานด้านพนักงาน (People) ด้านกระบวนการ (Process) และด้านเทคโนโลยีสารสนเทศ (Technology) ในเชิงบูรณาการ โดยมีวัตถุประสงค์เพื่อให้องค์กรการดำเนินงานตามภารกิจในด้านต่างๆ ให้เป็นไปตามเป้าหมายที่กำหนด สอดคล้องกับยุทธศาสตร์องค์กร ภายใต้กรอบของกฎหมาย นโยบาย ระเบียบ ข้อบังคับและมาตรฐานต่างๆที่เกี่ยวข้องกับการพัฒนาเทคโนโลยี

ดิจิทัล เช่น เช่น พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นต้น รวมถึงจริยธรรมและจรรยาบรรณ ตลอดจนให้ข้อมูลที่เหมาะสม น่าเชื่อถือ และทันกาลแก่ผู้ที่มีส่วนได้ส่วนเสีย (Stakeholders) ด้วยการสร้างกลไกการกำกับดูแลการดำเนินงานขององค์กรอย่างมีกระบวนการที่ชัดเจน เพื่อช่วยลดความสูญเสียและเพิ่มโอกาสให้แก่องค์กร โดยมีคณะกรรมการบริหารระดับสูงสุดของหน่วยงานในการกำกับดูแล ซึ่งสอดคล้องกับผู้ให้ข้อมูลที่สำคัญ ดังนี้

“ปัจจุบันในเรื่องของกระบวนการทำงานของ กปภ. มีทั้งหมด 20 กระบวนการ ทั้งในด้านการผลิต ระบบจำหน่าย รวมถึงระบบลูกค้า เป็นหลัก ซึ่งเราได้นำเทคโนโลยีดิจิทัลเข้าไปเป็นส่วนหนึ่งในทุกๆกระบวนงาน เพราะฉะนั้นจึงต้องมีทั้งเรื่องของความปลอดภัยและเรื่องของความเสี่ยงเข้ามาเกี่ยวข้องในทุกส่วน แต่ในเรื่องของการผลิต เรายังไม่ได้นำดิจิทัลเข้าไปใช้อย่างเต็มที่ เพราะมีทั้งส่วนที่เป็น manual และ auto ที่แยกออกจากกัน แต่ในเรื่องของระบบจ่ายเรามีทั้งระบบ DMA และ SCADA เพราะฉะนั้นระบบเหล่านี้ก็จะมีการเชื่อมโยงไปยัง Internet ซึ่งอาจจะถูกโจมตีหรือเผชิญกับภัยคุกคามได้ ดังนั้น ในด้านการผลิตเรากำลังจะมีการนำระบบเข้ามาใช้ และด้านการสร้างความพึงพอใจให้กับลูกค้าส่วนนี้อาจจะมีแนวโน้มในการเกิดภัยคุกคามเพิ่มขึ้น แต่เรามีระบบป้องกันด้วย Infrastructure มีห้องมั่นคงที่ได้การรับรองมาตรฐานสากลอย่างมาตรฐาน ISO/IEC 27001 : 2013 ที่ดูแลโดยเจ้าหน้าที่ของ กปภ. และอีกส่วนหนึ่งคือมีการจ้าง Outsource คอยดูแล นอกจากนี้ มีการจัดทำ Fishing mail เพื่อทดสอบระบบตามแผนรับมือภัยคุกคามทางไซเบอร์ปีละ 2 ครั้ง รวมถึงการเตือนภัย ให้ความรู้และสร้างความตระหนักให้กับพนักงานผ่านการสื่อสารภายในองค์กร และ กปภ. ไม่มีเรื่องของการขายข้อมูลภายในเนื่องจากเราเน้นเรื่องคุณธรรมและจริยธรรมเป็นหลักให้กับพนักงาน นอกจากนี้ เราได้จัดทำเรื่องของการจัดลำดับชั้นในการเข้าถึงข้อมูล การกำหนดสิทธิ์การเข้าใช้ข้อมูลต่างๆในองค์กร มีแนวทางเรื่องของการยืนยันตัวตน เรื่องของ PDPA ของลูกค้า เรากำลังดำเนินการอยู่ในด้านการทำธุรกรรมของ กปภ. ซึ่งเดิมเราให้ลูกค้ายืนยันตัวตนด้วยอีเมล แต่เข้าใจว่าลูกค้าบางคนไม่มีอีเมล เราก็จะแนะนำให้ลูกค้า

เดินทางมาที่สาขา ซึ่งเรามีบริการแนะนำวิธีการสมัครอีเมลและดาวน์โหลด application ที่สาขาเพื่อป้องกันไม่ให้ลูกค้าถูกมิจฉาชีพหลอกลวง”

(ผู้ให้ข้อมูลสำคัญที่ 1, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

“กปภ. มีการจัดทำนโยบายด้านสารสนเทศของการประปาส่วนภูมิภาค มีการปรับปรุงนโยบายทุกๆปี โดยเราจะดูในเรื่องของจุดอ่อนหรือช่องโหว่ที่มาจากคำแนะนำของ External audit และ Internal audit ผู้ปฏิบัติและผู้เกี่ยวข้อง รวมถึงศึกษานโยบายของหน่วยงานภาครัฐอื่นๆ นำมาปรับปรุงและแก้ไขทุกปีเพื่อให้ได้นโยบายที่ถูกต้องครบถ้วน กปภ. มีการจ้างบริษัทเข้ามาตรวจสอบช่องโหว่หรือเรียกว่า การทำ VA ในระบบสารสนเทศที่สำคัญ อย่างน้อยปีละ 1 ครั้ง หลังจากที่มีการประเมินช่องโหว่แล้ว หน่วยงานที่เป็นผู้ตรวจจะแจ้งผลการตรวจสอบช่องโหว่กลับมา และผมก็จะนำรายงานให้ผู้บริหารรับทราบและแจ้งหน่วยงานผู้ตรวจที่เป็นต้นสังกัดที่ดูแลโดยตรงรับทราบเพื่อดำเนินการแก้ไข หลังจากที่มีการแก้ไขในส่วนนั้นจะมีการแบ่งระดับของช่องโหว่ออกเป็นระดับสูง กลาง ต่ำ ซึ่งเราก็จะมีในเรื่องของข้อกำหนดอยู่แล้วว่า แต่ระดับจะต้องดำเนินการแก้ไขกี่วัน เพื่อให้เจ้าของระบบหรือผู้ดูแลระบบที่ดำเนินการแก้ไขและตรวจดูว่าช่องโหว่นั้นยังอยู่ไหม”

(ผู้ให้ข้อมูลสำคัญที่ 2, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

“มีหน่วยงานฝ่ายบริหารความเสี่ยงจัดทำเรื่อง BCM ทั้งนี้ด้านหน่วยงานไอทีไปสนับสนุนด้านความเสี่ยงเช่น ระบบการควบคุมการจ่ายน้ำ และมีการประเมินความเสี่ยงระบบไอทีที่เค้าใช้งานอยู่ว่า ถ้าเกิดเหตุการณ์ด้านความเสี่ยง ไอทีจะมีวิธีการจัดการความเสี่ยงอย่างไร อีกทางคือไอทีประเมินเองจากการทำแผน ISO27001 และเรามี Internal Audit ด้าน IT ตรวจสอบอีกครั้งนึง ในเรื่องของ open data และ PDPA เราก็จะดูในกฎหมายลูก เราก็จะทำหน้าที่ในด้าน data controller ต้องมีการกำกับดูแลข้อมูลที่เหมาะสมให้กับองค์กร มีคู่มือในการบริหารจัดการ”

(ผู้ให้ข้อมูลสำคัญที่ 3, สัมภาษณ์เมื่อวันที่ 30 มีนาคม 2566)

*“มีการนำกรอบของ กฟภ. มาใช้ โดยมี 3 ขั้นตอนหลักๆคือ ป้องกัน ตรวจสอบ recovery แต่ได้นำกรอบ NIST มาใช้ เป็น 5 ขั้นตอน ซึ่งเป็นกรอบที่นำมาดำเนินการให้ครอบคลุมตามมาตรฐาน แต่ในหลักการย่อยอาจจะมีข้อแตกต่างอยู่บ้าง จึงไม่ได้ดำเนินการตาม NIST แบบ 100% และมีการใช้ พ.ร.บ. ไซเบอร์ มาดำเนินการเป็นกรอบใหญ่ เรามีหน่วยงานด้านความเสี่ยงองค์กร และหน่วยงานความเสี่ยงด้านไอที น่าจะลักษณะเดียวกันกลับการประปาส่วนภูมิภาค จะดูแลกระบวนการผ่าน ISMS ซึ่งหลักการจริงๆจะเป็น Information risk management ดำเนินการผ่าน ISO27001 มีบอร์ดด้านความเสี่ยงทั้งขององค์กรและไอที ซึ่งเวลาจะมีการประเมินในภาพใหญ่ขององค์กร จะครอบคลุมถึงงานด้านไซเบอร์ไว้ด้วย สำหรับการไฟฟ้า มีความเสี่ยงด้านองค์กรทุกปี ถึงแม้จะเป็นความเสี่ยงที่ไม่รุนแรง แต่อยู่ในระดับองค์กร มีการรายงานด้าน cybersecurity กับบอร์ดเสี่ยงและควบคุมภายในและบอร์ดดิจิทัล ทุกๆ 3 เดือน ซึ่งใน 24*7 จะทราบว่าว่าเราโดน challenge เท่าไหร่ และ Incident เท่าไหร่ มีการแจ้งเคสไปเท่าไหร่ เคสที่เปิดมีการ close case เท่าไหร่ มี Progress เท่าไหร่ มีปัญหาและอุปสรรคอะไรบ้าง”*

(ผู้ให้ข้อมูลสำคัญที่ 4, สัมภาษณ์เมื่อวันที่ 31 มีนาคม 2566)

“เรามีการดูแผนยุทธศาสตร์ชาติเพื่อให้มีความสอดคล้องกัน แต่เนื่องจากแผนยุทธศาสตร์ชาติค่อนข้างใหญ่ และอาจจะเกี่ยวข้องกับหลายๆคนและใน level ที่เกี่ยวข้อง คนที่เป็นแม่งานก็จะเป็นหน่วยงาน DE เราก็จะมีการติดตาม มีเรื่อง compliance ติดตามว่าในแง่งานต่างๆของเราจะสอดคล้องกับยุทธศาสตร์ตรงนั้นหรือเปล่า หรือมีอะไรที่เราสามารถไปเกี่ยวข้องได้ แต่อาจจะไม่ขนาด directly connect ในด้านความเสี่ยง เรามีฝ่ายบริหารความเสี่ยงด้านดิจิทัลโดยเฉพาะ จะมีการกำหนด framework ต่างๆ ในการจัดการบริหารความเสี่ยง มีการกำหนด KRI ในการชี้วัดตรวจสอบ ว่าเรามีอะไรผ่านเกณฑ์หรือไม่ หรือเกณฑ์อะไรที่เริ่มสูงเกินไปหรือต่ำเกินไปที่อาจจะ

สร้างความเสียหายให้เราหรือเปล่า ส่วนถ้าเป็นเรื่องย่อย ๆลงมาอีกคือถ้า KRI บางตัวอาจจะเกี่ยวข้องกับการตรวจสอบช่องโหว่ว่า ตอนนี้เรามีการปิดช่องโหว่ได้รวมเร็วทันเวลาหรือไม่ และเรามีการกำหนดว่าจะต้อง patch ถ้าเป็น critical patch จะต้องแพตซ์ภายใน 15 วัน แล้วเราจะทำได้ตามนั้นหรือไม่ แต่ก็มี patch ที่มี level ลงมาเป็น 30 วัน 60 วัน หรือไม่ก็จะเป็น indicator ตัวนึง ส่วนในภาพใหญ่เราก็จะมีการประเมินความเสี่ยงในภาพรวม และมี indicator ชี้วัดปรับปรุง นอกจากนี้ เราได้ทำแผนที่มีความสอดคล้องไปเรียบร้อยแล้ว ยกตัวอย่างข้อมูลส่วนบุคคล เราก็มีเจ้าหน้าที่ DPO ดูแลอยู่ ฝ่ายตรวจสอบก็จะมาตรวจสอบว่าเราได้ดำเนินการตาม พ.ร.บ. PDPA หรือไม่ หากมี GAP เค้าก็จะ Comments มา"

(ผู้ให้ข้อมูลสำคัญที่ 5, สัมภาษณ์เมื่อวันที่ 26 เมษายน 2566)

"เรามีคณะกรรมการ ในการกำกับในการปฏิบัติงานของเรา ซึ่งก็จะมีผู้บริหารตั้งแต่ระดับผู้อำนวยการฝ่ายไปถึงผู้อำนวยการในคณะต่างๆ รวมถึงมีท่านบอร์ดทางด้านไอที ซึ่งจะมาช่วยในการกำกับดูแลในเชิงกลยุทธ์และนโยบาย แผนการดำเนินการดิจิทัลต่างๆ และดำเนินการยุทธศาสตร์ให้สอดคล้องกับยุทธศาสตร์ขององค์กร ในการจัดการเรื่องของความเสี่ยง ธนาคารเองจะมีเรื่องของการประเมินตนเอง ของแต่ละฝ่ายงานในการดูว่าภัยที่เกิดขึ้นของแต่ละหน่วยงานประกอบด้วยอะไร นอกจากนี้เรายังมีการประเมินในระดับองค์กรเพื่อที่จะดูว่าภัยภายในและภายนอกเป็นอย่างไรบ้าง ไซเบอร์ก็จะเป็นประเภทหนึ่งที่ธนาคารเป็นตัวแทนหนึ่งในการเข้าไปประเมินในส่วนของภัยไซเบอร์ภาคองค์กรในระดับภาคใหญ่ ส่วนเรื่องของการสแกนช่องโหว่เนี่ยเราจะมีการสแกนช่องโหว่เป็นประจำอยู่เสมออยู่แล้ว ก็คือทุกระบบงานนะคะจะมีการสแกนอย่างน้อยปีละ 1 ครั้งนะคะ ทั้งนี้นอกจากช่องโหว่แล้วก็ยังมีการทดสอบในเรื่องของการทำแพนเทสด้วย สำหรับระบบงานที่เป็นระบบงานสำคัญแล้วก็เป็นระบบงานที่เป็น internet fasting"

(ผู้ให้ข้อมูลสำคัญที่ 6, สัมภาษณ์เมื่อวันที่ 28 เมษายน 2566)

“ตามมาตรการประเมินและพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาล มีการประเมินผลการดำเนินงานตามหลักการ PDCA และ IT Risk Management เพื่อตรวจสอบช่องโหว่และความเสี่ยง รวมถึงมีแผนกลยุทธ์ด้านการจัดการความเสี่ยง ไปจนถึงการควบคุมและปรับปรุงตามกรอบแนวคิดด้าน Cybersecurity ของกระทรวงสาธารณสุข”

(ผู้ให้ข้อมูลสำคัญที่ 7, สัมภาษณ์เมื่อวันที่ 26 พฤษภาคม 2566)

(2) มาตรฐานและมาตรการเฝ้าระวังภัยไซเบอร์

ตาม พ.ร.บ.รักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ได้กำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ รวมถึงส่งเสริมการรับรองมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) และให้คำนึงถึงมาตรการในการประเมินความเสี่ยงที่อาจจะเกิดขึ้น มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ และมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ เพื่อให้รับมือกับภัยคุมคามทางไซเบอร์ได้ทันท่วงที และตามมาตรา 58ซึ่งสอดคล้องกับผู้ให้ข้อมูลสำคัญ ดังนี้

“สำหรับตัวแนวทางการตั้งศูนย์ปฏิบัติการไซเบอร์เพื่อ หรือศูนย์ SOC เฝ้าระวังและตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์เรายึดตามแบบมาตรฐานสากล ไม่ว่าจะเป็น ISO27001 หรือว่าจะเป็น NIST ที่เป็นมาตรฐานด้าน cyber security เนื่องด้วยตอนนี้เรามีเจ้าหน้าที่ที่ดูแลไม่เพียงพอกับงาน เราจึงมีการว่าจ้างหน่วยงานภายนอกที่เรียกว่าเป็นศูนย์ SOC เป็นผู้ดูแลหรือเฝ้าระวังให้ในกรณีเกิดเหตุการณ์ต่างๆขึ้น ศูนย์ SOC ก็จะแจ้งมายังการประปาส่วนภูมิภาคให้รับทราบแล้วก็รีบดำเนินการแก้ไข ในส่วนของ พรบ การรักษาความมั่นคงปลอดภัยไซเบอร์ 2562 หรือ cyber security ในส่วนนี้ทางผมได้ดำเนินการโดยยึดตัวนี้เป็นหลัก ว่าสิ่งที่การประปาจะต้องดำเนินการให้สอดคล้องทุกมาตราในฐานะที่เราเป็นหน่วยงาน 1 ใน CII ให้ครบถ้วนถูกต้องและสมบูรณ์ เราได้ดำเนินการโดยเรามีที่ปรึกษาเป็นผู้ช่วยเหลือและให้ข้อแนะนำในการปรับปรุงในส่วนที่การ

ประปาส่วนภูมิภาคจะต้องดำเนินการ และเราก็จะเรียนแจ้งให้ทางผู้บริหารรับทราบว่าผลการดำเนินงานเป็นระยะๆ”

(ผู้ให้ข้อมูลสำคัญที่ 2, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

“นำความรู้ที่ได้จากการค้นคว้าวิจัยเรื่องโฟดูโมเดล (Purdue model) มาปรับใช้โดยโรงงานผลิต เพื่อที่จะลดค่าใช้จ่ายในการซ่อมบำรุงต่างๆ โดยทางผู้บริหารได้วิเคราะห์และจัดทำเป็นมาตรฐานให้ทั้งด้าน OT ฝั่งโรงงานผลิตเรียกว่า Operation technology เช่น IoT Device ต่างๆ และกับทาง IT ต้องไปด้วยกัน เพื่อไม่ให้งานติดขัดและสามารถใช้ร่วมกันได้ และจะมีฝั่ง Security network ซึ่งจะเป็น part นึง เช่น SCADA ส่วนฝั่งไอทีเราจะเรียกว่า Data network Data logger นอกจากนี้ กปน ได้อ่านงานวิจัยโฟดูโมเดล เพื่อจะดำเนินงานไปพร้อมกันกับ NIST เพื่อจะสร้างเป็น standard ให้กับองค์กร มีการทำเป็น controller และ workflow กปน มีกระบวนการ security ที่เรียกว่า CIA Identify Detect Protect ซึ่ง Identify คืออุปกรณ์ใน Network และ Network function ที่ต้องทำได้คือการ Detect เพื่อ Detect device ที่เข้ามาว่าเป็น member เราจริงๆหรือไม่ และเค้าจะไปคุยกับ Access control ที่เราตั้งไว้ ซึ่งเราจะดูจาก profile ที่เค้าเป็น member เราก็นำหลักการมาจากงานวิจัยชิ้นนี้ เรานำมาถอด level ออกมา decide และเรากำลังจะทำ smart meter ซึ่งนำมาปรับและออกแบบที่เป็นของเราเอง”

(ผู้ให้ข้อมูลสำคัญที่ 3, สัมภาษณ์เมื่อวันที่ 30 มีนาคม 2566)

*“เรามีศูนย์ SOC คือ 24*7 แบบ Hybrid คือ ทั้งเป็นความร่วมมือระหว่าง กฟภ. และ outsource แต่ตลอดระยะเวลาที่ทำมาหลาย 10 ปี ภาครัฐจะมีข้อจำกัดอย่างหนึ่งคือ เราถูกจำกัดเรื่องงบประมาณ การได้มาเรื่องกระบวนการจัดซื้อจัดจ้าง ซึ่งปัญหาและอุปสรรคอีกอย่างหนึ่งคือเรื่องการหลุดสัญญา โดยศูนย์ SOC ที่ กฟภ ดำเนินการอยู่ตอนนี้มีทีมงานอยู่จำนวน 4-5 คน และสัญญา Outsource ของเราหลุดจริง ซึ่งเรารู้ว่าเคสแบบนี้ถ้าหากไม่มีหน่วยงานมา Support แบบ 24*7 ในองค์กร ก็หมายความว่า จะไม่มี*

*คนดูแบบ 24*7 เลย เพราะฉะนั้นจากสถิติส่วนใหญ่ เราจะโดน attack ในตอนกลางคืน ซึ่งหลักการที่เราจะเฝ้าระวังภัยคุกคามได้ เราต้องมี 24*7 นั่นคือข้อดี ดังนั้นเราต้องมีการลงทุน เพราะเมื่อเทียบกับผลเสีย เทียบกับการทำผิดกฎหมาย ผมว่าค่อนข้างที่จะคุ้มค่ากว่า ในส่วนของ NIST ผมมองว่าผมไม่ได้เอา NIST เป็นมาตรฐาน แต่มองว่าเป็นแค่กรอบ NIST คือ CSF หรือ Cyber Security Framework หมายความว่า ถ้าคิดถึง Security framework ให้นึกถึงกรอบตัวนี้ และในส่วนของรายละเอียด ก็จะ vary and adjust ไปตามแต่ละองค์กร แต่ถ้าเป็น กฟภ. ฝั่ง IT ก็จะมี ISO 27001 แต่ถ้าฝั่ง OT อาจจะเป็นตัว NERC- CIP เป็นมาตรฐานจากอเมริกา"*

(ผู้ให้ข้อมูลสำคัญที่ 4, สัมภาษณ์เมื่อวันที่ 31 มีนาคม 2566)

*"เรามีศูนย์ SOC ของเราเอง ทำงานแบบ 24*7 มีการ monitor ตลอดเวลา มีการแบ่งเจ้าหน้าที่เป็น Tier one และ Tier two และ SOC Manager Tier one จะมีหน้าที่ monitor ว่ามี Alert อะไรหรือไม่ ถ้ามีอะไรที่ผิดปกติก็จะมีการเริ่มเก็บข้อมูลว่าเกิดอะไรขึ้น ถ้าเป็นเคสปัญหาจริงๆก็จะส่งต่อไปให้ Tier two เพื่อทำการวิเคราะห์ เช่น หากบางส่วนพบว่ามี malware file ก็จะแก้ปัญหาโดย Tier one จะแจ้ง Tier two ให้เข้าไปแก้ปัญหาที่ผิดปกติ ซึ่ง Tier one จะเป็น outsource เพราะว่าจะมีการทำงานแบบ 24*7 แต่ Tier two เป็นพนักงานของเราเอง และเรามีการใช้มาตรฐานสากล ISO27001 และถ้าไม่ใช่ที่เกี่ยวกับไซเบอร์ ก็จะมี ISO 22301 เรื่อง BCM มีมาตรฐานด้าน financial center ที่เป็นเครือข่ายด้านการเงิน"*

(ผู้ให้ข้อมูลสำคัญที่ 5, สัมภาษณ์เมื่อวันที่ 26 เมษายน 2566)

"เรามี SOC ของเราเองนะคะโดยที่ในการจัดการภัยไซเบอร์เราก็ทำตาม framework ของ nist นะคะทั้งในเรื่องของการ detect protect response recover นะคะ และมี ISO27001 และ DCIDSS ด้วยค่ะ จัดทำโดยหน่วยงานการกำกับดูแลอยู่แล้ว อย่างถ้าเกิดมีการเผยแพร่ เท่าที่เราจะเห็นก็จะมีเรื่องของการจัดซื้อจัดจ้าง สมมุติเรื่อง

ของการป้องกันข้อมูลหลุดออกไป จะมีโครงการเช่นการป้องกันข้อมูลรั่วไหลเช่นเครื่องมือในการใช้ก็คือเรื่องของ DLP ก็จะมีการจัดเครื่องมืออะไรประมาณนี้มา ในการจัดซื้อจัดจ้างประกาศออกไป”

(ผู้ให้ข้อมูลสำคัญที่ 6, สัมภาษณ์เมื่อวันที่ 28 เมษายน 2566)

“เราปฏิบัติตาม พ.ร.บ.ไซเบอร์ รวมถึงกำหนดมาตรการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นขั้นตอน ตั้งแต่การป้องกันความเสี่ยงด้านดิจิทัลตามมาตรฐาน Cybersecurity ขั้นพื้นฐาน การนำกรอบ NIST cyber security framework มาใช้ทั้งการ Identify Protect Detect Response และ Recovery มีการสำรวจ cybersecurity risk assessment มีการจัดทำแผนงบประมาณและแผนปฏิบัติการตามประมวลแนวปฏิบัติโดยทีมดิจิทัลเขตสุขภาพ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มีการเตรียมด้าน cybersecurity ในการติดตั้งระบบ SOC ปีแรกนำร่องโรงพยาบาล 15 แห่ง โดยมอบหมายเจ้าหน้าที่รับผิดชอบอย่างน้อย 2 คนต่อ 1 โรงพยาบาล”

(ผู้ให้ข้อมูลสำคัญที่ 7, สัมภาษณ์เมื่อวันที่ 26 เมษายน 2566)

(3) การประสานความร่วมมือและถ่ายทอดสื่อสารให้แก่ผู้มีส่วนได้ส่วนเสีย

การประสานงานการดำเนินงานเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศนั้น เป็นไปตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 52 ว่าด้วยเรื่องของประโยชน์ในการติดต่อประสานงาน โดยให้หน่วยงาน CII แจ้งรายชื่อและข้อมูลการติดต่อผู้ครอบครองคอมพิวเตอร์และผู้ดูแลระบบคอมพิวเตอร์ไปยังสำนักงาน หน่วยงานควบคุมหรือกำกับดูแลของตน เพื่อประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ รวมถึงมีการประสานงานและถ่ายทอดสื่อสารให้แก่ผู้มีส่วนได้ส่วนเสียภายในหน่วยงาน CII อาทิเช่น หน่วยงานที่เกี่ยวข้องเชิงภารกิจ ลูกค้า คู่ค้า/ผู้ส่งมอบ คู่ความร่วมมือ พนักงาน ชุมชนสังคม คู่แข่ง สื่อมวลชน เป็นต้น สอดคล้องกับผู้ให้ข้อมูลสำคัญ ดังนี้

“ในเรื่องของการร่วมมือและประสานงานคือ เรามีการร่วมมือประสานงานกันทางกระทรวงมหาดไทย ทางกระทรวงมหาดไทยก็เชิญ

การประปาส่วนภูมิภาคเข้าไปร่วมประชุมนะ เพื่อรับทราบข่าวสารและมีการชี้แจงเพื่อให้รับทราบว่าตอนนี้หน่วยงานใดบ้างที่อยู่ภายใต้สังกัดกระทรวงมหาดไทยที่พบเจอปัญหาหรือถูกโจมตี เพื่อให้หน่วยงานที่เกี่ยวข้องทั้งหมดรีบดำเนินการแก้ไขหรือทำการป้องกัน อย่างล่าสุดการประปาส่วนภูมิภาคได้ร่วมมือกับการไฟฟ้าส่วนภูมิภาค และเบื้องต้นได้ประสานงานและจัดทำหนังสือเชิญเพื่อให้การไฟฟ้าส่วนภูมิภาคเข้ามาประชุมร่วมกันในเดือนหน้าที่จะถึงนี้"

(ผู้ให้ข้อมูลสำคัญที่ 2, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

"ช่องทางในการเข้าร่วมกลุ่มและร่วมอบรมด้าน Cybersecurity กับ สกมช. และกำลังจะมีการเรียนเชิญ สกมช. มาให้ความรู้กับคณะกรรมการต่างๆที่เกี่ยวข้องด้านป้องกันและรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ของ กปน และทางผมมีส่วนได้เข้าไป Recommend กับทาง สกมช. นอกจากนี้เรามี คู่มือและมีการสื่อสารโดยเฉพาะในช่วงสถานการณ์โควิด เรามีทั้งการใช้ฮาร์ดแวร์และซอฟต์แวร์ ในการบริหารจัดการ เช่น มี VPN ที่ให้พนักงาน ใช้รีโมทเข้ามาทำงานจากที่บ้าน มี Tool factor คือ Token ที่ใช้ และส่วนใหญ่ กปน จะได้ Notebook สะส่วนใหญ่ เนื่องจากว่า ประการแรก เราจะนำตัว notebook เองมาทำการ Register ว่าเป็น Device ขององค์กร ประการที่สองคือ นำ Account ที่อยู่ใน HR อีกกลุ่มคือ AD เราจะให้ Create user เองและจะให้ทาง HR เป็นผู้ Generate account ดังนั้นทางเราเองจะไม่มีสิทธิ์ที่จะ generate account ให้ได้ และ account จะมาจาก HR แต่ทางไอทีจะเป็นผู้กำหนดสิทธิ์ให้ตามที่คณะกรรมการทำออกมา เช่น คณะกรรมการจะออกนโยบายให้ว่า user จะต้องมีการเปลี่ยน password ทุก 90 วัน เราก็จะมี deploy เพื่อที่จะ Enforce ให้เค้าว่าต้องเปลี่ยน Password เมื่อครบกำหนดการใช้งาน 90 วัน พนง ก็จะปฏิบัติตามระเบียบของ กปน."

(ผู้ให้ข้อมูลสำคัญที่ 3, สัมภาษณ์เมื่อวันที่ 30 มีนาคม 2566)

“มีคู่มือในทุกกระบวนการและในส่วนของด้าน risk management ที่ไม่ใช่แค่ IT แต่เราถ่ายทอดสื่อสารให้ด้าน OT/ICS นำไปใช้ด้วย”

(ผู้ให้ข้อมูลสำคัญที่ 4, สัมภาษณ์เมื่อวันที่ 31 มีนาคม 2566)

“ในด้านความร่วมมือระหว่างหน่วยงานมีประสิทธิภาพอยู่ในระดับที่เพียงพอ เช่น เราได้มีการติดต่อสื่อสารกันกับ สกมช. คือถ้ากรณีมี incidents ต่างๆ เราก็จะเข้าไปคุยกับเค้า ในส่วนของแบงก์ชาติเองเป็นทั้งฝ่าย regulator และหน่วยรับบริการ ในส่วนหน่วยรับบริการก็จะเป็นหน่วยงานด้านการเงินการธนาคาร แต่โดยส่วนใหญ่หน่วยงานเหล่านี้จะไม่มีประกาศออกมาเนื่องจากเกรงว่าจะเป็นเป้าหมายในการโจมตีทางไซเบอร์ ในด้านการสื่อสารมีการจัดทำแผนงานประจำปี และมีการประเมินแผนงานว่าจัดทำแล้วได้อะไร คุ้มกับค่าใช้จ่ายที่สูญเสียไปหรือไม่ เป็นการคุยในรูปแบบจัดประชุมกับผู้ที่เกี่ยวข้องก่อนจะได้รับอนุมัติให้เผยแพร่ มีการนำคู่มือต่างๆมาใช้ เช่น คู่มือ BCP จะมีการนำมาทดสอบทุกปี ว่าจะต้องทำอะไรบ้างตามคู่มือเหล่านี้ นอกจากนี้ก็จะมีกระบวนการต่างๆที่เกี่ยวข้องกับกระบวนการด้านไอทีทั้งหมด ก็จะมีเขียนเอาไว้ว่าแต่ละกระบวนการต้องมีกรอบมีคู่มือที่เกี่ยวข้องและมีการสื่อสารอะไรกับใครที่เกี่ยวข้องบ้าง โดยเราใช้เป็น swim lane ในการจัดทำกระบวนการ”

(ผู้ให้ข้อมูลสำคัญที่ 5, สัมภาษณ์เมื่อวันที่ 26 เมษายน 2566)

“ในมุมมองว่าการประสานงานและความร่วมมือระหว่างหน่วยงานมีประสิทธิภาพเพียงพอ เพราะว่า เราเป็นหนึ่งในสมาชิกของ TB-CERT เพราะฉะนั้นหากเกิดเหตุใดๆก็ตามหรือสิ่งใดก็ตามเนี่ยก็จะมีสมาคมสิ่ง TB-CERT จะเป็นตัวกลางในการประสานงานระหว่างเราและทางแบงก์ชาติ ซึ่งก็จะมีการแชร์ข้อมูลกันอยู่แล้ว เวลาเกิดเหตุก็จะมีการติดต่อโดยตรงกับทางทั้งสอง สกมช. และก็ทางแบงก์ชาติ ถ้าเป็นของ สกมช. คือจะมีเกณฑ์ไว้อยู่แล้วว่าเกิดเหตุการณ์ที่รุนแรงนอกจากที่เราแจ้ง สกมช. เราจะต้องแจ้งแบงก์ชาติด้วย อันนี้คือเป็น

ทางด้านกฎหมายระบุไว้เช่นนั้นในระดับที่มีผลกระทบรุนแรง แบงก์ชาติเองเขาก็จะตั้งเกณฑ์เอาไว้อยู่แล้วว่าถึงแม้ไม่รุนแรงก็มีช่องทางในการแจ้งเหตุกับเขาที่เรียกว่า event report ของทางแบงก์ชาติที่ประกาศอยู่ในหน้าเว็บไซต์ ธปท. หลังจากที่เรามีการจัดทำแผนตอบสนองภัยไซเบอร์ซึ่งเราก็จะมีเหมือนกับผ่านมาตรฐานของ ISO มีการทบทวนครั้งแล้วก็แจ้งให้ผู้ที่เกี่ยวข้องผู้มีส่วนได้ส่วนเสียที่อยู่ในแผนมาร่วมดำเนินการทดสอบอย่างน้อยปีละ 1 ครั้ง และในทุกๆ 3 ปี จะมีการขยายผลในการทดสอบเป็น Bank wide (แบบกว้าง) คือ เราจะมีการทดสอบ โดยธนาคารจะมีการกำหนดโดยแบงก์ชาติว่า จะมีการทดสอบกันเป็นวงกว้างคือทั่วทั้งธนาคาร จะได้ร่วมทดสอบ Bank wide นี้ซึ่งระบบ scenario ทดสอบที่ถูกกำหนดขึ้นมาในทุกๆ 3 ปี เช่นกัน เพื่อให้แต่ละคนได้ทราบบทบาทหน้าที่ของตนเอง จะได้รู้ว่าช่องทางการสื่อสารที่กำหนดไว้ในแผน สามารถที่จะดำเนินการได้หรือไม่อย่างไร หลังจากที่ดำเนินการทดสอบก็จะมีการนำผลที่ได้จากการทดสอบมาปรับปรุงแผนให้เป็นปัจจุบันและให้สอดคล้องกับเหตุการณ์”

(ผู้ให้ข้อมูลสำคัญที่ 6, สัมภาษณ์เมื่อวันที่ 28 เมษายน 2566)

“มี Health CIRT หรือ Health Cyber Incident Response Team คือ ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งมีหน้าที่ในการประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ให้แก่หน่วยงาน CII และคอยให้การสนับสนุนหรือปฏิบัติงานร่วมกับสำนักงานหน่วยงานควบคุมหรือกำกับดูแล พนักงาน เจ้าหน้าที่ตาม พ.ร.บ.ไซเบอร์ ปี 2562”

(ผู้ให้ข้อมูลสำคัญที่ 7, สัมภาษณ์เมื่อวันที่ 26 พฤษภาคม 2566)

(4) การติดตามและประเมินผลลัพธ์

ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 54 กำหนดให้หน่วยงาน CII ต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจประเมินของหน่วยงานนั้นๆ และต้องให้มีการตรวจสอบด้านความมันคงปลอดภัยไซ

เบอร์โดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบอิสระภายนอกด้านความมั่นคงปลอดภัยสารสนเทศ อย่างน้อยปีละ 1 ครั้ง โดยหลังจากการประเมินแล้วเสร็จ หน่วยงาน CII ต้องจัดส่งผลสรุปรายงานการดำเนินการต่อสำนักงาน สกมช. ภายใน 30 วันนับตั้งแต่วันที่ดำเนินการแล้วเสร็จ ซึ่งจากการสัมภาษณ์หน่วยงาน CII ทุกหน่วยงานได้ให้ความสำคัญและดำเนินการตามที่กฎหมายกำหนด นอกจากนี้ หลายองค์กรมีการกำหนดตัวชี้วัดของกระบวนการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์เพื่อการพัฒนาและปรับปรุงการปฏิบัติงานในปีถัดไปให้เป็นไปตามแผนปฏิบัติการดิจิทัลของแต่ละองค์กร ซึ่งสอดคล้องกับผู้ให้ข้อมูลสำคัญ ดังต่อไปนี้

> *“ในส่วนของการกำหนดตัวชี้วัดในเรื่องของการดำเนินการโดยมีการรายงานให้ผู้บริหารรับทราบว่า ในเหตุการณ์ผิดปกติหรือ Incident ที่เกิดขึ้น จะต้องดำเนินการแก้ไขให้เสร็จภายในระยะเวลาเท่าไหร่ และจะต้องดำเนินการให้แล้วเสร็จทั้งหมด 100% ของการประเมินของหน่วยงานทุกปี โดยการปรับปรุงตัวชี้วัดให้ให้มีความท้าทายในเรื่องระยะเวลาแก้ไขที่เรากำหนดในตัวชี้วัด และจะมีผลต่อการประเมินผลรัฐวิสาหกิจจากสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจทุกปี”*
>
> (ผู้ให้ข้อมูลสำคัญที่ 2, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

> *“1. .มีตัวชี้วัดที่ขึ้นอยู่กับมิติที่จะประเมินเค้า เช่น เรื่องของเวลาในการแก้ไขปัญหาการแฮกว่าสามารถกลับมาใช้งานได้ปกติและเรื่อง Audit แต่ขอเอกสารจาก Outsource ด้าน SOC 2. ด้านไอทีเองก็จะมีเรื่องของ การ Attack เรามีการเก็บ log และจะมี Audit มาตรวจสอบ log ที่เรามี นอกจากนี้ มีรายงานภัยคุกคามการโจมตีภัยคุกคามทางไซเบอร์ มีรายละเอียดผลกระทบ ระดับ สูง ปานกลาง ต่ำต่อคณะกรรมการด้านรักษาความมั่นคงปลอดภัย ในรูปแบบแบบฟอร์มบทวิเคราะห์ทางไซเบอร์ (incident summary) การตรวจเช็คระดับความรุนแรง มี Response มีสถานการณ์ตรวจสอบและมีการ Recovery ทั้งด้าน Software และ Hardware ซึ่งถอดมาจาก NIST 1.1”*
>
> (ผู้ให้ข้อมูลสำคัญที่ 3, สัมภาษณ์เมื่อวันที่ 30 มีนาคม 2566)

“มีตัวชี้วัดด้าน management ตัวชี้วัดด้านการป้องกันการบุกรุก ว่าในหนึ่งปีต้องป้องกันไม่เกินเท่าไหร่ มีตัวชี้วัดด้านความพร้อมใช้ เป็นจำนวนชั่วโมงรวม Downtime”

(ผู้ให้ข้อมูลสำคัญที่ 4, สัมภาษณ์เมื่อวันที่ 31 มีนาคม 2566)

“เราจะมีหมวดของ KRI คือหมวด third party management ซึ่งจะมีการประเมินว่า Third Party ที่เราใช้งานอยู่มีความเสี่ยงหรือไม่ และ ของ ธปท. เอง patch ต่างๆมีการปิดช่องโหว่ทันเวลาหรือไม่”

(ผู้ให้ข้อมูลสำคัญที่ 5, สัมภาษณ์เมื่อวันที่ 26 เมษายน 2566)

“ในแต่ละแผนงานโครงการจะมีแบบฟอร์มให้ระบุเรื่องของ output outcome ระยะเวลาในการดำเนินการ ได้อย่างชัดเจนรวมถึงเรามีสายงานที่เรียกว่าฝ่ายบริหารงานโครงการนะคะเขาจะเป็นผู้ติดตามผลการดำเนินการงานแล้วก็ระยะเวลาที่มีความเหมาะสมแล้วก็ output outcome เหล่านั้นนะคะว่าเป็นไปตามข้อตกลงหรือไม่ซึ่งเราก็จะมีเรื่องของแผนเหล่านี้อาจจะเป็นตัวชี้วัดหน่วยงานซึ่งองค์กรจะเป็นคนวัดเราด้วยเช่นกัน ในเรื่องของตัวชี้วัด ยกตัวอย่าง โครงการ DLP เราก็จะมีการวัดว่า เราสามารถทำแผน TOR ได้ภายในเดือนมิถุนายน หลังจากนั้นจะมีการประกาศร่างและจัดซื้อจัดจ้างให้ได้ภายในเดือนพฤษภาคม จากนั้นจะมีการติดตั้งและใช้งานได้ในเดือนธันวาคม เป็นขั้นตอนตั้งแต่เริ่มทำ TOR จนกระทั่งติดตั้งใช้งาน”

(ผู้ให้ข้อมูลสำคัญที่ 6, สัมภาษณ์เมื่อวันที่ 28 เมษายน 2566)

“ตามเป้าหมายโรงพยาบาลในสังกัดกระทรวงสาธารณสุขมีโครงสร้างเทคโนโลยีสารสนเทศที่มั่นคงและมีข้อมูลที่ปลอดภัย โดยมีตัวชี้วัดคือ จำนวนโรงพยาบาลในสังกัดกระทรวงสาธารณสุขที่มีการปรับโครงสร้างเทคโนโลยีสารสนเทศให้มั่นคงและปกป้องข้อมูลอย่างปลอดภัย ตามหลักยุทธศาสตร์และมาตรการคือ 1. การปรับโครงสร้าง

เทคโนโลยีสารสนเทศให้มั่นคง 2. การสร้างมาตรการปกป้องข้อมูลอย่างปลอดภัย 3. การสร้างระบบเฝ้าระวังความปลอดภัยของข้อมูลจากภัยคุกคาม cyber โดยวัดระดับความสำเร็จรายไตรมาสในแต่ละปีงบประมาณ"

(ผู้ให้ข้อมูลสำคัญที่ 7, สัมภาษณ์เมื่อวันที่ 26 พฤษภาคม 2566)

4.4.1.2 การรับมือของหน่วยงานด้านการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์

(1) การกำกับดูแลและบริหารความเสี่ยง

ตามมาตรา 59 ใน พ.ร.บ.รักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ส่วนที่ 4 เรื่องการรับมือภัยคุกคามทางไซเบอร์ ได้บัญญัติถึงหน่วยงานควบคุมหรือกำกับดูแล ไว้ว่า ในกรณีที่มีการรับแจ้งเหตุการณ์ภัยคุกคามทางไซเบอร์จากหน่วยงาน CII ให้หน่วยงานควบคุมหรือกำกับดูแลร่วมกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (NCERT) รวบรวมข้อมูล ตรวจสอบ วิเคราะห์สถานการณ์ และประเมินผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์ โดยสนับสนุนและช่วยเหลือหน่วยงาน CII ในการป้องกันและรับมือ เพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมทั้งให้แจ้งเตือนหน่วยงานของรัฐและหน่วยงาน CII ที่อยู่ในการควบคุมดูแลของตน ตลอดจนหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานของรัฐหรือหน่วยงาน CII อื่นที่เกี่ยวข้องโดยเร็ว ซึ่งสอดคล้องกับผู้ให้ข้อมูลสำคัญ ดังนี้

"ในแง่ของกฎหมายไซเบอร์ เรามีแผนที่มีการออกกฎหมายรวมถึงการควบคุมกำกับโดยใช้กลไกตาม พ.ร.บ. ไซเบอร์ เป็นประจำอยู่แล้วในแต่ละปีงบประมาณ มีแผนปฏิบัติการที่เกี่ยวข้องกับเรื่องของมาตรการเหล่านี้ออกไป จะมีการให้หน่วยงานโดยเฉพาะหน่วยงานที่เป็น CII จะมีการประเมินความเสี่ยง ซึ่งในมาตรการการควบคุมหน่วยงานที่ใกล้ชิดที่สุดที่เข้าใจ Business ของหน่วยงาน CII ถือกฎหมายที่มีความเกี่ยวข้องกับ CII นั้นโดยตรง ได้แก่ หน่วยงานควบคุมกำกับดูแล เป็นผู้ที่จะเข้าไปมีส่วนร่วมในการประเมินความเสี่ยงตรงนี้ อีกส่วนหนึ่งก็คือ มาตรการควบคุม ยังมีข้อกฎหมายที่หน่วยงาน CII ต่างๆเหล่านี้จะต้องมีการตรวจสอบงานโดยผู้ตรวจสอบอิสระไม่ว่าจะเป็นภายในหรือภายนอกก็ตามอย่างน้อยปีละครั้ง ดังนั้นเรื่องของการประเมินความเสี่ยงแล้วก็มีมาตรการควบคุมในการ

ตรวจสอบ ก็จะเป็นหนึ่งในกลไกที่ทำให้หน่วยงานต่างๆ ลดความเสี่ยงในการถูกโจมตีได้"

(ผู้ให้ข้อมูลสำคัญที่ 8, สัมภาษณ์เมื่อวันที่ 27 มีนาคม 2566)

"สพร. เองมีการกำหนดค่าความเสี่ยง จริงๆแล้วในหน่วยงานภาครัฐทุกหน่วยงาน ควรจะมีการทำ risk continual เพราะว่าสุดท้ายองค์ความเสี่ยงที่มองจากในสำนักงาน คงไม่ไปมองในมุมเหมือน พ.ร.บ. ไซเบอร์ 2562 ยกตัวอย่าง เว็บไซต์ ในมุมของหน่วยงานก็ถือว่า critical แล้ว แต่ถ้าถามว่า สพร เคยเจอเหตุการณ์ที่มีความรุนแรงในการโจมตีระดับ critical หรือไม่ ก็เคยมีแต่เรา response ทันจนผลกระทบดังกล่าวเป็นอยู่ในเกณฑ์ที่ยอมรับได้ของสำนักงานอยู่แล้ว"

(ผู้ให้ข้อมูลสำคัญที่ 9, สัมภาษณ์เมื่อวันที่ 30 มีนาคม 2566)

"สวทช. มีแนวทางการด้าน security ที่ดีที่สุด เช่น ISO27001 และ PDPA และ Data governance มีการสอบเทสอยู่เสมอ มีการทำโครงการ มีการบรรยาย และล่าสุด สวทช ได้รับรางวัล security จาก สกมช. แต่สิ่งที่ สวทช. สู้ไม่ได้คือหน่วยงาน CII เนื่องจาก สวทช. เป็นหน่วยงานทางด้านวิจัย และคงไม่สำคัญเทียบเท่ากับธนาคาร อีกทั้ง สวทช. เป็นหน่วยงานภาครัฐ เรื่องงบประมาณก็ไม่เพียงพอเท่าหน่วยงานด้านการเงินอย่างธนาคาร ส่วนในเรื่องการบริหารจัดการความเสี่ยงด้านเทคโนโลยี มองว่าเรื่องของพื้นฐานสำคัญของหลักความมั่นคงและปลอดภัยทางไซเบอร์ คือหลักการ CIA Confidentiality Integrity Availability เป็นเรื่องที่สำคัญ นอกจากนี้ต้องมีการจัดทำแบบยั่งยืนและมีการสนับสนุนด้านงบประมาณประจำปี ที่ไม่ใช่ Ad hog ไม่ใช่มองเป็นเรื่องโครงการหรือปีถัดไปต้องจัดสรรเป็นงบพิเศษ แต่ต้องเป็นงบที่อยู่ในแผนทุกปี และควรจะต้องตั้งเป็นคณะกรรมการในการบริหารจัดการ"

(ผู้ให้ข้อมูลสำคัญที่ 10, สัมภาษณ์เมื่อวันที่ 27 มีนาคม 2566)

“พ.ร.บ. ไซเบอร์ ปี 2562 บังคับว่าให้ทุกหน่วยงานต้องปฏิบัติตาม พ.ร.บ. ว่าจะต้องมีการตรวจสอบ มีนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ของทุกหน่วยงาน โดยเค้าได้กำหนด criteria ลักษณะของหน่วยงานออกมา 3 ลักษณะ คือ 1. หน่วยงานกำกับดูแล 2. หน่วยงานโครงสร้างพื้นฐาน 3. หน่วยงานของรัฐ ซึ่งถ้าหน่วยงานของรัฐยังไม่พร้อมที่จะเป็นหน่วยงานโครงสร้างพื้นฐาน ก็จะไม่มีการบังคับว่าจะต้องเปลี่ยนเป็นหน่วยงานโครงสร้างพื้นฐานเมื่อไหร่ แต่ว่าหน่วยงานของรัฐจะต้องปฏิบัติตาม พ.ร.บ. ไซเบอร์ 2562 ด้วยในเรื่องที่กำหนดให้มีนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ และจะต้องมีการตรวจสอบกับหน่วยงานภายนอกด้วย โดยสรุปคือทุกหน่วยงานต้องปฏิบัติตาม พ.ร.บ. ไซเบอร์ 2562 ให้เป็นไปตามเกณฑ์การบริหารจัดการของภาครัฐ ซึ่งเกณฑ์ที่กล่าวถึงนี้คือมาจาก สกมช. ในส่วน สมช. เรามีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศปี 2565 แต่นโยบายตัวนี้ไม่มีตัวชี้วัด เพราะส่วนใหญ่จะมีเรื่องของการวิเคราะห์ system เช่น การเข้าตรวจคอมพิวเตอร์ต้องทำอย่างไรบ้าง การรักษาสภาพ การตรวจสอบจากบุคคลภายนอกต้องทำทุกปี อันนี้ก็จะกำหนดให้เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศจะต้องปฏิบัติตาม รวมทั้งเพื่อเป็นรายละเอียดให้เจ้าหน้าที่ สมช เรียนรู้และรับทราบว่าเราจะรักษาความมั่นคงปลอดภัยในคอมพิวเตอร์ที่ตัวเองใช้ยังไง นอกจากนี้เราก็จะมียุทธศาสตร์ชาติ 20 ปี นโยบายและแผนที่เป็นระยะเร่งด่วน 5 ปี นโยบายและแผนปฏิบัติการระดับชาติว่าด้วยความมั่นคงปลอดภัยไซเบอร์ ซึ่งแต่เดิมเป็นของ สมช หลังจาก มติ ครม. ปี 2562 ก็เปลี่ยนไปมอบให้ สกมช.”

(ผู้ให้ข้อมูลสำคัญที่ 11, สัมภาษณ์เมื่อวันที่ 19 เมษายน 2566)

“มีหน่วยงาน สกมช. เข้ามาตรวจสอบและแจ้งกระทรวงมหาดไทย และมหาดไทยแจ้งไปยังหน่วยงานท้องถิ่น เทศบาล อบจ. อบต. เพื่อตรวจหาภัยคุกคามและการโจมตีทางไซเบอร์โดยเฉพาะเรื่องการเจาะระบบ และหน่วยงานท้องถิ่นเองก็มีการแจ้งด้านภัยคุกคามทางไซเบอร์มายังกระทรวงมหาดไทยเช่นกัน”

(ผู้ให้ข้อมูลสำคัญที่ 13, สัมภาษณ์เมื่อวันที่ 25 เมษายน 2566)

“การจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัลขององค์กร นั้น สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม มีการกำหนดนโยบายรวมถึงแนวปฏิบัติที่อ้างอิงตามหลักมาตรฐานสากล (ISO27001:2013) รวมถึงการดำเนินการตามกฎหมายที่เกี่ยวข้อง ไม่ว่าจะเป็นพ.ร.บ.ธุรกรรมทางอิเล็กทรอนิกส์ฯ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ เป็นต้น มีการกำหนดแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กรเพื่อประเมินความเสี่ยงที่เกี่ยวข้องรวมถึงการบรรเทาความเสี่ยงเพื่อให้อยู่ในเกณฑ์ที่รับได้ โดยได้รับความร่วมมือจากหน่วยงานภายในสังกัดในการดำเนินการดังกล่าว ทั้งนี้ มีคณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นผู้ผลักดันการดำเนินการดังกล่าว มีการประเมินระดับความเสี่ยงด้านไซเบอร์และการบริหารความเสี่ยงด้านไซเบอร์ของสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ปีละหนึ่งครั้ง โดยมีขั้นตอนการประเมินความเสี่ยงดังนี้ 1. ระบุความเสี่ยง พิจารณาปัจจัยในการประมาณความน่าจะเป็นซึ่งมีความเกี่ยวข้องกับตัวภัยคุกคาม 2. ปัจจัยในการประเมินผลกระทบการท างานของระบบสารสนเทศแต่ละระบบของ สป.ดศ. 3. ก าหนดความรุนแรงของความเสี่ยงที่อาจส่งผลกระทบต่อระบบสารสนเทศ 4. จำลองการประเมินความเสี่ยง/การจัดลำดับความเสี่ยง และ 5. พิจารณาว่าจะแก้ไขช่องโหว่ที่เกิดขึ้นอย่างไร”

(ผู้ให้ข้อมูลสำคัญที่ 14, สัมภาษณ์เมื่อวันที่ 18 เมษายน 2566)

“มีกระบวนในการจัดทำแนวนโยบายการกำกับดูแลเรื่องความมั่นคงปลอดภัยไซเบอร์เป็นการเฉพาะเรื่อง และแนวปฏิบัติในด้านความมั่นคงปลอดภัย ที่มีการจัดทำและปรับปรุงทุกๆปี เชื่อมโยงกับ user และเจ้าหน้าที่รับผิดชอบด้านนี้ โดยจะต้องตรวจสอบว่า

ระบบที่เรามีอยู่ มีช่องโหว่หรือไม่และถ้ามีจะต้องปิดช่องโหว่นั้นให้เรียบร้อย เว้นเสียแต่ว่าบางเรื่องอาจจะปิดไม่ได้ และต้องมาตรวจสอบว่าปิดไม่ได้เพราะเหตุใด หรือถ้าปิดแล้วจะมีปัญหาอะไรตามมาหรือไม่ และต้องดูว่าร้ายแรงขนาดไหน ซึ่งใน 1 ปี จะมีการจ้าง outsource ที่ตรวจสอบระบบจากภายนอก และจะมีการทำ report ออกมาว่าได้ตรวจสอบอะไรไปบ้าง และจะทำการสแกนซ้ำปีละ 1 ครั้ง นอกจากนี้จะมีการทำ VA สแกนช่องโหว่ปีละ 2 ครั้ง"

(ผู้ให้ข้อมูลสำคัญที่ 15, สัมภาษณ์เมื่อวันที่ 29 มีนาคม 2566)

(2) มาตรฐานและมาตรการเฝ้าระวังภัยไซเบอร์

หน่วยงานกำกับดูแลหรือควบคุม ดำเนินการตาม พ.ร.บ.รักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 เป็นหลัก มีหน้าที่ตรวจสอบมาตรฐานขั้นต่ำ หากพบว่าหน่วยงาน CII ไม่ได้มาตรฐาน ให้หน่วยงานควบคุมหรือกำกับดูแลนั้นรีบแจ้งหน่วยงาน CII ที่ต่ำกว่ามาตรฐานแก้ไขให้ได้มาตรฐานโดยเร็ว ดังที่ระบุไว้ในมาตรา 53 นอกจากนี้ หน่วยงานควบคุมหรือกำกับดูแล ยอมรับในประสิทธิภาพของมาตรฐานสากลอย่าง ISO27001 และกรอบมาตรการด้านความมั่นคงปลอดภัยไซเบอร์อย่าง NIST เช่นเดียวกับหน่วยงาน CII ซึ่งสอดคล้องกับผู้ให้ข้อมูลสำคัญ ดังนี้

"เรามีมาตรฐานสากลอยู่แล้ว เพราะว่า พ.ร.บ.ไซเบอร์ มีการปรับหรือว่าแปลงหรือประยุกต์มาจากมาตรฐานสากลหลายประเทศ เช่น อเมริกา สิงคโปร์ ญี่ปุ่น ทั้งใน พ.ร.บ. และในตัวกฎหมายรองอื่นๆ ซึ่งจะเห็นว่า กรอบแนวคิดหลักหากพิจารณาเนื้อหาดีดีก็จะเห็นได้ว่ามีความสอดคล้องหรือใกล้เคียงกับนานาประเทศ สกมช. เรามีหน่วยงานภายใต้สังกัด เรียกว่า ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ตัวย่อคือ ศปช. ชื่อภาษาอังกฤษปัจจุบันคือ Thai-CERT ซึ่งเป็นหน่วยงานที่ดูแลรักษาความมั่นคงปลอดภัยไซเบอร์โดยตรง ผมก็เป็นสำนักปฏิบัติการที่เป็นส่วนหนึ่งในศูนย์แห่งนี้"

(ผู้ให้ข้อมูลสำคัญที่ 8, สัมภาษณ์เมื่อวันที่ 27 มีนาคม 2566)

*"สพร. มีศูนย์ SOC มีที่ตั้ง Operation center 24*7 มี Certify ISO 27001: 2013 /ISO9001 รวมถึงทางด้าน Technical*

Standard /Cloud /NIST แทบจะทุกมาตรฐานด้านความมั่นคงปลอดภัยเราได้การรับรองมาตรฐานสากลเรียบร้อยแล้ว”

(ผู้ให้ข้อมูลสำคัญที่ 9, สัมภาษณ์เมื่อวันที่ 30 มีนาคม 2566)

“ISO ไม่จำเป็นต้องมีก็ได้เพราะแค่เป็นการ check lists เพราะถ้าทำตามทั้งหมดแต่ไม่มีคุณภาพ ก็อาจจะไม่สามารถป้องกันได้ แต่ทุกองค์กรควรมีแนวปฏิบัติที่ดี NIST และการจัดทำ ISMS เป็นเรื่องที่จำเป็น”

(ผู้ให้ข้อมูลสำคัญที่ 10, สัมภาษณ์เมื่อวันที่ 27 มีนาคม 2566)

“เราดูเรื่อง พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์เป็นหลัก เพราะว่าเราคงยังไม่สามารถที่จะดำเนินการตามกรอบสากลอย่างพวกนี้หรือว่า ISO27001 ได้ ค่อนข้างเทคนิคมากเกินไป เรามีส่วนราชการอื่นที่เป็นหน่วยงานปฏิบัติพวกหน่วยงานลาดตระเวนทางไซเบอร์ให้ และมีหน่วยงานที่ทำหน้าที่ตามกฎหมาย ซึ่งหลักๆเราจะอยู่ในส่วนของการ Monitor มากกว่า หากพบอะไรผิดปกติ เราก็จะเข้าไปดำเนินการแก้ไขให้ทันท่วงที คือมีการเฝ้าระวังอยู่ตลอดเวลา ซึ่งเป็นการทำงานแบบ Cross Function”

(ผู้ให้ข้อมูลสำคัญที่ 11, สัมภาษณ์เมื่อวันที่ 19 เมษายน 2566)

“หน่วยงาน มีการนำ NIST Cybersecurity Framework มาประยุกต์ใช้ในการรับมือภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ แบ่งออกเป็น 5 ข้อ ดังนี้ 1.Identify – ประเมินความเสี่ยงด้านสารสนเทศ เพื่อนำมาปิดช่องว่างด้านความมั่นคงปลอดภัย 2.Protect – มีการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและให้ความรู้แก่บุคลากรในหน่วยงาน 3.Detect – มีการตรวจสอบความผิดปกติอย่างต่อเนื่องของระบบ 4.Respond – มีการกำหนดมาตรฐานขั้นตอนการตอบสนองต่อเหตุการณ์ความผิดปกติภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ 5.Recovery – มีการซักซ้อมแผนตามมาตรฐานแผนรองรับสถานการณ์ฉุกเฉิน (Contingency

Plan) ในการกู้คืนระบบการทำงานให้กลับมาเป็นปกติตามมาตรฐานที่ได้รับการยอมรับ"

(ผู้ให้ข้อมูลสำคัญที่ 14, สัมภาษณ์เมื่อวันที่ 18 เมษายน 2566)

(3) การประสานความร่วมมือและถ่ายทอดสื่อสารให้แก่ผู้มีส่วนได้ส่วนเสีย

ในการรักษาความมั่นคงปลอดภัยไซเบอร์ในประเทศไทยนั้น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ สกมช. คือ หน่วยงานหลักที่มีหน้าที่เป็นเลขาธิการคณะกรรมการทั้ง กบช. และ กกม. คอยประสานงานทั้งด้านงานธุรการ งานวิชาการ งานประชุม และงานเลขานุการ และประสานงานการดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ (CII) รวมทั้งให้ความร่วมมือในการตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ในประเทศและต่างประเทศที่เกี่ยวกับเหตุการณ์ มาตรการ ในการแก้ไขปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ และประสานงานหน่วยงานควบคุมและกำกับดูแลอื่นๆที่เกี่ยวข้องทั้งในภาครัฐและเอกชน อีกทั้งเป็นศูนย์กลางในการให้ความช่วยเหลือ ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคาม โดยเฉพาะภัยที่เกิดกับหน่วยงาน CII เสริมสร้างความตระหนักรู้ผ่านการอบรมเชิงนโยบายและเชิงปฏิบัติการ ซึ่งสอดคล้องกับผู้ให้ข้อมูลสำคัญ ดังนี้

"ยังอยู่ในช่วงพัฒนาเนื่องจากว่า กฎหมายรองที่ออกมาบังคับใช้เพื่อรองรับกับข้อบังคับหลักของกฎหมายไซเบอร์นั้น ต้องอาศัยระยะเวลาเนื่องจากว่า ตัวกฎหมายรองเหล่านี้จะเป็นเครื่องมือที่เสมือนให้อำนาจและให้แนวทางที่ชัดเจนที่ให้หน่วยงานที่เกี่ยวข้อง เช่น หน่วยงานด้านกำกับดูแลหรือว่าหน่วยงาน CII ต้องปฏิบัติตามกลไกเหล่านี้ กฎหมายรองที่ยังไม่เกิดหรือที่เพิ่งเกิดขึ้น ผลก็คือหน่วยงาน CII ต่างก็ยังไม่รู้วิธีในการปฏิบัติให้ชัดเจน อีกทั้งกฎหมายรองที่เกี่ยวข้องตรงนี้ก็ยังออกมาได้ไม่ครอบคลุม จึงทำให้บางส่วนก็ยังขาดๆแหว่งๆอยู่ กระบวนการภาพรวมก็เลยยังไม่สามารถบังคับใช้ได้อย่างเต็มที่ แต่ว่าก็อยู่ระหว่างการพัฒนาไปเรื่อย ๆ นอกจากนี้ เรามีการจัดทำแผน และสามารถปฏิบัติได้ตามแผน แผนดังกล่าวเป็นแผนภายในที่มีการอนุมัติผ่านบอร์ดบริหาร กบส. และมีรายงานไปยังรัฐบาลเพื่อให้รับทราบแนวทาง รวมถึงมีการนำเสนอแผนต่างๆในการ

ประชุมกับหน่วยงานที่เกี่ยวข้องตาม พ.ร.บ. ไซเบอร์ด้วย และตอนนี้เราก็มีเว็บไซต์หลักคือ ncsa.or.th ซึ่งเป็นเว็บไซต์หลัก ในส่วนของด้านปฏิบัติการเรามีเว็บไซต์ Thai-CERT ปัจจุบันคือ https://cert.ncsa.or.th/ และอีกหลายช่องทางเช่น Facebook Fan Page คือ NCSA Thailand"

(ผู้ให้ข้อมูลสำคัญที่ 8, สัมภาษณ์เมื่อวันที่ 27 มีนาคม 2566)

"เรามีการจัดอบรม พรบ / ประกาศ/ ระเบียบ ใหม่ๆให้พนักงานรับทราบตลอด และมีการติดตามข่าวสารใหม่ๆ ทั้งจากฝ่าย security และ ฝ่ายกฎหมาย ก็จะมีการแจ้งให้พนักงานทราบ รวมถึงมีการสื่อสารของ cert ภายใต้ sector ที่เราดูแล"

(ผู้ให้ข้อมูลสำคัญที่ 9, สัมภาษณ์เมื่อวันที่ 30 มีนาคม 2566)

"ต้องมีการวิเคราะห์ผู้มีส่วนได้ส่วนเสียให้ถูกต้องก่อนการสื่อสาร"

(ผู้ให้ข้อมูลสำคัญที่ 10, สัมภาษณ์เมื่อวันที่ 19 เมษายน 2566)

"การฝึกอบรม สมช. จะเข้าไปร่วมในการที่จะสร้าง scenario หรือว่าวางแผนการฝึกให้กับหน่วยงานต่างๆ ในระดับวิกฤต จะมีกองความมั่นคงความมั่นคงด้านการเตรียมพร้อมซึ่งจะดูแลเรื่องของการฝึกในระดับวิกฤตอยู่แล้ว ซึ่งระดับวิกฤตไม่ได้เป็นเพียงแค่ด้านไซเบอร์อย่างเดียว แต่จะเป็นวิกฤตในทุกๆรูปแบบและด้านไซเบอร์เป็น 1 ประเด็นนั้น ซึ่งทาง สมช. ได้เข้าไปร่วมวางกรอบการฝึกกับ สกมช. ว่าควรจะฝึกในแบบไหนดำเนินการในลักษณะไหนมีคู่มือหรือแนวทางหรือไม่ เราควรจะดำเนินการอย่างไรมีการจัดคล้ายๆว่าถ้ามีการโจมตีหน่วยงาน CII ในด้านนี้เราควรจะสร้าง Ad hog หรือว่าคณะทำงานหรือคณะทำงานพิเศษยังไงบ้าง มีหน่วยไหนบ้าง ที่ควรจะเข้ามารับผิดชอบในหน้าที่ต่างๆ"

(ผู้ให้ข้อมูลสำคัญที่ 11, สัมภาษณ์เมื่อวันที่ 19 เมษายน 2566)

“สมช. จัดทำแผนฉุกเฉินภัยคุกคามทางไซเบอร์ ในระดับวิกฤตตามมาตรา 67 ซึ่ง สมช. ได้จัดทำร่วมกับ สกมช. และมีโครงการการฝึกซ้อมการรับมือภัยคุกคามทางไซเบอร์ในระดับชาติภายในหน่วยงานร่วมกับ สกมช และหน่วยงาน CII ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ จะมีหน่วยงานทาง สกมช เป็นหลัก ส่วน สกมช ก็ออกเป็นแผนในเรื่องแผนปฏิบัติการไซเบอร์ เป็นแผนหลักของทั้งประเทศจะระบุว่าจะต้องทำขั้นตอนอะไรบ้าง และหน่วยงานภาครัฐก็จะต้องนำหัวข้อหรือขั้นตอนเหล่านั้นไปจัดทำเป็นแผนปฏิบัติการขององค์กรตนเอง ในส่วนของ IT ก็จะสรุปว่าหน่วยงานได้จัดทำอะไรไปบ้างตามที่ระบุไว้ในแผนใหญ่ และทางเราก็จะส่งให้ทาง สกมช. ตรวจว่าเราได้ทำตามนี้แล้ว 1 2 3 4 5 ซึ่งอะไรที่ขาดอยู่ สกมช ก็จะแจ้งให้ดำเนินการปรับปรุง แต่ถ้าหากดำเนินการเรียบร้อยแล้ว เค้าก็จะนำเสนอบอร์ดบริหารรับทราบ และก็จะเป็น policy ต่อไป ซึ่งก็จะเป็นจุดสิ้นสุดของกระบวนการและก็จะวนไปที่จุดเริ่มต้นในปีต่อไป”

(ผู้ให้ข้อมูลสำคัญที่ 12, สัมภาษณ์เมื่อวันที่ 19 เมษายน 2566)

“จะมีการส่งเจ้าหน้าที่ไปอบรมกับ สกมช. และด้านเอกชน แต่มีงบประมาณที่จำกัด จะเลือกอบรมหลักสูตรฟรีเป็นส่วนใหญ่ มีการประชุมทุกเดือน”

(ผู้ให้ข้อมูลสำคัญที่ 13, สัมภาษณ์เมื่อวันที่ 25 เมษายน 2566)

“สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม มีความร่วมมือกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) รวมถึงสำนักงานพัฒนารัฐบาลอิเล็กทรอนิกส์ (สพธอ.) อย่างต่อเนื่องในการประสานงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ ซึ่งการดำเนินการระหว่างภาครัฐ เป็นการดำเนินการที่สอดคล้องตามหลักกฎหมายระเบียบ รวมถึงข้อบังคับต่างๆ ที่เกี่ยวข้อง นอกจากนี้ มีการจัดทำแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยสารสนเทศซึ่งมีการอ้างอิงมาจาก ISO 27001:2013 โดยมีการถ่ายทอดองค์ความรู้รวมถึงการ

บริหารจัดการในรูปแบบของคณะทำงานปรับปรุงนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ และถ่ายทอดไปสู่หน่วยงานภายในสังกัด”

(ผู้ให้ข้อมูลสำคัญที่ 14, สัมภาษณ์เมื่อวันที่ 19 เมษายน 2566)

(4) การติดตามและประเมินผลลัพธ์

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ สกมช. ในฐานะผู้ดำเนินการหลักตาม พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 โดยในด้านการติดตามและประเมินผล สกมช. และหน่วยงานควบคุมหรือกำกับดูแล จะทำหน้าที่ระงับภัยคุกคามทางไซเบอร์ในระดับร้ายแรงหรือระดับวิกฤต โดยรวบรวมข้อมูล หรือพยานเอกสาร พยานบุคคล พยานวัตถุที่เกี่ยวข้องเพื่อวิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ นอกจากนี้ ในองค์กรอื่นๆของภาครัฐหรือเอกชน ได้มีการกำหนดตัวชี้วัดการรับมือภัยคุกคามทางไซเบอร์ เพื่อประเมินคุณภาพและระดับความสำเร็จในการประเมินความเสี่ยง พัฒนาประสิทธิภาพในการรับมือภัยคุกคามทางไซเบอร์ ซึ่งสอดคล้องกับผู้ให้ข้อมูลสำคัญ ดังนี้

“เรามีตัวชี้วัดในโครงการต่างๆ เช่น การจัดทำงบประมาณ ในส่วนของตัวชี้วัดสำนักงานก็จะเป็น commitment ที่หน่วยงานมีต่อบอร์ดบริหารคือ กบส. ว่าในรอบปีเราทำอะไรไปบ้าง นอกจากนี้เรายังมีตัวชี้วัดอื่นๆที่นำมาใช้กับหน่วยงานอย่างเช่นเรื่องของ ITA การบริหารงานภาครัฐ และ PMQA ด้วย”

(ผู้ให้ข้อมูลสำคัญที่ 8, สัมภาษณ์เมื่อวันที่ 19 เมษายน 2566)
(ผู้อำนวยการสำนักปฏิบัติการ สกมช.)

“มีการกำหนดตัวชี้วัดด้านไซเบอร์ มีฝ่ายสำหรับพัฒนาองค์กรกำกับดูแลเรื่อง policy ซึ่งทาง สพร. ก็จะมีการประสานร่วมกันกับฝ่าย cybersecurity เพื่อนำไปออกเป็นนโยบาย ซึ่งก็จะรวมอยู่ใน KPI ของแต่ละฝ่าย”

(ผู้ให้ข้อมูลสำคัญที่ 9, สัมภาษณ์เมื่อวันที่ 30 มีนาคม 2566)

“ผมมองว่าตัวชี้วัดที่เป็นด้าน security จะค่อนข้างดี แต่ยกตัวอย่างตัวชี้วัดที่ไม่ค่อยดี คือการทดสอบหลังอบรม เพราะบางคนอบรมไปผ่านทดสอบเพราะข้อสอบง่าย แต่พอผ่านไปก็จะลืม แต่ถ้ามีการทดสอบ Phishing mail จะ success เพราะถ้าไม่ผ่านก็ต้องอบรมใหม่”

(ผู้ให้ข้อมูลสำคัญที่ 10, สัมภาษณ์เมื่อวันที่ 27 มีนาคม 2566)

“ถ้าเป็นในเรื่องของแผนการฝึกจะมีตัวชี้วัด และมีแผนแม่บทด้านความมั่นคงปลอดภัยซึ่งในส่วนนี้จะมีตัวชี้วัดอยู่ และเราก็ได้ถ่ายทอดตัวชี้วัดนั้นร่วมกับแผนนโยบายระดับชาติเรื่องความมั่นคงแห่งชาติ และแยกออกมาเป็นตัวนโยบายและแผนปฏิบัติการการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สกมช. ที่มีการจัดทำรายละเอียดของโครงการต่างๆ และตรวจว่าแต่ละโครงการจะสามารถนำไปตอบโจทย์ตัวชี้วัดได้อย่างไรบ้าง ซึ่งมีการจัดทำทุก 6 เดือน ผ่านระบบ eMENSCR ของสภาพัฒน ซึ่ง สมช. จะช่วยกำกับดูแลอีกทาง”

(ผู้ให้ข้อมูลสำคัญที่ 11, สัมภาษณ์เมื่อวันที่ 19 เมษายน 2566)

“เรื่องตัวชี้วัดจะมีวัดเรื่องความปลอดภัยของระบบและมีการป้องกันระบบล่ม การว่าจ้างที่ปรึกษาภายนอกด้านไอที”

(ผู้ให้ข้อมูลสำคัญที่ 13, สัมภาษณ์เมื่อวันที่ 25 เมษายน 2566)

“สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้ดำเนินการตาม พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาโดยตลอดโดยดำเนินการตามที่นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ.2565-2570) เป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ และเป็นกรอบแนวทางการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ เป็นมาตรฐานขั้นต่ำที่กำหนดไว้ ในส่วนของการการกำหนดตัวชี้วัดในการติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (outcome) อยู่ระหว่างรอรอบการประเมินผลประจำปี (ปลายปี 66)

เพื่อจะนำมาวิเคราะห์ประเมินความเสี่ยงและกำหนดเป้าตัวชี้วัด ซึ่งจะกำหนดในปีงบประมาณ 2567 ต่อไป”

(ผู้ให้ข้อมูลสำคัญที่ 14, สัมภาษณ์เมื่อวันที่ 18 เมษายน 2566)

4.4.1.3 การรับมือของหน่วยงานด้านป้องกันและปราบปรามภัยคุกคามทางไซเบอร์

จากผู้ให้ข้อมูลสำคัญคนที่ 18 ได้แสดงทรรศนะด้านการรับมือภัยคุกคามทางไซเบอร์ในฐานะหน่วยงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไว้ว่า จากจำนวนของอาชญากรรมทางไซเบอร์ที่มีมากขึ้น และภัยคุกคามทางไซเบอร์มีแนวโน้มที่เพิ่มขึ้นและหลากหลายมากขึ้นตามลำดับ สำนักงานตำรวจแห่งชาติได้เห็นถึงความสำคัญในการป้องกันและรับมือการโจมตีทางไซเบอร์ จึงได้ก่อตั้งหน่วยงานใหม่ คือ กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) หรือเรียกสั้นๆว่า กองบัญชาการไซเบอร์ขึ้นในปี พ.ศ.2563 และมีกลุ่มงานที่ดูแลด้านความมั่นคงปลอดภัยไซเบอร์โดยเฉพาะ ให้ทำหน้าที่ในการสร้างความร่วมมือระหว่างหน่วยงานความมั่นคงปลอดภัยไซเบอร์ระดับชาติกับหน่วยงานความมั่นคงภายในประเทศ ปฏิบัติการร่วมกับสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์หรือ สกมช. เพื่อสร้างกรอบความร่วมมือโดยมุ่งไปที่การป้องกันข้อมูล สนับสนุนการมีวัฒนธรรมความปลอดภัยร่วมกัน ผลักดันให้มีศูนย์เฝ้าระวังเพื่อตรวจจับและป้องกันการโจมตีทางไซเบอร์ รวมถึงผลักดันให้สามารถใช้กฎหมายดำเนินการกับอาชญากรรมทางไซเบอร์ได้อย่างมีประสิทธิภาพ

ในด้านการกำกับดูแล บช.สอท. ได้ดำเนินการตาม พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ในการบริหารจัดการ และประสานงานให้ความร่วมมือกับ สกมช. ในฐานะหน่วยงานควบคุมและกำกับดูแล หรือ Regulator รวมถึงปฏิบัติตามประกาศคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์และกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้อง เช่น พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 หรือ PDPA และ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 เป็นต้น ในขณะที่ การประสานความร่วมมือและถ่ายทอดสื่อสารให้แก่ผู้มีส่วนได้ส่วนเสีย การดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศระหว่างหน่วยงานภาครัฐยังคงล่าช้า เมื่อเทียบกับหน่วยงานภาคเอกชนที่มีการพัฒนาอย่างรวดเร็ว เนื่องจากยังขาดความตระหนักรู้ ขาดแคลนบุคลากร ขาดแคลนอุปกรณ์ที่ทันสมัย หลายๆกิจกรรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จำเป็นต้องอาศัยความร่วมมือของผู้บังคับบัญชาระดับสูง ซึ่งปัจจุบันก็ยังคงมีการบริหารงานแบบเดิม ๆ ที่มีความล่าช้า ยึดถือเอกสารเป็นสำคัญ ขั้นตอนซ้ำซ้อนหลายขั้นตอน สอท.

จึงต้องการให้ สกมช. ผลักดันให้มี พ.ร.บ. หรือกำหนดมาตรฐานสากลที่จะนำมาใช้เพื่อรับมือภัยคุกคามทางไซเบอร์ที่เป็นทางการ และทุกหน่วยงานสามารถนำไปปฏิบัติได้ทันที เนื่องด้วยที่ผ่านมาทางผู้ปฏิบัติยังเข้าใจในกฎหมายรองต่างๆมากนัก เช่น ด้านเทคโนโลยีการป้องกันภัยไซเบอร์ที่ยังไม่ชัดเจน

ในด้านการให้บริการประชาชนเมื่อช่วงต้นปี 2565 สำนักงานตำรวจแห่งชาติได้มีการเปิดตัวเว็บไซต์ https://thaipoliceonline.com/ สำหรับแจ้งความออนไลน์ เฉพาะในหมวดหมู่คดีอาชญากรรมทางเทคโนโลยี เพื่อเพิ่มความสะดวกและรวดเร็วมากยิ่งขึ้น สำหรับผู้ที่ต้องการแจ้งความในคดีดังกล่าวรวมทั้งสามารถติดตามผลความคืบหน้าของคดีได้ทันทีไม่ต้องไปที่โรงพักอีกด้วย ซึ่งผลการแจ้งความออนไลน์สูงถึง 59,846 เรื่อง และพบว่า 3 อันดันแรกคือ หลอกให้ทำงานออนไลน์ หลอกให้กู้เงินแต่ไม่ได้เงิน และหลอกให้ลงทุนในรูปแบบต่างๆ ส่วนลำดับรองลงมาได้แก่ หลอกลวงจำหน่ายสินค้า 24,643 เรื่อง การพนันออนไลน์ 462 เรื่อง ข่าวปลอม 239 เรื่องและล่วงละเมิดทางเพศ 136 เรื่อง ซึ่งจากจำนวนคดีต่างๆตลอด 4 เดือนที่ผ่านมา ทางเจ้าหน้าที่สามารถดำเนินการอายัดบัญชีได้แล้วกว่า 121 ล้านบาท ถือว่าการจัดทำเว็บไซต์เพื่อให้บริการประชาชน ช่วยลดความสูญเสียด้านทรัพย์สินได้ไม่น้อย

ในด้านการป้องกันและปราบปราม จากผู้ให้ข้อมูลสำคัญคนที่ 17 ได้อธิบายไว้ว่า กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี หรือ บช.ปอท. เป็นลักษณะการรับแจ้งหรือรับมอบหมายให้ทำการดำเนินการสืบสวนสอบสวนหาตัวและติดตามจับกุมผู้กระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ลักษณะอาชญากรรมทางเทคโนโลยีที่ดำเนินการจะเป็นกรณีตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 และความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติอื่นๆ ที่มีโทษทางอาญา ตัวอย่างเช่น การเข้าถึงระบบ หรือ ข้อมูลคอมพิวเตอร์โดยมิชอบ หรือการแก้ไข ทำลายข้อมูลคอมพิวเตอร์โดยมิชอบ ตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 มาตรา 5,7,9 เป็นต้น ในส่วนของหน่วยงานเมื่อพบว่ามีลักษณะคดี หรือรูปแบบใดที่ประชาชนได้รับความเสียหายหา ก็จะมีการประชาสัมพันธ์ถึงลักษณะคดีที่เกิดขึ้น และแนะนำแนวทางการป้องกันให้แกประชาชนได้ทราบและระมัดระวังการตกเป็นเหยื่อได้

4.4.1.4 การรับมือตามทัศนคติของผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์

(1) การกำกับดูแลและบริหารความเสี่ยง

ในมุมมองของผู้เชี่ยวชาญที่มีประสบการณ์ด้านการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ในหน่วยงานต่างๆ ของภาครัฐ จากผู้ให้ข้อมูลสำคัญคนที่ 19 ที่แสดงทัศนคติด้านการกำกับดูแลและบริหารความเสี่ยงไว้ว่า

"ในฐานะที่ผมเป็นคณะกรรมการด้าน Security ขององค์กรต่างๆ ผมก็นำกฎหมายและพระราชบัญญัติที่หน่วยงานราชการจะต้องส่งแผน นโยบาย และแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศซึ่งคณะทำงานร่วมมีการวิเคราะห์ว่าเราควรนำประเด็นด้าน Security ต่างๆไปผูกกับ Risk คือ แม้ว่าจะไม่ได้ผลลัพธ์เป็นเงินเป็นทอง แต่มีผลกระทบกับภาครัฐหรือบริษัท จึงจัดทำออกมาในรูปแบบ Good Governance และ Compliance และ Risk Measurement เพราะฉะนั้น ยกตัวอย่างถ้าบริษัทหรือองค์กรคุณไม่มี Firewall เลยนั่นหมายถึง 1. Governance ไม่ดี 2. Risk สูง 3. Compliance ไม่ผ่าน รวมกัน 3 อย่างคือ GRC ถ้าเป็นตลาดหลักทรัพย์ นั่นหมายถึง หุ้นบริษัทก็ร่วง ฉะนั้นสิ่งเหล่านี้ก็เป็นการเชื่อมโยงให้เห็นภาพด้าน Security ที่ไม่เห็นผลทันทีกับผลประโยชน์ของบริษัท เพราะหากเน้นในเรื่อง Security อย่างเดียวไปไม่รอด ดังนั้นต้องบอกด้วยว่าทำแล้วได้อะไร ทำแล้วผู้บริหารไม่ติดคุก อย่างนี้ เป็นต้น ซึ่งหากนโยบายองค์กร ทำแบบเดียวกับ พ.ร.บ. และ ISO อาจจะยากเกินไป ดังนั้นต้องมีการนำมา compromise ไกล่เกลี่ยกันระหว่างด้านไอทีและด้านกฎหมาย และนำมาปรับให้ใกล้เคียง แล้วดูว่ามี GAP หรือไม่ระหว่างสิ่งที่เราต้องทำและสิ่งที่เรามีอยู่ ถ้ามีแล้วจะแก้ไขปัญหาเหล่านั้นได้อย่างไร เพราะฉะนั้นจะได้เห็นได้ว่ามาตรฐานทาง ISO27001 หรือด้านกฎหมายและ พ.ร.บ. ต่างๆ จะค่อนข้างไม่ลงรายละเอียด ซึ่งรัฐจะบอกแค่ว่าคุณต้องคำนึงถึงเรื่องนั้นเรื่องนี้ แต่ทุกหน่วยงานต้องมีเรื่องของ Access Control และ User Awareness Training เป็นต้น แต่จะทำได้มากน้อยแค่ไหนขึ้นอยู่กับแต่ละหน่วยงานว่ามองเห็น

ความสำคัญแค่ไหนและการจัดสรรงบประมาณได้มากน้อยแค่ไหน ซึ่งต้องระบุให้ชัดเจน”

(ผู้ให้ข้อมูลสำคัญที่ 19, สัมภาษณ์เมื่อวันที่ 19 มีนาคม 2566)

สำหรับผู้ให้ข้อมูลสำคัญคนที่ 20 แสดงทรรศนะไว้ 2 ประเด็นคือ 1) ต้องมีแผนรองรับ เช่น แผนด้านคน ที่จะต้องมีทักษะความรู้ด้านนี้โดยเฉพาะ มีการกำหนดหน้าที่ความรับผิดชอบที่ชัดเจน ซึ่งต้องดูแลระบบแบบ 24 ชั่วโมง 7 วันหรือเทคนิค เรียกว่า 24*7 (24 คูณ 7) และต้องมีแผนงานว่าจะต้องทำอะไรบ้างในแต่ละวัน นอกจากนี้ ต้องมีแผนหนึ่ง แผนสอง ในการรับมือ 2) ในแง่ของเครื่องมือหน่วยงานของรัฐส่วนใหญ่ค่อนข้างจะขาดแคลน 3) เรื่อง Social Engineering ที่เข้ามาเพื่อผลประโยชน์ การให้ข้อมูลหลอกลวงด้วยวิธีการใหม่ๆ ในขณะที่ ผู้ให้ข้อมูลสำคัญคนที่ 21 ได้แสดงความคิดเห็นเรื่องการรับมือของหน่วยงานภาคการเงินการธนาคารไว้ค่อนข้างแตกต่างจากผู้ให้ข้อมูลสำคัญ 2 ท่านที่ผ่านมา และมีการกล่าวถึงในประเด็นที่คล้ายคลึงกัน อาทิเช่น Social engineering ดังนี้

“การกำกับของผู้บริหารภาครัฐยังมีวิสัยทัศน์ที่ไม่ชัดเจน เว้นแต่หน่วยงานอย่างเช่น กลต. คปภ. ธปท. มีแนวทางที่ชัดเจน ตั้งแต่ระดับผู้บริหารและมีการติดตามในทันที นอกจากนโยบายและแผนยุทธศาสตร์ แต่ในปัจจุบันผู้นำในโลกของเราจะให้ความสำคัญกับ Cyber insurance หรือ ประกันภัยไซเบอร์ ซึ่ง ก.ล.ต. เองได้ให้บริษัทประกันต่างๆดำเนินการจัดทำ แล้วกลุ่มที่เชี่ยวชาญเรื่อง Cybersecurity ที่ดีที่สุดจริงๆจะอยู่ในภาคของประกันภัย เมื่อเราต้องการจะจ้างบบริษัทประกันภัย กรณีถ้ามีข้อมูลรั่วไหลหรือมีภัยคุกคามก็จะมีบริษัทประกันภัยรับผิดชอบให้ในส่วนนี้ ทำให้ลดความเสี่ยงองค์กร ในขณะเดียวกันการตกลงทำ Contract ระหว่างหน่วยงานกับบริษัทประกันภัยต้องมีการดำเนินงานตามข้อตกลงของบริษัทประกันภัยในเรื่องของมาตรฐานต่างๆที่องค์กรจำเป็นต้องมี เช่น ต้องรักษามาตรฐาน และต้องมีการสร้าง Awareness ทุกปี รวมถึงคุณสมบัติอื่นๆตามเงื่อนไขของบริษัทประกัน ทำให้ Cyber Insurance เป็นแนวทางที่ดีด้านความมั่นคงปลอดภัยไซเบอร์มากกว่า

นโยบายและแผนยุทธศาสตร์ ซึ่ง Cyber Insurance จะเข้ามาอุดช่องโหว่ในเรื่องนี้ ในเรื่องของความเสี่ยงเท่าที่ศึกษาในงานวิจัยต่างๆ พบว่าเรื่องปัญหา Cybersecurity ส่วนใหญ่มาจาก Human 95% ซึ่งอาชญากรแทบจะไม่มีการรีโมทไปที่เครื่องคอมพิวเตอร์เรา โดยที่คนร้ายจะสามารถทำได้ไม่ใช่มาจากเทคโนโลยี แต่มาจากการคลิกลิงก์และเทคนิคในการหลอกลวงต่างหากที่เรียกว่า Social engineering เช่น แฮกเกอร์ปลอมตัวเข้าไปในองค์กรทำทีว่าคุยกับพนักงาน เมื่อเผลอก็นำ USB เสียบไปที่เครื่องคอมพิวเตอร์เพื่อเข้าถึงข้อมูล หลังจากนั้นไม่ว่าพนักงานจะพิมพ์ข้อความหรือใช้งานใดๆ แฮกเกอร์ก็จะรู้ความเคลื่อนไหว ซึ่งสิ่งเหล่านี้ก็จะเป็นการรั่วไหลจากคนมากกว่า นอกจากนี้ต้องคำนึงถึงการติดสินบนพนักงานเพื่อต้องการเข้ามาล่วงรู้ข้อมูลความลับต่างๆขององค์กร ซึ่งยังไม่มีคนตระหนักรู้ในเรื่องนี้ ดังนั้น ทุกองค์กรควรมีความประเมินคุณธรรมจริยธรรมเรื่องความเสี่ยงในการทุจริต ทั้งในด้านของการรั่วไหลของข้อมูลจากบุคคลหรือแม้แต่การทุจริตติดสินบน การประเมินจิตวิทยาด้านความเสี่ยง”

(ผู้ให้ข้อมูลสำคัญที่ 21, สัมภาษณ์เมื่อวันที่ 25 มีนาคม 2566)

(2) มาตรฐานและมาตรการเฝ้าระวังภัยไซเบอร์

เป็นที่สังเกตว่า ผู้เชี่ยวชาญให้ทัศนคติด้านการนำเทคโนโลยีและมาตรฐานต่างๆของภาครัฐและเอกชน เป็นไปในทิศทางเดียวกันคือ การนำมาตรฐานสากลอย่าง ISO27001 และกรอบแนวคิดของ NIST จากประเทศอเมริกามาใช้ในการดำเนินการด้านการเฝ้าระวังและรับมือภัยทางไซเบอร์ในหลายๆองค์กร แต่สำหรับบางหน่วยงานยังไม่มีการใช้มาตรฐานในส่วนนี้หรือมีวิธีการรับมือที่เป็นกระบวนการของหน่วยงานเอง เนื่องด้วยขาดงบประมาณในการขับเคลื่อนทั้งเชิงนโยบายและเชิงเทคนิคกลวิธีในการปฏิบัติการ สอดคล้องกับผู้ให้ข้อมูลสำคัญ ดังต่อไปนี้

“ปัจจุบันองค์กรควรมีศูนย์ SOC ซึ่งมีความจำเป็นกับทุกองค์กร แต่ทั้งนี้ขึ้นอยู่กับแต่ละหน่วยงานรวมทั้งควรนำ ISO27001 มาใช้ในการดำเนินงาน หากองค์กรไม่มี ISO ถือว่าองค์กรละเลยในสิ่งที่จะต้องทำหรือควรทำ ประเด็นคือ ต้องดูว่า Risk อยู่ที่ไหน จะมีด้วยกัน 3 ส่วนคือ 1. GRC คือ Governance Risk เช่นดูว่าเสี่ยงตรงไหนบ้าง

อัตราความเสี่ยงเป็นอย่างไร และ Compliance เพราะการแก้ไขและอุดช่องโหว่ต่างๆเหล่านี้ต้องใช้ Resource คือ เงิน คน เวลา หรืออื่นๆ ก็ต้องเรียงลำดับไปจากสิ่งที่สำคัญมากไปหาน้อย เงินหมดเมื่อไหร่ คนหมดเมื่อไหร่คือจบ เพราะฉะนั้น เมื่อมีเรื่องที่จะต้องทำร้อยอย่างในหน่วยงานไอที แต่เราทำได้เพียงแค่งบประมาณและจำนวนคนเท่าที่ได้รับจัดสรรจากผู้บริหารซึ่งมีอยู่อย่างจำกัด ดังนั้นหากภาครัฐสนับสนุนงบประมาณให้องค์กรอย่างสมเหตุสมผลเพื่อให้รับมือได้เต็มประสิทธิภาพ"

(ผู้ให้ข้อมูลสำคัญที่ 19, สัมภาษณ์เมื่อวันที่ 19 มีนาคม 2566)

"แนวปฏิบัติ Industry Standard เป็นความพยายามของภาคอุตสาหกรรมที่พัฒนามาตรฐานด้านเทคโนโลยีเชิงอุตสาหกรรม ดังนั้น การที่เราใช้ ISO27001 หรือ Standard ที่ออกโดยรัฐบาลของคนอเมริกันอย่างมาตรฐาน NIST แต่ทั้งนี้ขึ้นอยู่กับหน่วยงานแต่ละองค์กรที่ต้องการพัฒนามาตรฐานการดำเนินงานและยกระดับคุณภาพของกระบวนการต่างๆเหล่านี้ เพราะแม้ว่าจะมีการเปลี่ยนผู้บริหารองค์กร แต่มาตรฐานเหล่านี้ยังคงอยู่ เพื่อควบคุมการปฏิบัติงานให้ได้มาตรฐาน ซึ่งเป็นเครื่องมือที่ดีมาก เป็นการสร้างความตระหนักรู้ และสร้างกรอบแนวความคิด รวมถึงแนวปฏิบัติย่อยในแต่ละด้าน เพื่อเป็นตัวชี้วัดและบรรทัดฐานว่าแต่องค์กรมีหรือยัง ถ้ายังควรปรับปรุงอย่างไร"

(ผู้ให้ข้อมูลสำคัญที่ 20, สัมภาษณ์เมื่อวันที่ 19 มีนาคม 2566)

"มีการนำกรอบ NIST และ ISO27001 มาใช้กันเป็นส่วนมาก แต่ปัญหาส่วนใหญ่อยู่ที่คนมากกว่าเรื่องมาตรฐานหรือเทคโนโลยี เพราะไม่ใช่แค่พนักงานไอที แต่ User หรือผู้ใช้งานนำอุปกรณ์อิเล็กทรอนิกส์อย่าง Thump-Drive มาขอใช้คอมพิวเตอร์ของหน่วยงานไอที และภาครัฐเองก็ละเลยเรื่องเหล่านี้"

(ผู้ให้ข้อมูลสำคัญที่ 21, สัมภาษณ์เมื่อวันที่ 25 มีนาคม 2566)

นอกจากนี้ ด้านการประสานความร่วมมือและถ่ายทอดสื่อสารให้แก่ผู้มีส่วนได้ส่วนเสีย ทางผู้ให้ข้อมูลสำคัญคนที่ 19, 20 และ 21 มีความคิดเห็นคล้ายคลึงกัน โดยอธิบายว่า การสื่อสารของภาครัฐยังไม่มีประสิทธิภาพเท่าที่ควร เช่น 1) เรื่องวัฒนธรรมการทำงาน 2) เรื่องของกฎหมาย ของภาครัฐยังไม่ครอบคลุมและการป้องกันยังทำแบบต่างคนต่างอยู่ ยังคงทำแบบกระจายแทนที่จะรวมศูนย์ เช่น กระทรวงสาธารณสุขของแต่ละโรงพยาบาลตั้งงบจัดซื้อเครื่องแม่ข่าย (Server) เป็นของตนเอง อีกทั้งในการติดตามและประเมินผลลัพธ์ ยังไม่ค่อยเห็นมีการทำตัวชี้วัด เพราะมองว่าคนที่จะมาทำตัวชี้วัดจริงๆคือ ด้านประกันภัย (Insurance) เพราะถ้ามีการทำประกันภัยเมื่อใด จะมีการตรวจสอบ (Checklist) ให้ว่าทำอะไรไปบ้าง และจะสอดคล้องกับสัญญาที่รับประกันไว้ตามเงื่อนไข

สรุปได้ว่า แนวทางการเตรียมแผนการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์และการกำกับดูแลการบริหารจัดการที่ดีด้านเทคโนโลยีดิจิทัลในองค์กร เพื่อลดความเสี่ยงและป้องกันภัยคุกคามทางไซเบอร์ในอนาคต พบว่า องค์กรหลายแห่งกำลังถูกคุกคามอย่างต่อเนื่องจากการโจมตีทางไซเบอร์ สถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกาตระหนักถึงความสำคัญของภัยคุกคามด้านไซเบอร์ดังกล่าว จึงได้มอบหมายให้สถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (National Institute of Standards and Technology ; NIST) ได้ทำการพัฒนากรอบดำเนินงานเพื่อปรับปรุงความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานระบบโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure Security) เพื่อให้เป็นแนวทางและมาตรฐาน ซึ่งครอบคลุมทั้งในระดับนโยบาย (Policy) การจัดการองค์กร (Organization) และเทคโนโลยี (Technology) เพื่อบริหารจัดการความเสี่ยงทางไซเบอร์ (Cyber Risk Management) ที่มีผลกระทบกับหน่วยงานได้อย่างเหมาะสม โดยกำหนดกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ (Framework Core) เพื่อนำมาใช้ในการดำเนินการร่วมกัน ประกอบด้วย กลุ่มหน้าที่งาน (Functions) เป็นกิจกรรมพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์ในระดับภาพรวม จำแนกเป็น 5 ขั้นตอน ได้แก่ (1) การระบุความเสี่ยง (Identity) (2) การป้องกันความเสี่ยง (Protect) (3) การตรวจสอบและเฝ้าระวัง (Detect) (4) การตอบสนอง (Respond) (5) การคืนสภาพ (Recovery) โดยจะเห็นปรากฏอยู่ในมาตรา 13 ของ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ของประเทศไทย

นอกจากนี้ แนวทางที่ใช้เป็นมาตรฐานในการกำกับดูแลและการรักษาความมั่นคงปลอดภัยไซเบอร์ที่องค์กรทั่วโลกยอมรับและนำไปใช้ร่วมกับแนวทางปฏิบัติขององค์กร คือ

มาตรฐานสากล ISO/IEC 27001 ซึ่งมีหลายหน่วยงานทั้งในประเทศและต่างประเทศ นำไปใช้ในการบริหารจัดการตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยมีเป้าหมายหลักของการรักษาความปลอดภัยข้อมูลคือ การปกป้องข้อมูลที่องค์กรรวบรวม เก็บ สร้าง รับ หรือส่ง ไม่สำคัญว่าจะต้องใช้อุปกรณ์เทคโนโลยีหรือกระบวนการใดในการจัดการแต่จะต้องได้รับการปกป้อง โดยให้ความสำคัญกับการรักษาความลับของข้อมูลสารสนเทศ (Confidentiality) การรักษาความครบถ้วนสมบูรณ์ของข้อมูลสารสนเทศ (Integrity) และการรักษาสภาพพร้อมใช้งานของระบบ (Availability) ซึ่งเป็นปัจจัยพื้นฐานในการพิจารณาความมั่นคงปลอดภัยทางไซเบอร์โดยอาศัยการประเมินความเสี่ยง (Risk assessment) ที่ข้อมูลสารสนเทศอาจได้รับผลกระทบหรือเกิดความเสียหายจากภัยคุกคามทางไซเบอร์ ซึ่งประโยชน์ของระบบมาตรฐาน ISO/IEC 27001 คือ ปกป้องข้อมูลองค์กร พร้อมใช้ทรัพยากรอย่างมีประสิทธิภาพ มีมาตรฐานของระบบจัดการความมั่นคงด้านสารสนเทศ ISO 27001 (ISMS) นำเสนอกรอบการปฏิบัติที่ช่วยองค์กรยกระดับความมั่นคงด้านสารสนเทศ พร้อมกับลดต้นทุนในเวลาเดียวกัน

4.4.2 การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์

การสร้างความตระหนักรู้ความปลอดภัยทางไซเบอร์ หมายถึง กระบวนการให้ความรู้แก่บุคคลและองค์กรเกี่ยวกับความเสี่ยงและภัยคุกคามที่อาจเกิดขึ้นจากการใช้อุปกรณ์ดิจิทัลและการเข้าถึงอินเทอร์เน็ต เพื่อช่วยให้ผู้คนเข้าใจวิธีการปกป้องข้อมูลและอุปกรณ์ของตนจากการโจมตีทางไซเบอร์ ซึ่งจุดมุ่งหมายของการสร้างความตระหนักรู้ด้านความปลอดภัยในโลกไซเบอร์ คือ การช่วยให้ผู้คนพัฒนาความรู้ ทักษะ และพฤติกรรมที่จำเป็นต่อการใช้อุปกรณ์ดิจิทัลอย่างปลอดภัย รวมถึงการสอนและชี้แนะให้คนเห็นถึงความสำคัญของการรักษาซอฟต์แวร์ให้ทันสมัยอยู่เสมอ การใช้รหัสผ่านที่รัดกุม การหลีกเลี่ยงอีเมลและเว็บไซต์ที่น่าสงสัย และการระมัดระวังเมื่อแชร์ข้อมูลส่วนบุคคลทางออนไลน์ เพื่อลดความเสี่ยงจากการโจมตีทางไซเบอร์และปกป้องข้อมูลที่สำคัญและอ่อนไหวจากการถูกขโมยหรือถูกบุกรุก เป็นสิ่งสำคัญสำหรับทุกคนที่จะต้องตระหนักถึงความเสี่ยงด้านความปลอดภัยในโลกไซเบอร์ และดำเนินการเพื่อป้องกันตนเองและอุปกรณ์ของตนจากภัยคุกคามที่อาจเกิดขึ้น

โดยผู้ให้ข้อมูลสำคัญคนที่ 8 กล่าวว่า พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดให้มีการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์

แห่งชาติ หรือ Thailand Computer Emergency Response Team (ThaiCERT) ขึ้น โดยเป็นหน่วยงานภายในสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เพื่อเฝ้าระวังความเสี่ยง ในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ อาศัยอำนาจตามความในมาตรา 22 วรรคสอง แห่ง พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่ง สกมช. มีหลายช่องทางในการสร้างความตระหนักรู้ผ่านการบรรยาย อาทิ หนังสือเชิญ, Facebook, Poster ประชาสัมพันธ์, Email, Line, Open Chat, เอกสารเวียนภายในหน่วยงาน, อบรมเชิงปฏิบัติการ และมีโครงการที่จัดขึ้นเพื่อให้บุคลากรจากหน่วยงานที่เกี่ยวข้องด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และประชาชนที่สนใจ มีความตระหนัก รับรู้ และเข้าใจ ถึงความสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์ และแบ่งปันประสบการณ์ องค์ความรู้ใหม่ๆ ที่ สกมช. ได้คัดเลือกมาให้ผู้ที่สนใจในหัวข้อต่างๆ ได้ Update อย่างรวดเร็วและทันสมัย หรือเรียกว่า โครงการ Cyber Knowledge Sharing ที่มีตารางตามแผนงานทุกเดือนและเปิดเผยหน้าเว็บไซต์ของ สกมช. นอกจากนี้ ยังมีการประชุมเชิงปฏิบัติการสำหรับหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือโครงการ Cyber Clinic ที่ทำหน้าที่ให้คำปรึกษาและความตระหนักรู้ให้กับองค์กรต่างๆ ซึ่งสอดคล้องกับข้อมูลจากการสัมภาษณ์ผู้ให้ข้อมูลสำคัญทั้งจากหน่วยงาน CII และหน่วยงานด้านการกำกับดูแลที่เกี่ยวข้อง รวมถึงผู้เชี่ยวชาญ ดังนี้

> *“มีการอบรม การสื่อสารให้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องให้ครอบคลุมทั้งหมด ทั้งด้านการจัดทำสื่อวารสาร Infographic นอกจากนี้ เราก็สนับสนุนให้พนักงานอบรมให้มากขึ้น เนื่องจากภาครัฐเองให้บริการอบรมฟรีทั้ง Onsite และ Online ทั้งสัมมนาและอบรมเชิงปฏิบัติการ ทั้งในเวลาและนอกเวลา รวมทั้งการส่งพนักงานไปดูงานหน่วยงานภาครัฐและรัฐวิสาหกิจอื่นๆที่สามารถนำมาปรับใช้กับบริบทขององค์กรได้ ทางเราเองก็สนับสนุนในเรื่องนี้”*
>
> (ผู้ให้ข้อมูลสำคัญที่ 1, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

> *“มีการจัดทำ infographic และ วิดิโอที่เป็น KM เพื่อให้พนักงานเข้าไปศึกษาในรูปแบบของการเรียนการสอน มีแบบทดสอบ*

ให้พนักงานทำการ Pre-test และ Post-test อย่างต่อเนื่อง และทดสอบ Phishing mail”

(ผู้ให้ข้อมูลสำคัญที่ 2, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

“มีการจัดส่งพนักงานอบรม ซึ่งแบ่งกลุ่มพนักงานทั่วไป พนักงานใหม่ และไอที มีจัดกลุ่มไอทีสอนพนักงานใหม่และเรื่อง security และ พรบ ที่เกี่ยวข้องกปน ใช้เมล์ google workspace มีการอบรมเรื่อง cloud มีการอบรบกับ DGA และรับรองใบเซอร์ กปน. มีการทดสอบ phishing mail กับ พนักงาน”

(ผู้ให้ข้อมูลสำคัญที่ 3, สัมภาษณ์เมื่อวันที่ 30 มีนาคม 2566)

“เรามีการจัดกลุ่มออกเป็น 5 กลุ่มคือ กลุ่มผู้บริหาร กลุ่มพนักงานพัฒนาระบบ User คู่ค้า และ outsource ซึ่งเรามีการจัดทำหลายรูปแบบ เช่น มีการอบรม มีจัดทำแบบ screen login ทุกเช้าว่าเราจะเตือนอะไร มีการจัดทำ infographic ซึ่งเราไม่ได้ทำเป็น Paper แปะ แต่เราเลือกช่องทางการสื่อสารผ่าน Line/Facebook/e-board /eLearning เรามีวิทยากรจากภายนอกและขออนุญาตบันทึกเพื่อนำมาใช้เป็นทรัพย์สินภายในและนำมาจัดทำเป็น Clip ใช้ในการ eLearning สร้างความตระหนักรู้ให้พนักงานเป็นคลิปสั้นๆประมาณ 3 นาที และมีตัวชี้วัดคือ แต่ละหน่วยงานภายในจะต้องมีพนักงานอบรมที่ไม่ต่ำกว่า 90% นอกจากนี้เรามีการทำ Phishing mail และถ้าทดสอบพนักงานแล้ว มีท่านใดตกเป็นเหยื่อก็จะต้องไปอบรม”

(ผู้ให้ข้อมูลสำคัญที่ 4, สัมภาษณ์เมื่อวันที่ 31 มีนาคม 2566)

“ถ้าเป็น security awareness ภายในองค์กร เราจะมีช่องทางสื่อสารภายใน เราจะไม่ใช่ช่องทางที่เป็นสาธารณะ เช่น Facebook เราไม่ใช้ เราใช้เป็นเว็บไซต์ภายในและไมโครซอฟต์ทีม มี email ภายในและจัด event ภายในในช่วงโควิด มี online training และปกติมีการจัดทำฟิชชิ่งเมล์ทุกปี อย่างน้อยปีละ 2 ครั้ง ในการอบรมบุคลากร จะ

แบ่งออกเป็น 2 กลุ่มคือกลุ่มเป็น bank wide และกลุ่มเฉพาะงานสำคัญก็จะมีการอบรมต่างหาก”

(ผู้ให้ข้อมูลสำคัญที่ 5, สัมภาษณ์เมื่อวันที่ 26 เมษายน 2566)

“สำหรับพนักงานในองค์กรทั้งหมด เราจะมีการสื่อสารโดยใช้เป็นสื่อเลือกว่าอีเมล ซึ่งเราจะทำ infographic แจ้งให้กับพนักงานในองค์กรผ่านทางอีเมล์ทุกๆเดือนเป็นอย่างน้อย นอกจากนี้ยังมีกิจกรรมที่เป็นเรื่องของประชาสัมพันธ์ในรูปแบบของเสียงตามสาย ซึ่งจะให้พนักงานที่เป็นสำนักงานใหญ่เองแล้วก็ทางสาขาเองได้ทราบซึ่งเขาจะมีระบบที่สามารถสื่อสารกันได้ผ่านทางช่องทางเสียตามสายเหล่านี้ นอกจากนี้ก็จะมีสื่อสังคมออนไลน์ที่เป็น internal นะคะสำหรับพนักงานที่เราจะเอามาตรการหรือวิธีปฏิบัติต่างๆไปแจ้งเตือนให้กับพนักงานสังคมออนไลน์เหล่านั้นด้วย นอกจากนี้จะมีการให้พนักงานได้เอ่อเป็น KPI ของพนักงานทุกคนในการทำการเรียน e-learning ซึ่งพื้นฐานก็คือเรื่องของความตระหนักรู้เบื้องต้น/พื้นฐานทางไซเบอร์ให้พนักงานทุกคนได้เรียน นอกจากนี้ก็จะมีการซักซ้อมเป็นอีเมล phishing อยู่สม่ำเสมอสำหรับพนักงานและผู้บริหารทุกท่าน ยกตัวอย่าง เช่นผู้บริหารจะเป็นคอร์สเรียนกับผู้บริหารค่ะเราอาจจะมีการให้ท่านเข้ามาร่วมในการเรียนกับเราโดยใช้ช่องทางไม่ว่าจะเป็นเรื่องของออนไลน์หรือเรียกเข้าห้องประชุมตอนที่มีโควิดก็จะใช้การออนไลน์ meeting งานแล้วตอนนี้ก็จะเป็นเหมือนกับห้องประชุมแล้วก็จัดขอ 30 นาทีให้กับท่านผู้บริหารบอร์ดพวกอย่างนี้ ส่วนของพนักงานทั่วไปก็อาจจะเป็นห้องประชุมซึ่งจะแยกหลักสูตรสำหรับของ outsource หรือผู้ให้บริการภายนอกเราก็จะมีการฝึกอบรมให้กับเขาเหล่านั้นโดยการที่ทางทีมเองอาจจะมีการจัดคอร์สขึ้นมาแล้วให้ผู้ที่มีส่วนได้ส่วนเสียเหล่านั้นเข้ามาร่วมกิจกรรมการฝึกอบรมกับเรา”

(ผู้ให้ข้อมูลสำคัญที่ 6, สัมภาษณ์เมื่อวันที่ 28 เมษายน 2566)

“1. พัฒนาทักษะบุคลากร ตามแนวทางพัฒนาคุณภาพ ระบบเทคโนโลยีสารสนเทศโรงพยาบาล หรือ HAIT : Healthcare

Accreditation Information Technology และ 2. อบรมเชิงปฏิบัติการ" หลักสูตรธรรมาภิบาลข้อมูล การรักษาความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลสุขภาพส่วนบุคคล หรือ Data Governance and Cyber Security and PDPA"

(ผู้ให้ข้อมูลสำคัญที่ 7, สัมภาษณ์เมื่อวันที่ 26 พฤษภาคม 2566)

"สพร. มีการกำหนดไว้ว่าจะต้องมีการจัดทำ cybersecurity awareness ปีละ 2 ครั้งเป็นอย่างน้อย แต่เราก็ทำเป็น standard ที่ควรเป็นของ ISO อยู่แล้ว แต่สิ่งที่เราทำมากกว่านั้นก็คือฝ่ายไซเบอร์เองจะติดตามพวกข่าวช่องโหว่ใหม่ๆหรือข่าวการโจมตีที่เกิดขึ้นไม่ว่าจะเป็นภายในประเทศ นอกประเทศ แล้วก็สรุปรวบรวมแล้วส่งสื่อสารภายในสำนักงานให้ทั้งฝั่งแอดมินภายในหรือบุคลากรต่างๆ รวมถึงแนวทางการป้องกันเราก็มีการทำลักษณะแบบที่องค์กรอยู่ตลอดเวลา"

(ผู้ให้ข้อมูลสำคัญที่ 9, สัมภาษณ์เมื่อวันที่ 30 มีนาคม 2566)

"สมช. มีการจัดอบรมหรือส่ง email เพื่อสร้างความตระหนักรู้ให้กับพนักงาน อาทิตย์ละ 1 ครั้ง ซึ่งเป็นแนวทางที่ สมช พยายามผลักดันมาโดยตลอดคือการสร้าง awareness และเราก็ยอมรับในบริบทอย่างนึงว่าการป้องกันเชิงระบบแทบจะทำอะไรไม่ได้เลยในปัจจุบัน แต่ว่าการป้องกันเชิงโครงสร้างที่เราทำได้คือการสร้าง awareness เช่น มีการแจ้งเตือนให้พนักงาน reset password ในระบบ email ทุกๆ 6 เดือน และในระบบ intranet ถ้ามีการเข้าใช้ข้างนอกจะต้องต่อ VPN"

(ผู้ให้ข้อมูลสำคัญที่ 11, สัมภาษณ์เมื่อวันที่ 19 เมษายน 2566)

"ในด้านการสร้างความตระหนัก จะมีการส่งเจ้าหน้าที่ไปอบรมกับ สกมช. และด้านเอกชน แต่มีงบประมาณที่จำกัด จะเลือกอบรมหลักสูตรฟรีเป็นส่วนใหญ่ มีการประชุมทุกเดือน"

(ผู้ให้ข้อมูลสำคัญที่ 13, สัมภาษณ์เมื่อวันที่ 25 เมษายน 2566)

“สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม มีการจัดทำองค์ความรู้ในรูปแบบของสื่อการเรียนการสอน รวมถึงสื่อเสริมสร้างความตระหนักรู้เช่น Infographic Video เสียงตามสาย เพื่อเสริมสร้างองค์ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศของหน่วยงานอยู่อย่างสม่ำเสมอ รวมถึงการศึกษาข้อมูลเกี่ยวกับภัยคุกคามที่เกิดขึ้นในปัจจุบันเพื่อนำมาประกอบการจัดทำสื่อ”

(ผู้ให้ข้อมูลสำคัญที่ 14, สัมภาษณ์เมื่อวันที่ 18 เมษายน 2566)

“ในส่วนของ พ.ร.บ. ไซเบอร์ เรามีหน่วยงานจัดฝึกอบรมโดยเฉพาะ โดยมีการแบ่งกลุ่มในการอบรมทั้งในระดับผู้บริหาร user และบุคลากรด้านไอที เพื่อสร้างความตระหนักรู้”

(ผู้ให้ข้อมูลสำคัญที่ 15, สัมภาษณ์เมื่อวันที่ 29 มีนาคม 2566)

“ในส่วนของ กองบังคับการปราบปรามการกระทำความผิดทางเทคโนโลยี นั้น จะมีการประชุมร่วมกับ นานาชาติ และมีการอัพเดท เทรน ของ cyber crime ต่างๆ ผ่านการประชุมหารือ หาความร่วมมือ รวมถึงการทำงานร่วมกับ หน่วยงาน นานาชาติ ไม่ว่าจะเป็น TCIU,HSI,INTERPOL ทำให้ในหน่วยงาน สามารถเข้าถึงและรับรู้ถึง ภัยคุกคามทางไซเบอร์ อยู่ตลอด ส่วนวิธีรับมือ กับการป้องกัน แก้ไขปัญหานั้น ได้มีการพัฒนาองค์ความรู้ ให้กับเจ้าหน้าที่ ในหน่วยงาน เพื่อให้เข้าใจและทราบถึง ภัยในรูปแบบใหม่อย่างสม่ำเสมอ มีการ เฝ้าระวังและหาข้อมูลข่าวสาร ในระดับ นานาชาติ มีการ ศึกษา จาก Darkweb และกลุ่มของ พวก hacker อย่างสม่ำเสมอ”

(ผู้ให้ข้อมูลสำคัญที่ 16, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

“ในการสร้างความตระหนักรู้ ด้านการเฝ้าระวังภัยคุกคามทางไซเบอร์และวิธีการรับมือ ป้องกัน แก้ไข ให้กับบุคลากรในองค์กร นั้น ทางหน่วยงานจะมีการจัดอบรมให้ความรู้ทางด้านอาชญากรรมทางเทคโนโลยีอยู่เสมอ การจัดหาอุปกรณ์เครื่องมือที่ทันสมัยและเหมาะสมให้แก่บุคคลากรเพื่อใช้ในการดำเนินการจัดการกรณี

อาชญากรรมทางเทคโนโลยี หรือการส่งไปอบรมกับเจ้าหน้าที่ระหว่างประเทศเพื่อแลกเปลี่ยนแนวคิดและวิธีการในการรับมือภัยคุกคามอาชญากรรมทางเทคโนโลยีต่างๆ”

(ผู้ให้ข้อมูลสำคัญที่ 17, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

“สร้างความตระหนักรู้ด้านความมั่นคงของระบบเครือข่าย โดยสร้างจิตสำนึกให้เจ้าหน้าที่ตำรวจในองค์กรตระหนักถึงอันตรายอันเกิดจากการละเลยด้าน security กำหนดกรอบแนวทางมาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ และให้หน่วยงานในสังกัดสำนักงานตำรวจแห่งชาติ ปฏิบัติตามมาตรฐานดังกล่าวด้วย รวมทั้งการพัฒนาบุคลากรและถ่ายทอดเทคโนโลยี การบริหารจัดการทางด้านเทคโนโลยีสารสนเทศที่ดี การประสานความร่วมมือระหว่างประเทศเพื่อความมั่นคงปลอดภัยทางไซเบอร์ การเตรียมความพร้อมทั้งในส่วน Database, Software, Hardware และ Network สำหรับภาคประชาชน ทางสำนักงานตำรวจได้สร้างระบบแจ้งความออนไลน์หรือสายด่วน 1441 เพื่อรับแจ้งการกระทำผิดทางไซเบอร์ที่เกิดขึ้นตลอด 24 ชม. จัดทำ Infographic สื่อสารผ่าน Facebook มีการผลักดันให้เกิดกฎหมายต่างๆ เพื่อให้ทันต่ออาชญากรรมทางไซเบอร์ที่มีรูปแบบอาชญากรรมเปลี่ยนแปลงอย่างรวดเร็ว มีการทำ MOU กับภาคเอกชนเพื่อผลิตสื่อไซเบอร์วัคซีน ร่วมสร้างความรู้ให้คนไทยเท่าทันกลโกงอาชญากรรมออนไลน์ เป็นต้น”

(ผู้ให้ข้อมูลสำคัญที่ 18, สัมภาษณ์เมื่อวันที่ 28 เมษายน 2566)

“ต้องให้บุคลากรจึงต้องมี Awareness เป็นเรื่องที่สำคัญ และที่สำคัญไปกว่านั้นคือการสร้างนิสัย ยกตัวอย่างเช่น กรณีใส่หมวกกันน็อค แต่บางคนไม่ใส่ ดังนั้นการบังคับใช้อาจไม่เพียงพอ และส่วนมากในเรื่องการบริหารจัดการที่เป็น Personal นั้น Awareness นั้นยังไม่พอ จึงต้องเป็นการสร้างนิสัย หรือ Habit Forming มากกว่า ยกตัวอย่างเพิ่มเติมเพื่อให้เห็นภาพยิ่งขึ้นเช่น คุณจะไม่เก็บขนมที่ตกพื้นขึ้นมากิน ซึ่งอันนี้เป็นเรื่องของนิสัยไม่ใช่เรื่องของวิชาการ เพราะเราถูกสั่งสอนมาตั้งแต่เด็กว่าของตกพื้นแล้วห้ามกิน พอหลังๆมาเรารู้

ว่ามันมีเชื้อโรคแม้ว่ามองไม่เห็นเชื้อโรค แต่ถ้าเราเห็นใครหยิบของตกพื้นขึ้นมากินหรือเพื่อนหยิบใส่ปากเรา มันจะรู้สึกขยะแขยง ซึ่งความขยะแขยงนี่คือ Habit Forming คือการสร้างนิสัยให้เกิดขึ้น เพราะฉะนั้น เราจะขยะแขยงทุกครั้งที่จะกดลิงก์ใน SMS หรืออีเมลอย่างนี้เป็นต้น ซึ่งยากเพราะการสร้างนิสัยแบบนี้ต้องสร้างตั้งแต่เด็กๆ ถ้าสร้างตอนโตเรียกว่า ไม้แก่ดัดยาก ดังนั้นกลุ่มคนที่เป็น Social Engineering จะรู้ว่าจะทำอย่างให้ที่จะหลอกล่อให้คนกดลิงก์ได้"

(ผู้ให้ข้อมูลสำคัญที่ 19, สัมภาษณ์เมื่อวันที่ 19 มีนาคม 2566)

"ภาครัฐควรมี Creative มาช่วยในการดำเนินการให้ชัดเจนขึ้น ซึ่งบางครั้งสิ่งที่อยากพูด กับสิ่งที่คนทั่วไปอยากฟังมักไม่ตรงกัน คนจึงไม่ค่อยสนใจ แล้วรัฐก็บริหาร Content ไม่เป็น เช่น เด็กกับผู้ใหญ่ ภาคไอทีกับภาคธุรกิจ หรือเช่น มีแก๊งคอลเซ็นเตอร์โทรมาล้านครั้ง แต่ตำรวจทำ Infographic เตือนภัยแชร์บน Facebook มีคนกดไลค์ 40 คน ก็คนละเรื่องกัน ถ้าจะทำให้คนพูดและคนฟังอย่างประชาชนเข้าใจง่ายขึ้นก็ต้องมี Creative ที่เชี่ยวชาญด้านการทำสื่อความรู้มาช่วย เช่น จะให้คนเห็นสื่อ 1 แสนคนต่อวัน แล้วจะต้องมีคนมา engagement เท่าไหร่ เรื่องนี้มันไกลเกินกว่าที่รัฐจะเข้าใจในด้านการเอาสื่อเข้าถึงประชาชน"

(ผู้ให้ข้อมูลสำคัญที่ 21, สัมภาษณ์เมื่อวันที่ 25 มีนาคม 2566)

สรุปได้ว่า จากการสร้างความตระหนักรู้ขององค์กรให้แก่ผู้มีส่วนได้ส่วนเสียของหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ หน่วยงานด้านการกำกับดูแลนโยบายและยุทธศาสตร์ หน่วยงานด้านกระบวนการยุติธรรม และประสบการณ์การให้ความรู้จากผู้เชี่ยวชาญ ซึ่งสามารถสรุปในลักษณะการเผยแพร่ความรู้ตามวิธีการต่างๆได้ ดังนี้

ตารางที่ 7 ช่องทางการสื่อสารการสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง (ข้อมูลจากการสัมภาษณ์)

ช่องทาง/ รูปแบบ/ วิธีการ	หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	หน่วยงานด้านการด้านการกำกับดูแลความมั่นคงปลอดภัยทางไซเบอร์	หน่วยงานด้านยุติธรรม
วารสาร Infographic	✓		✓
อบรมเชิงปฏิบัติการ	✓	✓	✓
สื่อการเรียนการสอน	✓	✓	
Website	✓	✓	✓
Line	✓	✓	
Facebook	✓	✓	✓
e-Board	✓		
e-Learning	✓		
e-Meeting	✓	✓	✓
ทดสอบ Phishing Mail	✓		
Open chat		✓	
Screen login	✓		
อื่นๆ (เช่น MOU, Poster, Email, เสียงตามสาย, โทรศัพท์)	✓	✓	✓

ทั้งนี้ ในมุมมองผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์เห็นว่า การสร้างนิสัยหรือ Habit Forming เป็นเรื่องที่สำคัญมากกว่าวิธีอื่นใด แต่อาจต้องมีการปลูกฝังลักษณะนิสัยมาตั้งแต่เยาว์วัย และภาครัฐควรมี Creative ด้านการสื่อสารหรือการใช้สื่อ Infographic มาช่วยในการดำเนินการให้ชัดเจนขึ้น เพราะการเตือนภัยผ่านช่องทาง Facebook อาจไม่ได้ผลเท่าที่ควร

4.4.3 ปัญหาและอุปสรรคในการรับมือและป้องกันภัยคุกคามทางไซเบอร์

ปัญหาจากสถานการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศทั้งด้านสาธารณสุขและด้านสาธารณูปโภค โดยส่วนมากมักจะนำไปสู่การหาผลประโยชน์ด้านการเงิน จนกลายเป็นภัยคุกคามทางไซเบอร์ที่กระทบต่อภาคการเงินการธนาคาร

โดยในปี ปี 2559 ธนาคารออมสิน ถูกแฮกเงินจากตู้เอทีเอ็ม โดยการสกรีมมิ่งโจรกรรมเงินจากบัญชีของลูกค้า ซึ่งจากการตรวจสอบพบว่า ถูกโจรกรรมเงินจากตู้เอทีเอ็มทั้งหมด 21 เครื่อง รวมเป็นเงินกว่า 12 ล้านบาท เป็นลักษณะการโจรกรรมเงินในกล่องเงินเครื่องเอทีเอ็ม โดยการติดตั้งอุปกรณ์สั่งการที่ตู้ และสามารถเสียบบัตรให้เงินออกมาได้ทันที ต่อมาในปี 2563 การไฟฟ้าส่วนภูมิภาค ถูกโจมตีจากมัลแวร์เรียกค่าไถ่ ส่งผลให้แอปพลิเคชัน PEA Smart Plus ไม่สามารถใช้งานได้ชั่วคราว ในขณะที่โรงพยาบาลสระบุรีถูกไวรัสโจมตี โดยแฮกเกอร์ได้ใช้ Ransomware เข้ารหัสข้อมูลคนไข้ในโรงพยาบาลสระบุรีทั้งหมด ซึ่งข้อมูลที่โดนเข้ารหัสนั้นล้วนเป็นข้อมูลคนไข้ในระบบซึ่งเป็นข้อมูลที่จำเป็นต่อการรักษา และวินิจฉัยโรคเป็นอย่างมาก ซึ่งถึงแม้ว่าทางโรงพยาบาลได้มีการแบคอัพข้อมูลบางส่วนเอาไว้บ้างแล้ว แต่ข้อมูลเหล่านั้นกลับเป็นข้อมูลเก่าตั้งแต่ปี 2558 ทำให้ไม่สามารถหยิบเอามาใช้ได้เลย และในปี 2564 โรงพยาบาลเพชรบูรณ์โดยแฮกข้อมูลผู้ป่วยไปขายบนเว็บไซต์ ซึ่งข้อมูลที่รั่วไหลออกไปไม่ได้เป็นข้อมูลหลักที่ใช้ในการให้บริการและมีประวัติการรักษาผู้ป่วย

สำหรับปี 2566 การประปาส่วนภูมิภาค สังกัดกระทรวงมหาดไทย ถูกปลอมแปลงเว็บไซต์องค์กร ซึ่งจากการตรวจสอบพบว่า เว็บไซต์ชื่อ https://pwa-co.cc/ ไม่ใช่เว็บไซต์ขององค์กรแต่อย่างใด เป็นการปลอมและเลียนแบบเว็บไซต์ที่มิจฉาชีพทำขึ้นมาเท่านั้น นอกจากนี้ ยังมีการใช้มัลแวร์เรียกค่าไถ่ (Ransomware) และการโจมตีด้วยการปล่อยไวรัสคอมพิวเตอร์ที่พบมากในหลายหน่วยงานด้านควบคุมกำกับดูแลและด้านการให้บริการ อีกทั้งการโจมตีแบบ Denial of Service (DoS) และ Distributed Denial-of-Service (DDoS) ไปยังเว็บไซต์ขององค์กรเพื่อเข้าถึงข้อมูลที่สำคัญ ทำให้ระบบปฏิเสธการให้บริการ หยุดชะงัก หรือระบบล่มไม่สามารถใช้งานได้ชั่วคราว

อย่างไรก็ตาม ภัยคุกคามที่มีลักษณะของการสแกนหาช่องโหว่ (Vulnerability) เพื่ออาศัยจุดอ่อนหรือข้อบกพร่องของโปรแกรมและระบบสารสนเทศ ในการเข้าถึงข้อมูลที่สำคัญขององค์กรนั้น สามารถต่อยอดกระบวนการก่ออาชญากรรมทางไซเบอร์ของอาชญากรในการปลอมแปลงเว็บไซต์ ขโมยข้อมูลไปขายในตลาดมืด หรือการโจรกรรมทางสินทรัพย์ เป็นต้น ขณะที่สถานการณ์ภัยคุกคามทางไซเบอร์ที่พบในประเทศไทยได้มุ่งเป้าไปยังหลายภาคส่วน โดยพบภัยคุกคามไซเบอร์ที่มีจุดประสงค์ทางการเงินในรูปแบบต่าง ๆ ที่พบมากที่สุด คือ ฟิชชิ่ง (Phishing) ซึ่งปัจจุบันเป็นภัยไซเบอร์ที่แฮกเกอร์ได้พัฒนากลวิธีในการหลอกลวงหลากหลายรูปแบบมากขึ้น เรียกว่า วิศวกรรมเชิงสังคม (Social engineering) เช่น ฟิชชิ่งอีเมล เพื่อหลอกให้กดลิงก์เพื่อเข้าถึงข้อมูลทางการเงินของบุคคล หรือเข้าถึงระบบฐานข้อมูลสำคัญขององค์กร การฝากลิงก์ปลอมบนเว็บไซต์องค์กรไปสู่เว็บ

พนัน การส่ง SMS หลอกล่อชักจูงด้วยผลตอบแทนเป็นรางวัลที่เกินจริง ดังนั้นกลุ่มคนที่เป็น Social Engineering จะมีความชำนาญและรู้ว่าจะทำอย่างไรเพื่อที่จะหลอกล่อให้คนกดลิงก์ได้

จากการสัมภาษณ์ผู้ให้ข้อมูลสำคัญ สิ่งที่น่าสนใจของผู้ให้ข้อมูลจากสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งสรุปได้เป็น 3 ประเด็นดังนี้

1) คนหรือบุคลากร

บุคลากรด้าน security หรือ คน IT แต่ได้รับมอบหมายหน้าที่ให้ดูแลทางด้าน cybersecurity ยังขาดความรู้ความเข้าใจในด้านเทคนิค ทั้งเรื่องของการขาดความรู้ด้วยส่วนหนึ่งแล้วอีกประการคือเรื่องของจำนวนหรือปริมาณของคนที่มีความรู้ความสามารถเพียงพอในการทำงานด้านนี้ที่เป็นหน่วยของรัฐแล้วก็หน่วยงาน CII รวมถึงหน่วยงานเอกชน ซึ่งตลาดตรงนี้ขาดไปมาก ทั้งขาดคนในเรื่องของจำนวนและขาดคนคุณภาพและความสามารถจริงๆด้วย

2) ระบบหรืออุปกรณ์

หน่วยงานจำนวนมากที่มีงบประมาณที่สามารถจัดซื้อหรือจัดหาอุปกรณ์ที่จำเป็นได้ แต่ว่า ณ ปัจจุบัน ปัญหาของระบบอุปกรณ์ นอกจากเรื่องของงบประมาณที่มีจำกัดในบางที่จะมีความเหลื่อมล้ำกันอยู่พอสมควร ปัญหาสำคัญมากๆคือ การจัดซื้อของให้เป็นไปตามการนำเสนอของ vendor ซึ่งอยู่บนพื้นฐานความเชื่อหรือความคาดหวังว่าตัวระบบหรืออุปกรณ์จะสามารถป้องกันอะไรต่างๆนานาได้ ทั้งที่ตามข้อเท็จจริง การปกป้องในด้าน cybersecurity ไม่สามารถที่จะพึ่งพาเฉพาะอุปกรณ์ได้ ดังนั้นการลงทุนทางด้าน cyber ที่ผ่านมาอาจจะไม่ได้ตอบโจทย์ที่แท้จริง แม้ว่าบางแห่งจะมีเงินลงทุนแต่ก็ยังไม่ได้ตอบโจทย์เพราะต้องพึ่งเรื่องของคนในองค์กร เรื่องของความรู้ความเข้าใจ เรื่องของกระบวนการจัดการต่างๆด้วยไม่ใช่แค่เรื่องของอุปกรณ์

3) กระบวนการ มาตรการ กฎหมาย ข้อบังคับต่างๆ

พ.ร.บ. ไซเบอร์ เป็นกรอบหรือกฎหมายที่ใหญ่ที่สุดที่จะเป็นแนวทางมาตรการหรือกึ่งมาตรการที่ควบคุมให้เกิดความปลอดภัย เป็นแนวทางหรือว่าเป็นมาตรการหรือกึ่งมาตรการในการควบคุมให้เกิดความปลอดภัย โดยธรรมชาติของของ พ.ร.บ. ไซเบอร์ 2562 ไม่ได้มีลักษณะเป็นการบังคับ แท้จริงก็คืออาจจะมีการปฏิบัติราชการกำหนดโทษประกอบ แต่ว่า พ.ร.บ. ไซเบอร์ 2562 จะเป็นลักษณะของการเป็น Guideline หรือเป็นแนวทางหรือว่าเป็นคล้ายๆคู่มือที่จะให้หน่วยงานสำคัญๆมีแนวทางในการควบคุมที่เขาเรียกว่า baseline หรือว่าขั้นต่ำในการปฏิบัติเท่านั้นยังไม่ได้มีไปถึงขั้นที่จะทำให้ผู้รับผิดชอบหรือว่าหน่วยงานเกิดความรู้สึกหรือว่าอยากที่จะร่วมมืออย่างเต็มที่ เพราะว่า ไม่มีคำว่าบังคับหรือบทลงโทษที่ชัดเจน จริงๆก็ถือว่าเป็นปัญหา แต่บางคนอาจจะคิดว่าไม่ใช่ปัญหาก็ได้ เพราะถือว่าเป็นไปโดยธรรมชาติ เป็นวัฒนธรรมของคนที่อยู่ในองค์กร ซึ่งในประเทศนี้มักทำสิ่งที่ที่ต้องทำเพราะว่ามันมีอะไรบังคับอยู่ แต่ว่าการที่จะสมัครใจทำหรือว่าเข้าใจ

ความสำคัญของสิ่งที่ประกาศออกมาเพื่อให้เราสามารถที่จะป้องกันหรือควบคุมได้ดีขึ้น เรามักจะไม่ค่อยให้ความสำคัญ อันนี้คือในส่วนของ พรบ ไซเบอร์

มากกว่านั้นคือ **ระบบวิธีคิดในระดับบุคคล** ยังมุ่งเน้นในเรื่องของการใช้งานของระบบหรือของอุปกรณ์โดยที่ยังขาดความตระหนักในเรื่องความปลอดภัย ด้วยวิธีคิดแบบนี้ก็จะทำให้เกิดช่องโหว่หรือเกิดความเสี่ยงเกือบจะตลอดเวลาที่มีการใช้งาน เช่น มีการตั้งพาสเวิร์ดด้วยเลขบัตรประชาชนหรือหมายเลขโทรศัพท์ ซึ่งถ้าเกิดความไม่เข้าใจตรงนี้ ก็จะส่งผลกระทบเยอะเพราะจะทำให้ถูกแฮกได้ง่าย อีกประการคือ **ระบบวิธีคิดในระดับองค์กร** ผู้เกี่ยวข้องโดยตรงที่เป็นแผนกทางด้านไซเบอร์หรือไอทีที่ปฏิบัติงานด้าน cybersecurity ยังอยู่ในกรอบหรืออยู่ใน mindset ที่มุ่งการให้บริการเป็นหลัก หมายถึง ให้ระบบตรงนั้นสามารถเดินไปได้ โดยการที่ระบบดำเนินไปได้อาจจะมองข้ามเรื่องความปลอดภัยไปทำให้มีผลกระทบ จะเห็นได้ว่า ทั้งระดับบุคคลและองค์กรในกระบวนการเกี่ยวข้องก็จะเป็นจุดอ่อน ซึ่งจากความคิดเห็นดังกล่าวมีความคล้ายคลึงกับผู้ให้ข้อมูลสำคัญคนที่ 7 ที่อธิบายถึงปัญหาและอุปสรรคที่แบ่งออกเป็น 2 กรณี คือ

กรณีที่ 1 สำหรับบุคคล ได้แก่

(1) ไม่ระมัดระวังในการใช้อินเทอร์เน็ต โดยหลีกเลี่ยงการเข้าไปยังเว็บไซต์ที่ไม่เหมาะสม ไม่เปิดไฟล์ที่ไม่ มีการตรวจสอบแน่ชัดหรือเปิดไฟล์จาก บุคคลที่ไม่รู้จัก และระมัดระวังการเปิดไฟล์ผ่าน Social Media ทั้งนี้เพื่อหลีกเลี่ยงพวกมัลแวร์

(2) ไม่ใช้รหัสผ่านบน โลก cyber เป็นรหัสชุดเดียวกันทุกระบบ

3) ไม่ติดตามข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัย และพิจารณาข้อมูลก่อนการแชร์ข้อมูลต่อเพื่อป้องกันตนเองเป็นต้นตอ ต่อการส่งแพร่กระจายไวรัส

กรณีที่ 2 สำหรับหน่วยงาน ได้แก่

1) ไม่มีระบบตรวจสอบและยืนยันสิทธิการเข้าระบบที่สำคัญของบัญชีผู้ใช้ให้สอดคล้องกับความจำเป็นในการ เข้าถึงระบบและข้อมูล

2) ไม่มีการเพิ่มมาตรการป้องกันเว็บไซต์สำคัญด้วยระบบป้องกันการโจมตีของ ไวรัส Web Application Firewall หรือ DDoS Protection

3) ไม่แจ้งเจ้าหน้าที่ของหน่วยงานให้เพิ่มความระมัดระวังในการใช้อินเตอร์เน็ต โดยหลีกเลี่ยงความเหมาะสม ป้องกัน ข้อความจาก Social Media

4) ขาดการตรวจสอบเมื่อหากพบพิรุธว่าระบบถูกโจมตี เช่น ไม่สามารถเข้าใช้งานระบบ/เว็บไซต์ได้หรือมีความล่าช้าปกติควรตรวจสอบ Log การ login ย้อนหลังทุกๆ เดือน

5) ไม่ตั้งค่าระบบงานที่สำคัญให้บันทึกเหตุการณ์ต่างๆตามที่กฎหมายกำหนดไว้

จากเหตุผลดังกล่าวข้างต้น สอดคล้องกับความคิดเห็นของผู้ให้ข้อมูลสำคัญทั้งด้านหน่วยงานโครงสร้างพื้นฐานสารสนเทศ หน่วยงานควบคุมและกำกับดูแล รวมถึงหน่วยงานด้านการป้องกันและปราบปรามและผู้เชี่ยวชาญด้านไซเบอร์ ดังนี้

“สำหรับปัญหาอุปสรรคที่เราพบเจอคือ อุปกรณ์ที่ที่เราใช้อยู่นั้นมีอายุการใช้งานที่ยาวนาน อย่างระบบเครือข่าย 10 ปี แล้ว ซึ่งอุปกรณ์บางชิ้น บางยี่ห้อ จะเป็นลักษณะของ end of support ไปแล้วทำให้ช่องโหว่ยังมีอยู่ สิ่งที่การประปาส่วนภูมิภาคแก้ปัญหาคือ มีการดำเนินการในรูปแบบของการจัดซื้ออุปกรณ์มาเพื่อทดแทนเพิ่มเติมในส่วนของทางด้านความมั่นคงปลอดภัย หลังจากนั้น มีโครงการปรับปรุงสื่อสัญญาณและโครงการ upgrade ระบบเครือข่ายไร้สาย รวมทั้งโครงการวงแหวนหลายชั้นที่จะดำเนินการในปีนี้”

(ผู้ให้ข้อมูลสำคัญที่ 2, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

“ไม่มีปัญหาและอุปสรรคอะไรที่เป็นพิเศษ เนื่องจาก ธปท. ผู้ว่าการตลอดจนถึงผู้บริหารให้ความสำคัญเรื่อง cybersecurity มีการรายงานคณะกรรมการ ในแง่ของงบประมาณได้รับอย่างเพียงพอ เป็น % ที่ค่อนข้างสูง เมื่อเทียบกับองค์กรภาคีในภาพรวม ถ้าจะมีบ้างก็ในเรื่องของคน ซึ่งแบงก์เองก็จะมีการกำหนดตำแหน่งงาน ที่เพียงพอให้กับเรา แต่ปัญหา Recruit คนให้เพียงพอเหมาะกับงานมากกว่า Pool ของคนจะมีไม่เยอะในประเทศไทย ส่วนเรื่องคุณสมบัติของคนในเรื่องของ Cyber จะมี Spectrum ที่ค่อนข้างกว้าง จริงๆแล้ว ดีกรีอาจจะเป็นจุดเริ่มต้นมากกว่า ไม่เจาะจงว่าต้องจบคอม แต่เรามองหาผู้ที่มีประสบการณ์ด้านไซเบอร์ และสิ่งที่เราต้องการคือ จะต้องมี Mindset ที่ใฝ่รู้ เพราะด้านไซเบอร์ภัยนั้นมีการพัฒนาไปเรื่อย ๆ เพราะฉะนั้นเราต้องวิ่งตามและเข้าใจภัยใหม่ๆที่เกิดขึ้น และคนที่จะมาต้องมี Growth Mindset ค่อนข้างดี เนื่องจากมีการพัฒนาด้านไซเบอร์และมีภัยใหม่ๆแทบทุกเดือน เพราะฉะนั้นคนที่อยู่ตรงนี้ได้ แต่เราไม่ได้ Require ที่สูงมากที่ต้องได้รับใบประกาศ แต่เราได้ส่งบุคลากรไปอบรม และสอบเซอร์ด้านไซเบอร์ และมี Awareness ให้พนักงาน”

(ผู้ให้ข้อมูลสำคัญที่ 5, สัมภาษณ์เมื่อวันที่ 26 เมษายน 2566)

“อุปสรรคของเราคือด้าน บุคลากรด้าน security เองที่มีความชำนาญ ค่อนข้างมีจำกัด และหายาก ตามองค์กรต่างๆก็จะมีการดึงตัวและซื้อตัวกันไป อย่างเราก็มีทีมงานที่ซื้อตัวโดยองค์กรอื่นไป และมีการลาออกอยู่บ้าง จึงเป็นประเด็นเป็น GAP ในเรื่องการยกระดับให้กับองค์กรไปว่าตอนนี้ทางหน่วยงานเองมีปัญหาในเรื่องของบุคลากร เพื่อขอปรับโครงสร้าง และขออัตรากำลังเพิ่มขึ้น แต่อย่างไรก็ตามก็จะมีข้อจำกัดในหลายๆด้านคือ 1. องค์กรให้เท่าที่จำเป็น 2. เรื่องของคนที่จะเข้ามาทำกับเรา ด้วยเราเป็นแบงก์ที่เป็นรัฐวิสาหกิจรัฐบาล อัตราตอบแทนค่าจ้างก็จะเป็นไปตามพื้นฐานที่ไม่สูงมาก ดังนั้นบุคคลที่จะเข้ามาทำงานกับเราจึงค่อนข้างที่จะไม่ได้ผู้เชี่ยวชาญ ด้วยผลตอบแทนตรงนี้ไม่ได้เป็นสิ่งจูงใจให้กับคนภายนอก ก็จะใช้วิธีการจ้างเหมาบริการจัดการจ้างเหมาคือจ้างเป็นโครงการไป เป็นโครงการให้ผู้บริการภายนอกซึ่งมีความเชี่ยวชาญมาดูแลเรา”

(ผู้ให้ข้อมูลสำคัญที่ 6, สัมภาษณ์เมื่อวันที่ 28 เมษายน 2566)

“ผมมองว่าแม้ว่าเรามีการลงทุนแค่ไหนก็ไม่สามารถป้องกันได้ 100% เพราะฉะนั้นปัญหาที่สำคัญคือ แค่ไหนถึงจะเหมาะสมของแต่ละหน่วยงานไม่เหมือนกัน ดังนั้น แต่ละหน่วยงานคงต้องประเมินความเสี่ยงตัวเอง ว่าแค่ไหนยอมรับได้ แค่ไหนยอมรับไม่ได้ อันที่ยอมรับไม่ได้ก็ต้องหา Process people technology มาปิดเพื่อให้ความเสี่ยงลดลงจนถึงอยู่ในเกณฑ์ที่ยอมรับได้ ซึ่ง ณ ตอนนี้ สพร. มี process ต่างๆ ไม่ว่าจะเป็น incident response plan /BCP /BCM/ cybersecurity policy เหล่านี้เป็นตัวที่เรานำมากดค่าความเสี่ยงให้ลดลงและอยู่ในเกณฑ์ที่ สพร. ยอมรับได้”

(ผู้ให้ข้อมูลสำคัญที่ 9, สัมภาษณ์เมื่อวันที่ 30 เมษายน 2566)

“ในบริบทของการป้องกันภัยในมุมมองของ เหยื่อ อาจจะกล่าวได้ว่า ทางหน่วยงาน ของ ปอท.เอง ได้มีการพยายามประชาสัมพันธ์ ให้ความรู้กับประชาชน อย่างต่อเนื่องแล้วก็ตาม แต่ด้วย การพัฒนาทางเทคโนโลยี ที่รวดเร็ว และความรู้พื้นฐานด้านการ

ป้องกันตัวเองของประชาชน หรือ องค์กรต่างๆยังไม่รู้เท่าทัน กับผู้ก่อเหตุ ด้านการสืบสวนจับกุมผู้ก่อเหตุ ที่เป็นไปด้วยความยาก เนื่องมาจาก การก่อเหตุต่างๆ สามารถกระทำจากที่ใด ก็ได้ ฉะนั้นการจะสืบสวน ระหว่างประเทศ ย่อมต้องใช้เวลา และความร่วมมือระหว่างประเทศ จะต้องมีการศึกษาข้อกฎหมายของแต่ละประเทศ โดยภาพรวม ปัจจุบันแล้ว เป็นไปได้ยาก และล่าช้า ก่อให้เกิด ช่องว่าง ทำให้ ผู้ก่อเหตุ สามารถรอดจากการสืบสวนจับกุม และก่อเหตุซ้ำได้เรื่อย ๆ ด้านกฎหมาย พรบ.คอมฯมีการอัพเดท ล่าสุดคือปี 2560 ซึ่งหากมอง การพัฒนา ด้านเทคโนโลยี ระหว่างปี 2560-ปัจจุบัน มีการพัฒนาแบบก้าวกระโดด ส่งผลให้ ในการกระทำความผิดบางเคสจะต้องมีการตีความตัวบทกฎหมายกันยาก ตัวอย่างเช่น ทรัพย์สินดิจิทัล ต่างๆ ไม่ว่าจะเป็น คริปโต, เงินในกระเป๋า payment ต่างๆ หรือแม้กระทั้ง code ลดราคา ซึ่ง มีการก่อเหตุ กันบ่อยครั้ง และยังเป็นปัญหาด้านการตีความ"

(ผู้ให้ข้อมูลสำคัญที่ 16, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

"ในกรณีของผู้ปฏิบัติหน้าที่ จะประสบปัญหาในเรื่องของเครื่องมือที่ใช้ในการสืบสวน การขาดแคลนผู้เชี่ยวชาญเฉพาะด้าน หรือการสร้างความเข้าใจกับประชาชนในด้านของอาชญากรรมทางเทคโนโลยี เพราะ บางครั้งก็เป็นเรื่องใหม่ สำหรับประชาชน"

(ผู้ให้ข้อมูลสำคัญที่ 17, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

"ปัญหาหลักของภาครัฐคือ 1. ขาดแคลนทุนทรัพยากร และขาดแคลนบุคลากรที่มีความรู้ความสามารถด้านเทคโนโลยี โดยเฉพาะด้านความมั่นคงปลอดภัยไซเบอร์ 2. การบริหารงานภาครัฐยังมีความล่าช้า เนื่องจากต้องปฏิบัติตามหลายขั้นตอนและต่อเนื่อง"

(ผู้ให้ข้อมูลสำคัญที่ 18, สัมภาษณ์เมื่อวันที่ 28 เมษายน 2566)

"ปัญหาคือ แต่ละรัฐพอรับกฎหมายและนโยบายก็จะ Compile Standard และสั่งให้จัดซื้อจัดจ้าง ซึ่งส่วนใหญ่ก็จ้าง outsource การรั่วไหลจึงอยู่ที่ third party นอกจากนี้ปัญหาที่สำคัญ

ที่สุดคือ 1. ผู้บริหารไม่มีวสัยทัศน์ 2. ไม่มีการสร้าง Awareness ให้องค์กร เนื่องจากมีภัยเกิดขึ้นใหม่ทุกวัน และทุกองค์กรควรจะต้องเชิญผู้เชี่ยวชาญมาอัพเดตเรื่องใหม่ๆตลอดเวลา 3. ควรให้มีทีมงานในองค์กรที่คอยติดตามความเคลื่อนไหว หรือเรื่องใหม่ๆที่เกิดขึ้นในประเทศไทย เพื่อมาปรับปรุงนโยบายต่อไป"

(ผู้ให้ข้อมูลสำคัญที่ 21, สัมภาษณ์เมื่อวันที่ 21 มีนาคม 2566)

"หากมองในด้านของปัญหาการบริหารในองค์กรที่มาจากผู้บริหาร ยกตัวอย่างเช่น เรื่องถังดับเพลิง ที่หลายบ้านไม่มีเพราะมองว่า 1. หากมีไว้ในบ้านจะถือว่าเป็นลางร้าย 2. เปลืองเงินเพราะถังดับเพลิงมีราคาสูง นี่คือการบริหารจัดการ แม้รู้ว่ามีความจำเป็นและมีอันตรายอยู่รอบตัว แต่บางบ้านยังไม่มีถังดับเพลิง เพราะเรื่องที่จำเป็นสำหรับพวกเขาที่มีมากกว่าคือซื้อข้าวใส่ท้อง เปรียบได้กับในองค์กร ที่มองเห็นความจำเป็นของการดูแลลูกค้า การขยายสาขา มากกว่าเรื่องของ Security เพราะเรื่อง Security เป็น Infrastructure ซึ่งเป็นการลงทุนที่ไม่เห็นผลในทันทีกับผลประโยชน์ขององค์กร เพราะฉะนั้นในเชิง Business ก็มักจะไม่ทำหรือมี Priority ที่ต่ำ ฉะนั้น ช่วงหลังๆมานี้เมื่อเกิดภัยคุกคามมากขึ้น เช่น เกิดเหตุที่โรงพยาบาลสระบุรี ก็เริ่มมีแนวทางป้องกันเพื่อบังคับใช้มากขึ้น"

(ผู้ให้ข้อมูลสำคัญที่ 19, สัมภาษณ์เมื่อวันที่ 19 มีนาคม 2566)

สรุปได้ว่า ปัญหาและอุปสรรคสำคัญที่เกิดขึ้นกับองค์กรส่วนใหญ่ คือ งบประมาณที่ไม่เพียงพอและทรัพยากรที่มีอยู่อย่างจำกัด หลายหน่วยงานจึงแก้ปัญหาด้วยการจัดลำดับความสำคัญของสิ่งที่จะทำภายใต้งบประมาณที่จำกัด รวมถึงตามอายุการใช้งานของคอมพิวเตอร์และอุปกรณ์ขององค์กร และปรับปรุงนโยบายการกำกับดูแลกิจการที่ดีด้านเทคโนโลยีดิจิทัล หรือ GRC ที่หน่วยงานโครงสร้างพื้นฐานทางสารสนเทศให้ความสำคัญ โดยคาดหวังให้ผู้บริหารองค์กรและหน่วยงานภาครัฐที่เกี่ยวข้องด้านการจัดสรรงบประมาณให้องค์กร มีความตระหนักและเล็งเห็นความสำคัญของการลงทุนด้านความปลอดภัยทางไซเบอร์มากยิ่งขึ้น

4.5 การอภิปรายผลการศึกษา

จากผลการศึกษาวิจัยเรื่อง แนวทางการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ขององค์กรในยุคดิจิทัล เมื่อพิจารณาผลการวิจัยตามวัตถุประสงค์ทั้ง 3 ข้อ สามารถอภิปรายผลการวิจัยที่น่าสนใจได้ ดังนี้

4.5.1 สถานการณ์ภัยคุกคามไซเบอร์หน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศด้านสาธารณสุข สาธารณูปโภค และการเงินการธนาคาร

4.5.1.1 ภัยคุกคามทางไซเบอร์

สถานการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศด้านสาธารณสุข สาธารณูปโภค และการเงินการธนาคารในประเทศไทยในการบุกรุกเข้าถึงฐานข้อมูลและส่งผลกระทบกับข้อมูลที่สำคัญขององค์กร พบว่า เป็นมัลแวร์ประเภทแรนซัมแวร์ (Ransomware) ทำให้คอมพิวเตอร์ด้อยประสิทธิภาพและผู้ใช้งานระบบไม่สามารถเข้าใช้งานได้เนื่องด้วยมีการล็อครหัสไฟล์ข้อมูลไว้ และโยงใยไปสู่กระบวนการเรียกค่าไถ่ ที่เป็นเช่นนี้เนื่องมาจาก ข้อมูลที่หลุดออกไปเป็นข้อมูลอ่อนไหวอย่างข้อมูลส่วนบุคคล คนร้ายจึงสามารถใช้เป็นเครื่องต่อรองและหาประโยชน์ทางการเงินเพื่อแลกกับการปลดล็อกรหัส ผลการวิจัยนี้สอดคล้องกับผลการศึกษาวิจัยของ Sangtongdee & Youngyuen (2020) เรื่อง แนวทางการรับมือและรับแจ้งเหตุของตำรวจต่อกรณีมัลแวร์เรียกค่าไถ่ และพบว่า มัลแวร์แบบเข้ารหัส เป็นการโจมตีเหยื่อด้วยรูปแบบการเข้ารหัสไฟล์และโฟล์เดอร์ส่วนบุคคล เช่น เอกสาร รูปภาพ ไฟล์ตาราง และวิดีโอ ทำให้ไฟล์เหล่านั้นถูกลบทันทีเมื่อมีการเข้ารหัส จากนั้น ผู้ใช้งานจะได้รับไฟล์ข้อความแสดงขั้นตอนจ่ายค่าไถ่ซึ่งจะอยู่ในโฟล์เดอร์เดิมที่ไฟล์ถูกลบทิ้งไป และจะมีเนื้อหาของข้อความแจ้งวิธีการเข้าถึงเว็บไซต์เพื่อชำระเงิน และท้ายที่สุด คนร้ายจะแจ้งข้อความเป็นตัวอักษรและตัวเลขซึ่งเป็นกุญแจสาธารณะสำหรับนำไปยืนยันเมื่อเหยื่อชำระเงินผ่านระบบของคนร้าย

นอกจากนี้ การโจมตีในรูปแบบ Distributed Denial-of-Service (DDoS) Attack ที่ทำให้เว็บไซต์ของเหยื่อล่มไม่สามารถใช้งานได้นั้น ปัจจุบันหลายองค์กรเผชิญกับภัยคุกคามลักษณะเช่นนี้อยู่บ่อยครั้ง ทั้งนี้อาจเนื่องมาจาก มีการนำอุปกรณ์ภายนอกมาใช้เชื่อมต่อกับคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ภายในองค์กรโดยไม่มีการตรวจสอบหรือเฝ้าระวังจากผู้ดูแลระบบ หรือไม่มีการป้องกันที่เพียงพอ เช่น ไม่มีโปรแกรม Antivirus หรือโปรแกรมไม่มีการอัพเดตแพตช์เป็นเวลานาน ทำ

ให้ระบบการป้องกันที่มีอยู่ ไม่สามารถตอบสนองต่อภัยคุกคามใหม่ๆได้ ซึ่งสอดคล้องกับผลการศึกษาวิจัยของ นัทธมน เพชรกล้า (2564) เรื่อง การรับมือของภาครัฐกับการก่อการร้ายทางไซเบอร์ในประเทศไทย ที่พบว่า ในปี 2007 ประเทศเอสโตเนีย ถูกโจมตีด้วยคำสั่ง ดีดีโอเอส (DDoS) ด้วยการระดมคำสั่งเพื่อโจมตีเครื่องเซิร์ฟเวอร์ ส่งผลให้การบริการโดยโครงข่ายอินเตอร์เน็ตทั้งหมดถูกระงับ ประชาชนเอสโตเนียไม่สามารถใช้บริการเว็บไซต์ สื่อ หรือบริการอิเล็กทรอนิกส์ของรัฐบาลได้

ข้อค้นพบอีกประเด็นหนึ่งของโจมตีระบบด้วย DDoS มาจากวิธีการที่แฮกเกอร์พยายามสแกนหาช่องโหว่เพื่อให้เข้าถึงระบบเครือข่ายโดยมีเป้าหมายของการเข้าถึงข้อมูลองค์กร โดยอาศัยจุดบกพร่องของโค้ดที่โปรแกรมเมอร์เขียนไว้ไม่รอบคอบ หรือเป็นข้อผิดพลาดจนเกิดเป็นช่องโหว่ที่ไม่สามารถป้องกันการโจมตีได้ ซึ่งอาจส่งผลให้แฮกเกอร์สามาถเข้าไปทำลาย ขโมยข้อมูล จนทำให้เกิดการหยุดชะงัก และปฏิเสธการใช้งาน สอดคล้องกับแนวคิดทฤษฎีการโจมตีทางไซเบอร์ (Cyber Attack Theory) ของ Rui Zhuang, Alexandra G. Bardas, Scott A.Deloach และ Xinming Ou (2015) ที่พบว่า ผู้โจมตีพยายามหาช่องโหว่ในการวางแผนการโจมตี และหากมีช่องโหว่อยู่ ผู้โจมตีสามารถใช้ประโยชน์จากช่องโหว่นั้นเพื่อเข้าถึงข้อมูลในคอมพิวเตอร์หรืออุปกรณ์ที่เป็นเป้าหมายใจการโจมตีได้

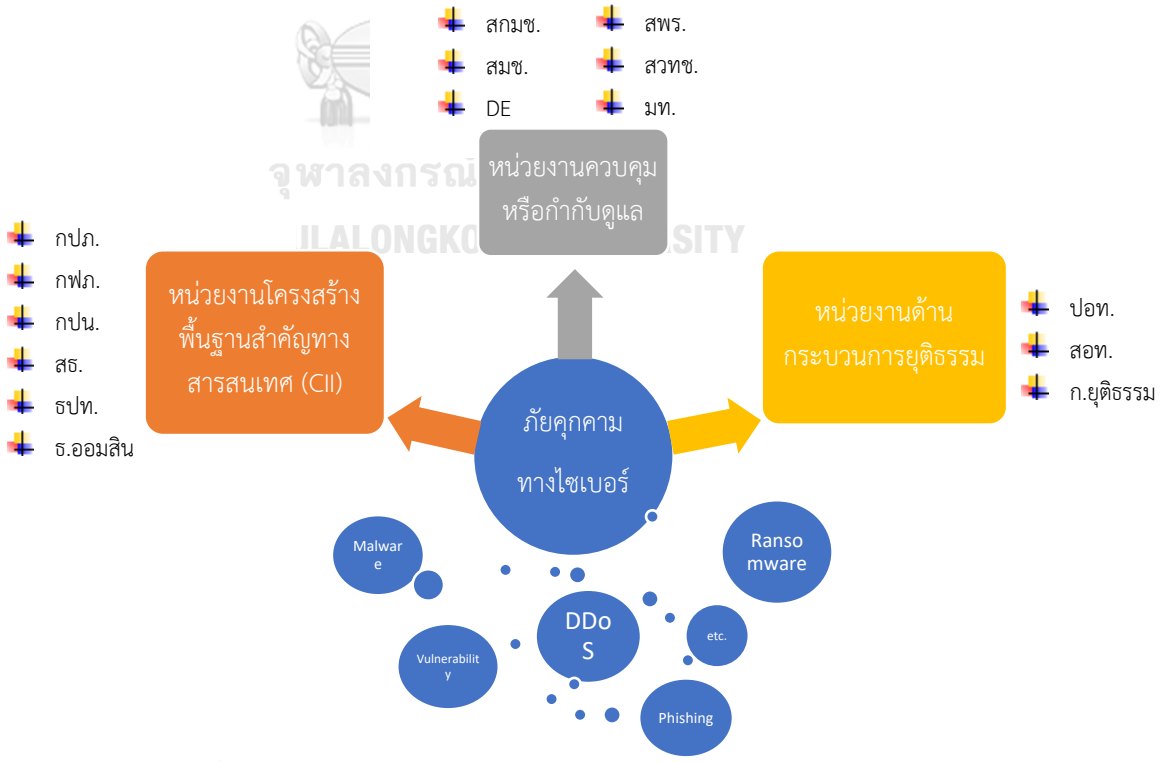
อย่างไรก็ตาม แม้ว่าสถานการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในประเทศไทย ยังอยู่ในระดับที่ไม่ร้ายแรง แต่ภัยคุกคามทางไซเบอร์ยังคงเพิ่มมากขึ้น ทั้งภัยคุกคามที่เคยเกิดขึ้นมาแล้วและภัยคุกคามที่ยังไม่เคยเกิดขึ้นมาก่อน อันเกิดจากผู้ไม่ประสงค์ดีมุ่งเป้าโจมตีหน่วยงานหรือองค์กร หรือบุคคล เพื่อแสวงหาผลประโยชน์ทั้งในด้านทรัพย์สิน ชื่อเสียง หรือแม้แต่สนองความคึกคะนองของตนเอง จนนำไปสู่การก่ออาชญากรรม โดยเฉพาะการโจมตีไปยังระบบคอมพิวเตอร์และเครือข่าย หรือระบบสารสนเทศของหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสนเทศ เช่น โรงพยาบาล การไฟฟ้า การประปา สถาบันการเงิน ส่งผลกระทบในวงกว้างต่อภาครัฐ ภาคเอกชน ไปจนถึงประชาชน ทั้งนี้เนื่องมาจากคนร้ายพยายามใช้วิธีการใหม่ๆกับเป้าหมายหรือเหยื่อหรือองค์กรที่มีข้อมูลที่สำคัญ เพื่อไม่ให้เหยื่อรู้ตัวหรือรู้วิธีการป้องกันจากการเรียนรู้จากประสบการณ์ที่ผ่านมาในลักษณะที่เคยเกิดขึ้นมาแล้ว

ผลการวิจัยนี้สอดคล้องกับทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) และปัจจัยที่ทำให้เกิดภัยคุกคามทางไซเบอร์และอาชญากรรมไซเบอร์ ของ George W. Reynolds (2012) ที่จำแนกการเกิดอาชญากรรมไว้ 3 องค์ประกอบคือ (1) คนร้ายหรือผู้ไม่ประสงค์ดีใช้ข้อผิดพลาดหรือจุดบกพร่องของผู้ใช้งานคอมพิวเตอร์ในการเข้าถึงระบบหรือข้อมูล (2) เหยื่อหรือเป้าหมาย เช่น คอมพิวเตอร์หรือวัตถุที่คนร้ายมุ่งหมายเข้าควบคุมมีความซับซ้อนมากขึ้น โดยสามารถ

ปฏิบัติการได้หลายระบบที่ทำงานอยู่บนคอมพิวเตอร์แม่ข่ายที่เดียว ทำให้ยากต่อการป้องกันความปลอดภัย และ (3) โอกาสที่เหมาะสม เช่น สถานที่และเวลาที่คนร้ายสามารถกระทำผิดหรือก่ออาชญากรรมได้ ซึ่งสำหรับยุคดิจิทัล การใช้แพลตฟอร์มต่างๆ เช่น Facebook, Line หรือ YouTube เป็นแหล่งของข้อมูลที่คนร้ายใช้เป็นเครื่องมือในการก่อเหตุภัยคุมคามทางไซเบอร์ ซึ่งการใช้งานอินเตอร์เน็ตและแอปพลิเคชันเหล่านี้ มีสถิติการใช้งานเพิ่มมากขึ้นอย่างรวดเร็ว การขยายตัวและการเปลี่ยนแปลงของระบบเครือข่ายคอมพิวเตอร์เท่ากับความเสี่ยงใหม่และปัญหาใหม่ที่จะเกิดขึ้นตามมา

4.5.1.2 ผลกระทบ

จากการศึกษาวิจัยค้นพบว่า ปัจจุบันผู้ไม่ประสงค์ดีหรือคนร้ายมีวิธีการหลอกลวงเหยื่อในรูปแบบใหม่อยู่เสมอ โดยส่วนใหญ่เป้าหมายของคนร้ายที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ คือ หน่วยงานที่มีข้อมูลอ่อนไหวและเกี่ยวข้องกับประชาชนเป็นหลัก อาทิ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยมีหน่วยงานด้านการกำกับดูแลและควบคุมเข้ามาสนับสนุนและช่วยเหลือเมื่อได้รับแจ้งเหตุภัยคุกคามทางไซเบอร์จากหน่วยงานที่อยู่ภายใต้การกำกับดูแล รวมทั้งหน่วยงานด้านกระบวนการยุติธรรมที่นำกฎหมายมาบังคับใช้และรับมือภัยคุกคามทางไซเบอร์ที่มีอยู่มากมายในขณะนี้



ภาพที่ 15 ภัยคุกคามทางไซเบอร์กับการโจมตีหน่วยงานสำคัญของไทย

โดยจากภาพที่ 15 แสดงภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานด้านยุติธรรม ส่งผลกระทบต่อด้านระบบสารสนเทศและเครือข่าย ด้านข้อมูลสารสนเทศ ด้านการให้บริการ ด้านความมั่นคงปลอดภัย ด้านการกำกับดูแล และด้านอื่นๆ ที่มีความเชื่อมโยงกันซึ่งขึ้นอยู่กับลักษณะภัยคุกคามทางไซเบอร์ แต่ข้อค้นพบที่น่าสนใจคือ วิธีการที่แฮกเกอร์ใช้ในการเข้าถึงระบบและข้อมูลที่สำคัญขององค์กร รวมถึงศิลปะที่ใช้ในการสื่อสารเพื่อหลอกลวงให้เหยื่อคล้อยตาม ซึ่งเรียกวิธีการนี้ว่า Social Engineering หรือ วิศวกรรมสังคม เป็นหนึ่งในภัยคุกคามทางไซเบอร์ที่พบบ่อยในหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยเฉพาะในประเทศไทย คนร้ายใช้โอกาสในการเปิดตัวแอปพลิเคชันหรือแพลทฟอร์มรูปแบบใหม่ๆในการให้บริการประชาชน เช่น การปลอมเป็นเจ้าหน้าที่ภาครัฐให้คำแนะนำการใช้งานแอปพลิเคชันใหม่ขององค์กรต่าง ๆ การส่งข้อความรับชำระค่าบริการการส่ง SMS แจ้งว่าเป็นผู้โชคดีได้รับรางวัลต่างๆ หรืออีเมล Phishing หลอกล่อให้เหยื่อคลิกลิงก์ปลอม เป็นต้น

ผลการวิจัยนี้สอดคล้องกับทฤษฎีการกระทำที่เป็นกิจวัตร (Routine Activity Theory) ของโคเฮนและเฟลสัน (Lawrence E. Cohen and Marcus Felson, 1979) ที่มีสาเหตุที่ทำให้เกิดอาชญากรรม 3 ประการ ได้แก่ เป้าหมายที่เหมาะสม การขาดผู้ดูแลสถานที่นั้นๆ และแรงจูงใจอาชญากร พบว่า ผู้ไม่ประสงค์ดีเห็นพฤติกรรมเหยื่อผ่านโซเชียลมีเดีย สถานที่ เวลา ที่เป็นช่องโหว่หรือโอกาสที่จะบุกรุกเข้าไป หรือหาอรรถประโยชน์จากเหยื่อได้ตลอดเวลาในการกระทำของเหยื่อที่เป็นทำซ้ำๆ เดิม ๆ หรือทำเป็นกิจวัตรประจำวัน นอกจากนี้ยังสอดคล้องกับงานวิจัยของ พงศ์พนธ์ ภาวศุทธิ์ (2561) เรื่อง สาเหตุเชิงลึกของการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคมของกลุ่มเจเนอเรชั่นวาย ในเขตกรุงเทพมหานครและปริมณฑล และพบว่า สาเหตุที่ส่งผลต่อการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคมนั้น แบ่งได้เป็น 2 กรณี คือ (1) เป็นบุคคลที่เคยได้รับสารสนเทศที่เป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมสังคมและถูกโจมตี จะมีปัจจัยที่ส่งผล ได้แก่ การตัดสินใจอย่างไม่มีเหตุผลที่เกิดขึ้นจากความอยากรู้อยากเห็น ความกลัว และความโลภ โดยเป็นอารมณ์ ความรู้สึกพื้นฐานของมนุษย์ โดยผู้โจมตีจะใช้ลักษณะเฉพาะของสารสนเทศ เช่น ช่องทาง เนื้อหา รูปแบบ และรูปภาพ ที่สร้างมาเพื่อให้ผู้ถูกโจมตีนั้น เกิดอารมณ์ความรู้สึกอย่างใดอย่างหนึ่งข้างต้นและตัดสินใจอย่างไม่มีเหตุผลจนส่งผลให้ถูกโจมตีได้ (2) เป็นบุคคลที่เคยได้รับสารสนเทศที่เป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมสังคม หรือ Social engineering ในรูปแบบต่างๆ แต่ไม่ถูกโจมตี จะมีปัจจัยส่งผล ได้แก่

การรับรู้ภัยคุกคามที่เกิดขึ้นมาจากประสบการณ์ก่อนหน้าและการแจ้งเตือน โดยเมื่อบุคคลมีการรับรู้ภัยคุคามมากเพียงพอแล้วจะมีการตัดสินใจที่ใช้เหตุผลไตร่ตรองมากยิ่งขึ้นและไม่ถูกโจมตี

อย่างไรก็ตาม ในมุมมองของผู้วิจัยหากสถานการณ์ภัยคุกคามทางไซเบอร์โดยการแฮกข้อมูลไม่ได้เกิดขึ้นเพียงแค่ในหน่วยงานด้านสาธารณสุข ด้านสาธารณูปโภคและภาคการเงินการธนาคารเท่านั้น หากแต่ทุกองค์กรโดยเฉพาะด้านกระบวนการยุติธรรมควรให้ความสำคัญในเรื่องนี้ เนื่องจากอาจเกิดภัยคุกคามทางไซเบอร์ในลักษณะนี้กับหน่วยงานทางด้านกระบวนการยุติธรรม เช่น ศาล สำนักงานตำรวจแห่งชาติ กรมราชทัณฑ์ เพื่อเข้าไปเปลี่ยนแปลงแก้ไขข้อมูลการรับโทษแก้คดีความจากผิดเป็นถูก จากคนร้ายกลายเป็นผู้บริสุทธิ์ ซึ่งกรณีเช่นนี้จะสร้างความเสียหายให้แก่กระบวนการยุติธรรมเป็นอย่างยิ่ง ดังนั้นหน่วยงานด้านกระบวนการยุติธรรมควรเล็งเห็นถึงความสำคัญของปัญหาและผลกระทบด้านภัยคุกคามทางไซเบอร์ เพื่อเตรียมความพร้อมรับมือและป้องกันเหตุการณ์เหล่านี้ให้ดีที่สุด

4.5.2 โครงสร้างการกำกับดูแล การขับเคลื่อนการบังคับใช้นโยบายและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ในการบริหารจัดการความเสี่ยง เพื่อสร้างความตระหนักและเฝ้าระวังภัยคุกคามความมั่นคงปลอดภัยไซเบอร์

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานด้านยุติธรรม ได้นำ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาปรับใช้ในการจัดทำนโยบาย แผนยุทธศาสตร์ และแนวปฏิบัติในการเฝ้าระวังและรับมือภัยคุกคามทางไซเบอร์ให้สอดคล้องกับบริบทขององค์กร โดยเฉพาะอย่างยิ่งหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศที่สำคัญ ที่มีหน้าที่คอยควบคุมและกำกับดูแล รวมถึงมีภารกิจในการให้บริการประชาชน ไม่ว่าจะเป็นหน่วยงานด้านสาธารณสุข ด้านสาธารณูปโภค ด้านการเงินการธนาคาร ทั้งภาครัฐและภาคเอกชน ประกอบกับการเฝ้าติดตามช่องทางการเผยแพร่ข้อมูลข่าวสารของภาครัฐเรื่องภัยคุกคามใหม่ๆ อีกทั้งการประกาศกฎหมายหลักและกฎหมายรองเพื่อช่วยในการเพิ่มประสิทธิภาพการรับมือภัยคุกคามทางไซเบอร์ได้ดียิ่งขึ้น อาทิเช่น พ.ร.บ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ.2560 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 พ.ร.ก.มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.2566 ยุทธศาสตร์ชาติ 20 ปี และประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่ประกาศหลักเกณฑ์ด้านความมั่นคงปลอดภัยทางไซเบอร์เป็นระยะๆ

โดยผู้วิจัยค้นพบว่า พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 นั้น ยังไม่มีบทลงโทษที่ชัดเจนในการบังคับใช้ ถือว่าเป็นความหละหลวมของกฎหมายที่หลายคนมองข้าม ทั้งนี้อาจเป็นเพราะว่า กฎหมายรองฉบับนี้จัดทำขึ้นเพื่อเป็นแนวทางหรือคู่มือบริหารจัดการปัญหาด้านไซเบอร์ตามสถานการณ์ที่เกิดขึ้นเพื่อขอความร่วมมือให้หน่วยงานปฏิบัติตามเท่านั้น อีกทั้งไม่มีการระบุรายละเอียดที่ชัดเจนด้านมาตรฐานทางเทคโนโลยีที่องค์กรควรนำมาใช้และกระบวนการรับมือและป้องกันภัยคุกคามทางไซเบอร์ที่ยังไม่อาจครอบคลุม ทั้งนี้อาจเนื่องด้วยความก้าวหน้าของเทคโนโลยีที่พัฒนาไปอย่างรวดเร็ว ก่อให้เกิดภัยคุกคามทางไซเบอร์ในรูปแบบใหม่ๆมากขึ้น ทำให้กฎหมายที่มีอยู่ไม่ครอบคลุมในการรับมือ ป้องกัน และการควบคุมสถานกาณ์ภัยคุกคามทางไซเบอร์ได้ในปัจจุบัน อีกทั้งความพร้อมของอุปกรณ์และเทคโนโลยีขององค์กร ที่ยังขาดงบประมาณในการพัฒนาระบบป้องกันภัย เนื่องจากหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศบางแห่ง ไม่ได้รับการสนับสนุนด้านงบประมาณที่เพียงพอจากภาครัฐ ทำให้หลายหน่วยงานยังไม่มีการขับเคลื่อนด้านมาตรฐานทางเทคโนโลยีที่ดีมากพอ รวมไปถึงยังไม่มีการจัดทำแผนรองรับและซักซ้อมแผนการตอบสนองต่อสถานการณ์ฉุกเฉิน ซึ่งสอดคล้องกับงานวิจัยของ ณัฐวี อุตกฤษฎ์ (2555) เรื่อง การวางแผนรองรับเหตุการณ์ฉุกเฉินเพื่อความมั่นคงสารสนเทศในองค์กร ที่พบว่า การมุ่งเน้นให้เห็นถึงความสำคัญของการวางแผนรองรับสำหรับเหตุการณ์ฉุกเฉินกับการรักษาความมั่นคงสารสนเทศองค์กรมีความสัมพันธ์กัน ซึ่งองค์กรไม่ควรมองข้าม โดยพิจารณาตามแนวทางปฏิบัติของ NIST SP800-34 ประกอบด้วยหลัก 4 ประการ คือ (1) การวิเคราะห์ผลกระทบทางธุรกิจ (2) การวางแผนเพื่อตอบสนองต่อเหตุการณ์แบบไม่คาดคิด (3) การวางแผนฟื้นฟูเหตุการณ์จากความเสียหายที่รุนแรง และ (4) การวางแผนเพื่อดำเนินธุรกิจต่อไปได้ในสถานการณ์ฉุกเฉินที่รุนแรง พร้อมทั้งกระบวนการในการทดสอบแผนเล่านั้นอย่างเป็นระบบ

อนึ่ง ข้อค้นพบด้านการบริหารจัดการองค์กร กล่าวได้ว่า ปัจจุบันหลายหน่วยงานมีโครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศและเครือข่าย และการรับมือภัยคุกคามทางไซเบอร์ขององค์กรที่ยังไม่ครอบคลุมทั้งในบทบาทหลักของ (Key Role) และผลลัพธ์ของงาน (Output) ทั้งนี้อาจเป็นเพราะว่า ข้อจำกัดของกรอบอัตรากำลังเดิมไม่รองรับกับปริมาณงานที่เพิ่มขึ้นหรือภารกิจใหม่ที่ได้รับมอบหมาย ส่งผลให้หน่วยงานนั้นๆ มีการพิจารณาปรับโครงสร้างองค์กรใหม่ เพื่อตอบสนองต่อการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงการวางแผนเพื่อรับมือและป้องกันภัยคุมคามไซ

เบอร์ อีกทั้งภาครัฐให้ความสำคัญในการพัฒนาศักยภาพของบุคลากรและการลงทุนด้านความมั่นคงปลอดภัยไซเบอร์มากขึ้น

ผลการวิจัยนี้สอดคล้องกับงานวิจัยของ ปรัชญา ฮวดปากน้ำ (2559) เรื่อง ยุทธศาสตร์การพัฒนากำลังพลของกองทัพไทยเพื่อต่อต้านภัยคุกคามไซเบอร์ในทศวรรษหน้า พบว่า ผู้เชี่ยวชาญจากภาคเอกชน และผู้รับผิดชอบโดยตรงจากกองบัญชาการกองทัพไทย กองทัพบก กองทัพเรือ กองทัพอากาศ ได้ร่วมกันวิเคราะห์จุดอ่อน จุดแข็ง โอกาส และอุปสรรค ภายใต้สภาวะแวดล้อมปัจจุบันและอนาคตในระยะสิบปีข้างหน้าเพื่อกำหนดเป็นยุทธศาสตร์ผลการวิจัยทำให้ทราบถึง ปัญหาความไม่พร้อมของหน่วยงานและกำลังพลของกองทัพไทยตลอดจนภัยคุกคามในปัจจุบันและแนวโน้มของภัยคุกคามที่จะเกิดขึ้นในอนาคตและส่งผลกระทบต่อความปลอดภัยของการใช้ข้อมูลข่าวสารในการปฏิบัติงานรักษาความมั่นคงของกองทัพไทยบนพื้นฐานของความปลอดภัยของข้อมูล ตลอดจนทราบถึงความจำเป็นในการปรับปรุงโครงสร้างหน่วยงานสงครามไซเบอร์ของกองทัพ จัดเตรียมสรรหา ผลิตและพัฒนาบุคลากรสำหรับการต่อต้านภัยคุกคามไซเบอร์และได้ยุทธศาสตร์แนวทางพัฒนากำลังพลกองทัพไทยสำหรับต่อต้านภัยคุกคามไซเบอร์ให้มีความพร้อมรับสถานการณ์ในห้วงสิบปีข้างหน้าโดยมีรูปแบบของยุทธศาสตร์และแผนการพัฒนากำลังพลของกองทัพไทยสำหรับต่อต้านภัยคุกคามไซเบอร์

ในด้านการบริหารความเสี่ยงความมั่นคงปลอดภัยทางไซเบอร์ ที่เป็นแนวปฏิบัติในการจัดลำดับความสำคัญของมาตรการป้องกันความปลอดภัยทางไซเบอร์ โดยพิจารณาจากผลกระทบที่อาจเกิดขึ้นจากภัยคุกคามที่ออกแบบมาเพื่อใช้ในการโจมตีเป้าหมาย การสร้างแนวทางการบริหารความเสี่ยงเพื่อการสร้างความมั่นคงด้านความปลอดภัยทางไซเบอร์ ผู้วิจัยค้นพบว่า การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศ อาจไม่สามารถกำจัดช่องโหว่ของระบบทั้งหมดหรือบล็อกการโจมตีทางไซเบอร์ได้ทั้งหมด ทั้งนี้อาจเป็นเพราะธุรกิจและองค์กรยังไม่ให้ความสำคัญกับข้อบกพร่องของระบบเท่าที่ควร และขาดการวิเคราะห์แนวโน้มภัยคุกคามและการโจมตีที่สำคัญที่สุดต่อธุรกิจก่อน อันเป็นผลมาจากการดำเนินงานและการใช้ระบบสารสนเทศ

ผลการศึกษาวิจัยนี้สอดคล้องงานวิจัยของ อนาวิล แก้วสะอาดและณัฐวี อุตกฤษฎ์ (2564) เรื่อง แนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร ที่พบว่า การประเมินความเสี่ยงด้านไซเบอร์ถือว่าเป็นส่วนสำคัญในการบริหารความมั่นคงปลอดภัยไซเบอร์ขององค์กร เนื่องจากองค์กรได้มีการนำเทคโนโลยีสารสนเทศเข้ามาใช้งานเพื่อสนับสนุนภารกิจขององค์กร ทั้งนี้ การประเมินความเสี่ยงจะเป็นการพิจารณานำมาตรการควบคุมมาใช้อย่างเหมาะสมเพื่อให้เกิดประสิทธิภาพสูงสุด โดยมีแนวทางการวิเคราะห์ช่องโหว่ของระบบสารสนเทศในองค์กรทั้งในด้านการ

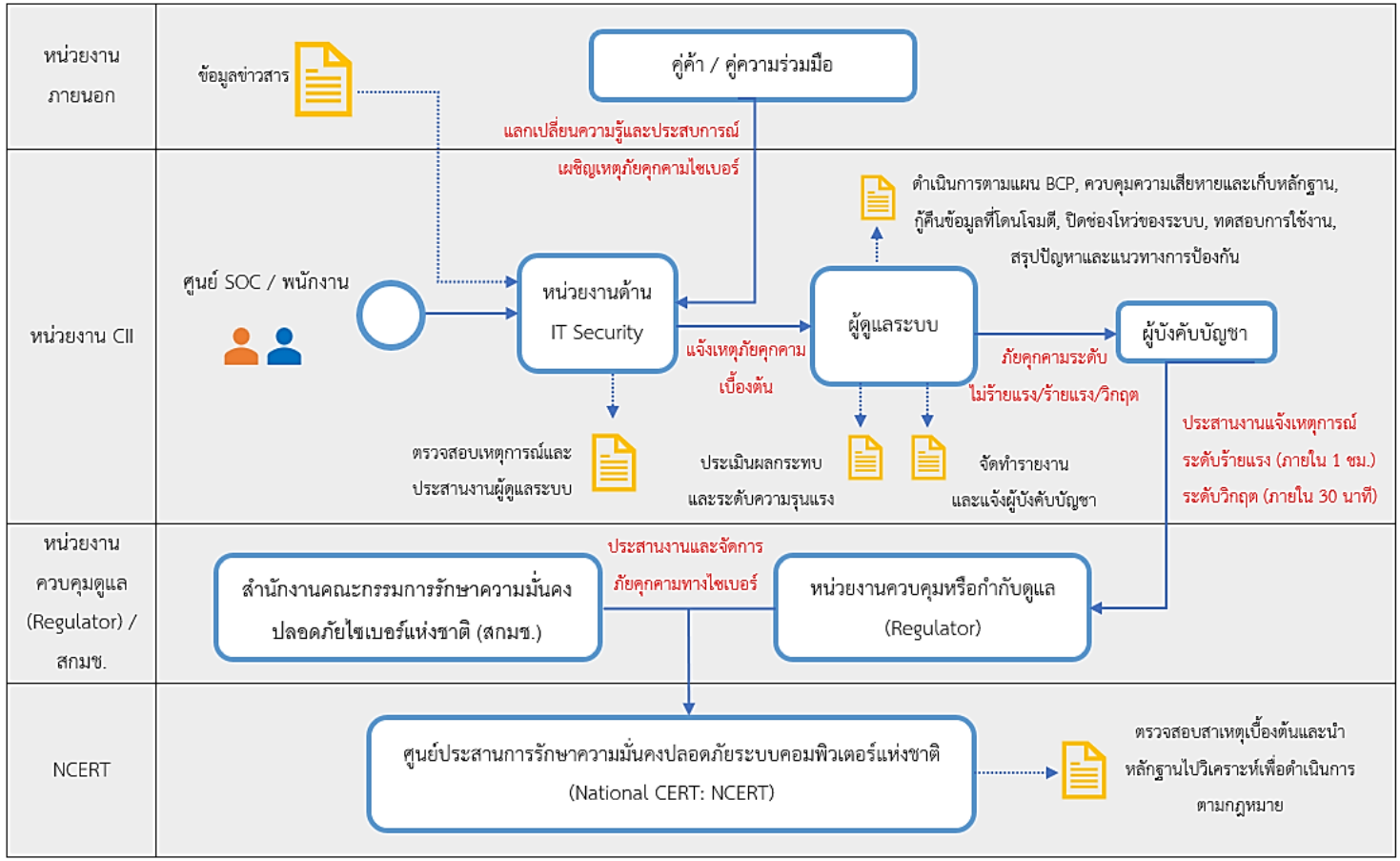
วิเคราะห์ช่องโหว่จากหลักฐานที่เป็นเอกสารหรือรายงาน และการทดสอบความมั่นคงปลอดภัยระบบสารสนเทศขององค์กร อีกทั้งมีการวิเคราะห์ความสัมพันธ์ของภัยคุกคามรูปแบบการโจมตีและช่องโหว่ และศึกษาผลกระทบในทางไซเบอร์เชิงคุณภาพ อธิบายระดับของผลกระทบ สูง ปานกลาง ต่ำ โดยพิจารณาระดับความเสี่ยงที่เกิดขึ้นกับความมั่นคงปลอดภัยไซเบอร์ภายในองค์กร จากโอกาสเกิดภัยคุกคาม ความรุนแรงที่เกิดขึ้นของภัยคุกคามต่อช่องโหว่ขององค์กร และแผนหรือมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ที่ช่วยลดหรือขจัดความเสี่ยงที่เกิดขึ้นให้อยู่ในเกณฑ์ที่ยอมรับได้ นอกจากนี้ยังสอดคล้องกับงานวิจัยของ Teeraratchakarn (2019) เรื่อง การสำรวจช่องโหว่เครือข่ายเพื่อการปฏิบัติด้านความปลอดภัยองค์กร พบว่า มีแนวทางการประเมินความเสี่ยง และโอกาสที่จะเกิดความเสี่ยงในลักษณะเดียวกันกับธนาคารแห่งประเทศไทย แต่การพิจารณาเกณฑ์การประมาณโอกาสที่จะเกิดความเสี่ยงมีการแบ่งระดับที่มากกว่า คือ น้อยมาก น้อย ปานกลาง สูง สูงมาก และมีระดับคะแนน 1 2 3 4 5 ตามลำดับ ซึ่งสามารถนำรายงานหลังการประเมินระดับความเสี่ยงเหล่านี้มาสนับสนุนการกำหนดนโยบายองค์กรได้

ในด้านการสร้างความตระหนักรู้ คือ การแสดงออกซึ่งความรู้สึก ความคิดเห็น ความสำนึก เป็นภาวะที่บุคคลเข้าใจและประเมินสถานการณ์ที่เกิดขึ้นเกี่ยวกับตนเองได้โดยอาศัยระยะเวลา เหตุการณ์และประสบการณ์หรือสภาพแวดล้อมเป็นปัจจัยทำให้เกิดความตระหนัก ซึ่งข้อค้นพบน่าสนใจ คือ ยังมีผู้คนค่อนข้างมากที่ตกเป็นเหยื่อจากภัยคุกคามทางไซเบอร์ แม้ว่าจะมีการสื่อสารจากหน่วยงานภาครัฐในด้านการป้องกันภัยคุกคาม จากสื่อมวลชนที่นำเสนอข่าวสารเตือนภัยผ่านโซเชียลมีเดียทุกช่องทาง หรือการสร้างความตระหนักรู้ให้กับบุคลากรในองค์กรต่าง ๆ จึงเป็นที่น่าสังเกตว่า ความตระหนักเป็นพฤติกรรมด้านจิตพิสัย ซึ่งเกี่ยวกับความรู้สึกนึกคิดทางจิตใจ อารมณ์ และคุณธรรมของบุคคลเป็นขั้นตอนทำความรู้จักกับเหตุการณ์หรือปรากฏการณ์ที่เกิดขึ้นโดยยอมให้สิ่งเร้าเหล่านั้น เข้ามาอยู่ในความสนใจตนเอง อย่างไรก็ตาม หลายหน่วยงานยังคงหาวิธีที่จะพัฒนาคนในองค์กรให้มีความตระหนักรู้อยู่เสมอ ไม่ว่าจะเป็นการอบรมเชิงปฏิบัติการ สัมมนาหลักสูตรที่เกี่ยวข้องทั้ง Onsite และ Online จัดกิจกรรมหรือโครงการที่มุ่งเน้นเฉพาะด้านความมั่นคงปลอดภัยไซเบอร์เป็นสำคัญ การให้ความรู้จากผู้เชี่ยวชาญในการกฎหมายและนโยบายต่างๆ ผลการวิจัยนี้สอดคล้องกับผลการวิจัยของ Sakchareonkul (2019) เรื่อง การเตรียมความพร้อมของบุคลากรภาครัฐไทยสู่การเป็นรัฐบาลดิจิทัล ที่ค้นพบว่า บุคลากรภาครัฐจำเป็นต้องตระหนักรู้ เข้าใจ และยอมรับการเปลี่ยนแปลง พร้อมพัฒนา

ศักยภาพของตนเองให้มีสมรรถนะที่ตรงกับบทบาทหน้าที่ที่รับผิดชอบ และตระหนักถึงการรู้เท่าทันดิจิทัล เทคโนโลยีอินเทอร์เน็ตและเครือข่ายสังคมออนไลน์

4.5.3 แนวทางการเตรียมแผนการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์และการกำกับดูแลการบริหารจัดการที่ดีด้านเทคโนโลยีดิจิทัลในองค์กร เพื่อลดความเสี่ยงและป้องกันภัยคุกคามทางไซเบอร์ในอนาคต

จากการนำ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาปรับใช้ในการกระบวนการและแนวปฏิบัติในการรับมือภัยคุกคามทางไซเบอร์ให้สอดคล้องกับบริบทขององค์กรนั้น ทั้งนี้หน่วยงานโครงสร้างพื้นฐานทางสารสนเทศที่สำคัญ ภายใต้หน่วยงานควบคุมและกำกับดูแล ได้เฝ้าระวังและตรวจจับภัยคุกคามทางไซเบอร์ ร่วมกับการประสานงานภายในและภายนอกองค์กร ไปจนถึงการติดตาม รายงาน และประเมินผลของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ หรือ NCERT เป็นหน่วยงานหลักในการประสานงานด้านความมั่นคงปลอดภัยไซเบอร์ในประเทศไทย สามารถนำมาอธิบายขั้นตอนการดำเนินการตามมาตรการของกฎหมายดังกล่าวในภาพรวม ได้ดังภาพที่ 16



ภาพที่ 16 แสดงกลไกการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์

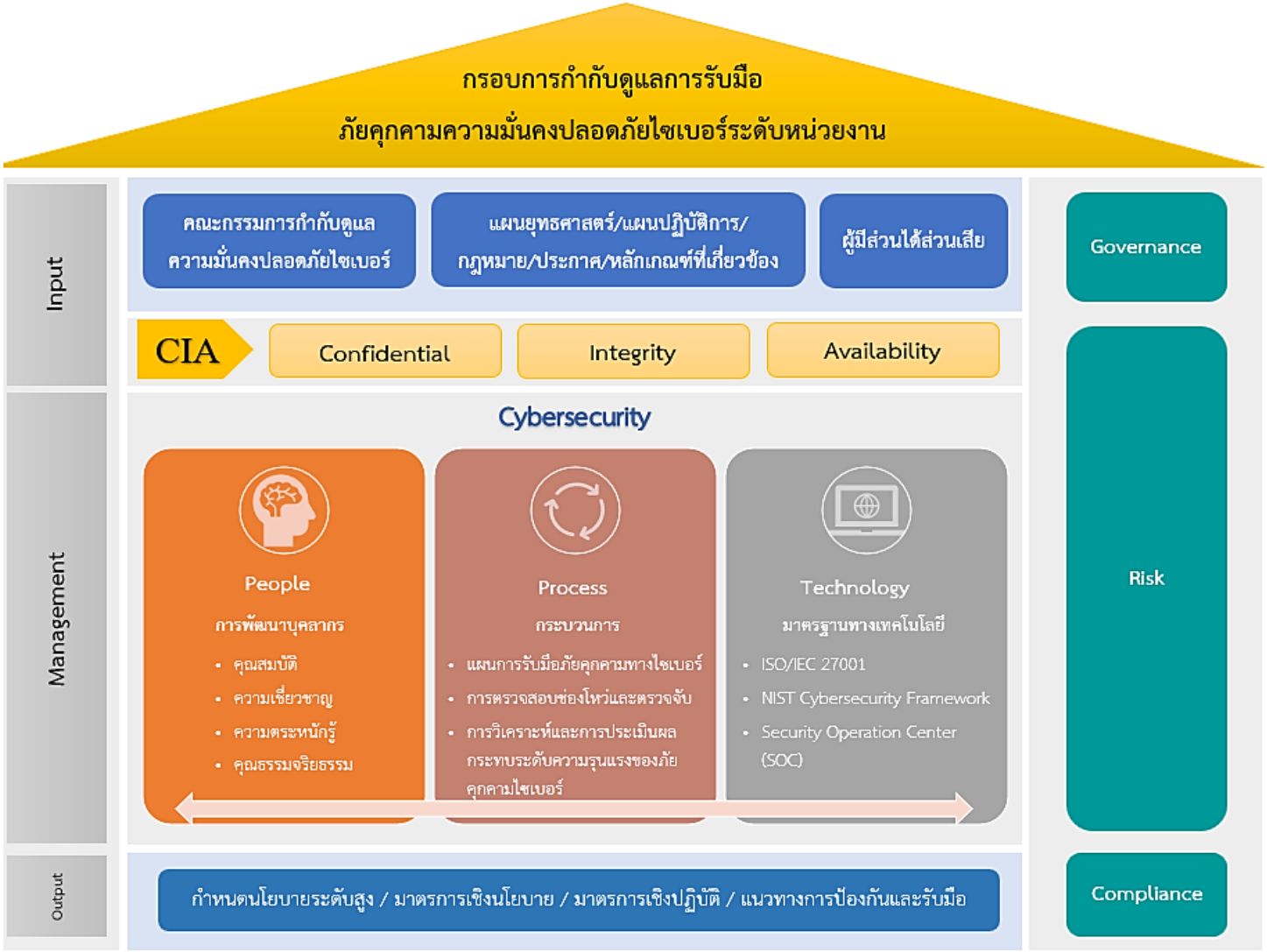
ผู้วิจัยค้นพบว่า หลายหน่วยงานมีการนำกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ หรือ NIST และมาตรฐานสากลอย่าง ISO27001 มาปรับใช้เพื่อยกระดับความมั่นคงปลอดภัยไซเบอร์ ซึ่งสอดคล้องกับผลการวิจัยของ Phantawornchai (2018) เรื่อง แนวทางการสร้างกรอบการพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคราวด์ พบว่า การอิงตามแนวคิดมาตรฐานและตัวแบบที่เกี่ยวข้อง เช่น NIST Cybersecurity Framework เป็นไปเพื่อวิเคราะห์ความเสี่ยงและภัยคุกคามด้านไซเบอร์และหาแนวทางในการพัฒนากรอบการคืนสภาพด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ อีกทั้งมีการนำมาตรฐาน ISO27001 มาใช้งาน 4 องค์ประกอบหลักคือ (1) จัดทำระบบการจัดการความมั่นคงปลอดภัยเพื่อเตรียมการและวางแผนปกป้องสารสนเทศ (2) นำแผนไปปฏิบัติและจัดทำระบบไปปฏิบัติจริงหน้างาน (3) ปฏิบัติควบคู่ไปกับการทำงานปกติ (4) ปรับปรุงอย่างต่อเนื่องคือ ทบทวนผลการทำระบบและหาจุดปรับปรุงอย่างต่อเนื่อง โดยมีโมเดล CIA ใน ISO27001 เน้นการปกป้องข้อมูลสารสนเทศให้มีคุณสมบัติคือ (1) Confidential : การปกป้องสารสนเทศให้เข้าถึงได้เฉพาะผู้ที่มีสิทธิ ถ้าหากข้อมูลรั่วไหลแสดงว่าขาดคุณสมบัติในข้อนี้ (2) Integrity : ปกป้องความถูกต้องสมบูรณ์ของสารสนเทศไม่ให้ถูกแก้ไขเปลี่ยนแปลงผิดไปจากความเป็นจริง เช่น การแฮกระบบเพื่อแก้ไขข้อมูลเป็นต้น และ (3) Availability : สร้างความเชื่อมั่นว่าระบบสารสนเทศพร้อมใช้งาน

นอกจากนี้ยังสอดคล้องกับงานวิจัยของ ณัฐวี อุตกฤษฎ์. (2555) เรื่อง การวางแผนรองรับเหตุการณ์ฉุกเฉินเพื่อความมั่นคงสารสนเทศในองค์กร พบว่า เป็นการเตรียมรับเหตุการณ์ฉุกเฉินที่คุกคามต่อสารสนเทศ ซึ่งองค์กรควรให้ความสำคัญเพราะบางครั้งองค์กรอาจตกอยู่ในสภาวะที่ไม่สามารถรองรับและตอบสนองเหตุการณ์ดังกล่าวได้ด้วยการปฏิบัติตามแผนปกติ โดยการจัดทำแผนรอบรับเหตุการณ์ฉุกเฉินในองค์กรนั้น พิจารณาตามแนวทางปฏิบัติของ NIST SP 800-34 ได้แก่ (1) การวิเคราะห์ผลกระทบทางธุรกิจ (2) การวางแผนเพื่อตอบสนองต่อเหตุการณ์ที่ไม่คาดคิด (3) การวางแผนฟื้นฟูเหตุการณ์จากความเสียหายที่รุนแรง และ (4) การวางแผนเพื่อดำเนินธุรกิจต่อไปได้ในสถานการณ์ฉุกเฉินที่รุนแรง เรียกว่า Business Continuity Plan หรือ BCP

ในด้านการกำกับดูแลของผู้บริหารระดับสูงในแต่ละองค์กร ทั้งในเรื่องของการบริหารจัดการด้านการใช้ทรัพยากรเทคโนโลยีดิจิทัลอย่างเหมาะสมทั้งด้าน เงิน คน เวลาและสถานที่ รวมถึงด้านความปลอดภัยนั้น มีการจัดทำแผนรับมือภัยคุกคามทางไซเบอร์ในหลายองค์กร การทดสอบเจาะระบบหรือที่เรียกว่า Penetration Testing และตรวจสอบช่องโหว่หรือ Vulnerability

Assessment ซึ่งเป็นวิธีการประเมินความเสี่ยงด้วยการทดสอบเจาะระบบเพื่อค้นหาจุดอ่อนในการเข้าถึงระบบต่างๆ เพื่อป้องกันการถูกคุกคามผ่านช่องโหว่ที่กำลังระบาดอยู่ในปัจจุบันได้ สร้างความตระหนักด้านความมั่นคงปลอดภัยในการปรับปรุงระบบตลอดเวลา ลดความเสี่ยงด้านกฎหมายและสร้างความตระหนักให้กับผู้บริหาร รวมถึงสนับสนุนการปฏิบัติตามมาตรฐาน ISO/IEC 27001, PCI DSS และกฎหมายต่างๆ ผลการวิจัยนี้สอดคล้องกับงานวิจัยของ Back and LaPrade (2020) เรื่อง Cyber-Situation Crime Prevention and the Breadth of Cybercrimes among Higher Education Institutions พบว่า ในการตอบสนองต่ออาชญากรรมทางไซเบอร์ เป้าหมายหลักของระบบความปลอดภัยทางไซเบอร์ ได้แก่ การรักษาความเป็นส่วนตัว การรักษาข้อมูล ความสมบูรณ์ ชี้ให้เห็นว่าอาชญากรรมสามารถป้องกันได้ด้วยสิ่งแวดล้อมที่ส่งผลกระทบทางตรงและทางอ้อมต่อการรับรู้ของอาชญากร อาชญากรรมไซเบอร์มีความซับซ้อนในการกระทำความผิด เนื่องจากคนร้ายมีการเชื่อมโยง WIFI internet จากที่ไหนก็ได้ ทำให้การติดตามสืบสวนตัวผู้กระทำผิดได้ยากมาก ซึ่งมีกรณีที่เคยพบคือ เจ้าหน้าที่ได้ตรวจสอบ IP Address ของคนร้ายปรากฏว่า มีหลาย IP Address ปรากฏขึ้นเป็นสถานที่ของรัฐ สถานที่ต่างๆ ในเวลาที่ไล่เลี่ยกัน หรือไม่ก็ในเวลาที่ไม่แน่นอน เป็นไปได้ทั้งกลางวันและกลางคืน ทำให้ตรวจสอบยากนั่นคือ คนร้ายจะใช้สถานที่ก่อเหตุได้หลาย ๆ ที่ ที่ไหนก็ได้ เวลาใดก็ได้ไม่มีข้อจำกัดในการกระทำความผิด

โดยจากนโยบายการกำกับดูแลที่ดีด้านเทคโนโลยีดิจิทัลหรือ GRC แผนยุทธศาสตร์ กฎหมายที่เกี่ยวข้อง การนำ 3 เสาหลักด้าน Data Security อย่างการปกปิดข้อมูล ความน่าเชื่อถือของข้อมูล และความพร้อมใช้ของข้อมูล หรือ CIA มาพิจารณาช่วยในการปกป้องข้อมูลจากการทำลาย แก้ไข หรือเปิดเผยข้อมูลทั้งเจตนาและไม่เจตนา โดยการนำเทคนิคต่างๆและเทคโนโลยีที่หลากหลายมาควบคุมและจัดการความปลอดภัย ไปจนถึงการนำมาตรฐานและมาตรการต่างๆมาใช้ของแต่ละองค์กร ไม่ว่าจะเป็นหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ หน่วยงานด้านการควบคุมหรือกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ และหน่วยงานกระบวนการยุติธรรม ตลอดจนความคิดเห็นของผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ สามารถนำมาสรุปเป็นกรอบการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ระดับหน่วยงาน ได้ดังภาพที่ 17



ภาพที่ 17 แสดงกรอบการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ระดับหน่วยงาน

บทที่ 5
สรุปผลการศึกษาและข้อเสนอแนะ

จากผลการวิเคราะห์การศึกษาเรื่อง แนวทางการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ขององค์กรในยุคดิจิทัล เป็นการวิเคราะห์การรับมือภัยคุมคามทางไซเบอร์ของภาครัฐในลักษณะของสถานการณ์ภัยคุกคามทางไซเบอร์ของหน่วยงานต่าง ๆ ที่มีผลกระทบต่อโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศด้านสาธารณูปโภคของประเทศไทย โดยจะเริ่มศึกษาตั้งแต่สถานการณ์ภัยคุกคามทางไซเบอร์หน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศด้านสาธารณสุข ด้านสาธารณูปโภค และภาคการเงินการธนาคาร ตลอดจนโครงสร้างการกำกับดูแลด้านเทคโนโลยีดิจิทัลขององค์กรและการขับเคลื่อนด้วยนโยบายและมาตรการรักษาความปลอดภัยทางไซเบอร์ในการบริหารจัดการ เพื่อสร้างความตระหนักและเฝ้าระวังภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ และวิเคราะห์เพื่อให้ได้แนวทางการเตรียมแผนการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์และการกำกับดูแลการบริหารจัดการที่ดีด้านเทคโนโลยีดิจิทัลในองค์กร เพื่อลดความเสี่ยงและป้องกันภัยคุกคามทางไซเบอร์ในอนาคต

โดยผู้วิจัยดำเนินการวิจัยเชิงคุณภาพ (Qualitative Research) ด้วยการศึกษาจากเอกสาร (Documentary Research) และการสัมภาษณ์เชิงลึก (In-depth Interview) มาวิเคราะห์ (Analysis) และสังเคราะห์ (Synthesize) ถึงสถานการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศด้านสาธารณสุข สาธารณูปโภค และการเงินการธนาคาร รวมถึงหน่วยงานภาครัฐในด้านนโยบาย ด้านการกำกับดูแล ด้านกระบวนการยุติธรรม และองค์กรต่างๆที่เป็นเป้าหมายที่สำคัญของประเทศไทย เพื่อให้ทราบถึงภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยในระดับองค์กร และการตอบสนองต่อเหตุการณ์ นำไปสู่แนวทางการกำกับดูแลเพื่อรับมือภัยคุกคามและการประเมินความเสี่ยงในระดับที่องค์กรยอมรับได้

ดังนั้นในบทนี้จะสรุปผลการศึกษาทั้งหมดตามจุดประสงค์ที่วางไว้พร้อมทั้งข้อเสนอแนะเชิงวิชาการและข้อเสนอแนะในการปฏิบัติ เพื่อตอบปัญหาตามจุดประสงค์ทั้งหมดที่ได้ตั้งไว้วิจัยเล่มนี้จะสรุปผลตามสถานการณ์ภัยคุกคามทางไซเบอร์ในประเทศไทย โครงสร้างการการกำกับดูแลการขับเคลื่อนนโยบายและแนวปฏิบัติ และการรับมือภัยคุกคามทางไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ ทั้งนี้อาจมีนำนโยบายและประกาศใหม่ๆมาอธิบายเพื่อให้เห็นแนวทาง

ด้านการกำกับดูแลการรับมือภัยคุกคามทางไซเบอร์ในปัจจุบันให้ชัดเจน เพื่อเตรียมความพร้อมในการรับมือภัยคุกคามในอนาคต

5.1 สถานการณ์ภัยคุกคามทางไซเบอร์หน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศด้านสาธารณูปโภคในประเทศไทย

สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและหน่วยงานด้านการควบคุมและกำกับดูแลหน่วยงานที่มีภารกิจการให้บริการ จัดระดับของเหตุการณ์ภัยคุกคามทางไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศด้านสาธารณูปโภคในประเทศไทยให้อยู่ใน ระดับไม่ร้ายแรง เนื่องจากที่ผ่านมาภัยคุกคามทางไซเบอร์ส่วนใหญ่เป็นลักษณะของการเข้าไปก่อกวน ทำลายอุปกรณ์และระบบเครือข่ายคอมพิวเตอร์หรือการให้บริการของรัฐด้อยประสิทธิภาพลงไปกว่าเดิมเท่านั้น ซึ่งภัยคุกคามด้านไซเบอร์ที่ส่งผลกระทบต่อองค์กรในปัจจุบันอยู่ในระดับผลกระทบที่ต่ำ สืบเนื่องจากทุกองค์กรมีการออกมาตรฐานกำหนดหลักเกณฑ์การรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศโดยภายรวม โดยใช้กฎหมาย ระเบียบ แนวนโยบายและแนวปฏิบัติที่เกี่ยวข้อง เช่น พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 แนวนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ นโยบายและแผนปฏิบัติการว่าด้วยความมั่นคงปลอดภัยไซเบอร์ เป็นมาตรฐานและแนวทางเพื่อจัดทำหลักปฏิบัติหรือวิธีปฏิบัติที่ช่วยลดความเสี่ยงจากภัยคุกคามไซเบอร์ที่เกิดขึ้นให้อยู่ในระดับที่องค์กรยอมรับได้ และส่งผลกระทบต่อระบบสารสนเทศขององค์กรน้อยที่สุด

5.1.1 ปัญหาภัยคุกคามทางไซเบอร์ในประเทศไทย

การพัฒนาการด้านรูปแบบการโจมตีทางไซเบอร์ทั้งในเชิงกลยุทธ์และเชิงเทคนิคมีความซับซ้อน รุนแรง พัฒนาขึ้นตามลำดับเพื่อหลีกหนีการตรวจจับจากอุปกรณ์ป้องกันการโจมตี และการพยายามสแกนหาช่องโหว่และข้อบกพร่องจากเครื่องมือและระบบการป้องกันเหล่านั้น โดยภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในประเทศไทย มักจะเกิดกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสาธารณสุข ด้านสาธารณูปโภค และด้านการเงินการธนาคาร โดยมีเหตุการณ์ที่สำคัญดังนี้

1) ปี 2559 ธนาคารออมสิน ถูกแฮกเงินจากตู้เอทีเอ็ม โดยการสกรีมมิ่งโจรกรรมเงินจากบัญชีของลูกค้า ซึ่งจากการตรวจสอบพบว่า ถูกโจรกรรมเงินจากตู้เอทีเอ็มทั้งหมด 21 เครื่อง รวม

เป็นเงินกว่า 12 ล้านบาท เป็นลักษณะการโจรกรรมเงินในกล่องเงินเครื่องเอทีเอ็ม โดยการติดตั้งอุปกรณ์สั่งการที่ตู้ และสามารถเสียบบัตรให้เงินออกมาได้ทันที

2) ปี 2563 การไฟฟ้าส่วนภูมิภาค ถูกโจมตีจากมัลแวร์เรียกค่าไถ่ ส่งผลให้แอปพลิเคชัน PEA Smart Plus ไม่สามารถใช้งานได้ชั่วคราว

3) ปี 2563 โรงพยาบาลสระบุรีถูกไวรัสโจมตี โดยแฮกเกอร์ได้ใช้ Ransomware เข้ารหัสข้อมูลคนไข้ในโรงพยาบาลสระบุรีทั้งหมด ซึ่งข้อมูลที่โดนเข้ารหัสนั้นล้วนเป็นข้อมูลคนไข้ในระบบซึ่งเป็นข้อมูลที่จำเป็นต่อการรักษา และวินิจฉัยโรคเป็นอย่างมาก ซึ่งถึงแม้ว่าทางโรงพยาบาลได้มีการแบคอัพข้อมูลบางส่วนเอาไว้บ้างแล้ว แต่ข้อมูลเหล่านั้นกลับเป็นข้อมูลเก่าตั้งแต่ปี 2558 ทำให้ไม่สามารถหยิบเอามาใช้ได้เลย

4) ปี 2564 โรงพยาบาลเพชรบูรณ์โดยแฮกข้อมูลผู้ป่วยไปขายบนเว็บไซต์ ซึ่งข้อมูลที่รั่วไหลออกไปไม่ได้เป็นข้อมูลหลักที่ใช้ในการให้บริการและมีประวัติการรักษาผู้ป่วย

5) ปี 2566 การประปาส่วนภูมิภาค สังกัดกระทรวงมหาดไทย ถูกปลอมแปลงเว็บไซต์องค์กร โดยใช้ชื่อ https://pwa-co.cc/ ซึ่งไม่ใช่เว็บไซต์ขององค์กรแต่อย่างใด เป็นการปลอมและเลียนแบบเว็บไซต์ที่มิจฉาชีพทำขึ้นมาเท่านั้น

นอกจากนี้ การโจมตีทางไซเบอร์ที่เกิดขึ้นบ่อยครั้ง ได้แก่ (1) การใช้มัลแวร์เรียกค่าไถ่ (Ransomware) และการโจมตีด้วยการปล่อยไวรัสคอมพิวเตอร์ (2) การโจมตีแบบ Denial of Service (DoS) และ Distributed Denial-of-Service (DDoS) เพื่อเข้าถึงข้อมูลที่สำคัญไปยังเว็บไซต์ขององค์กรต่างๆ ทำให้ระบบปฏิเสธการให้บริการ หยุดชะงัก หรือระบบล่มไม่สามารถใช้งานได้ชั่วคราว (3) การสแกนหาช่องโหว่ (Vulnerability) เพื่ออาศัยจุดอ่อนหรือข้อบกพร่องของโปรแกรมและระบบสารสนเทศ ในการเข้าถึงข้อมูลที่สำคัญขององค์กร ซึ่งการโจมตีในลักษณะนี้สามารถต่อยอดกระบวนการก่ออาชญากรรมทางไซเบอร์ของอาชญากรในการเรียกค่าไถ่ การปลอมแปลงเว็บไซต์ขโมยข้อมูลไปขายในตลาดมืด หรือการโจรกรรมทางสินทรัพย์ เป็นต้น (4) การฟิชชิ่ง (Phishing) ซึ่งปัจจุบันเป็นภัยไซเบอร์ที่แฮกเกอร์ได้พัฒนากลวิธีในการหลอกลวงหลากหลายรูปแบบ คือ ฟิชชิ่งอีเมล (Phishing Email) เพื่อหลอกให้กรอกข้อมูลสำคัญหรือการขโมยข้อมูล โดยการแพร่ระบาดของมัลแวร์ (Malware) ที่ฝังตัวมากับอีเมล และปัจจุบันยังพบ มัลแวร์เรียกค่าไถ่ (Ransomware) สายพันธุ์ต่าง ๆ ที่เข้ารหัสลับข้อมูลในเครื่องทำให้เปิดใช้งานไม่ได้ ซึ่งวิธีการดังกล่าวเป็นการโจมตี โดยอาศัยวิธีวิศวกรรมสังคม (Social Engineering) ซึ่งเป็นวิธีการโจมตีจุดอ่อนของคนที่ยังขาดความรู้

ความเข้าใจ และความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ต่าง ๆ ที่มีความซับซ้อนมากขึ้น

จากสถานการณ์ภัยคุกคามทางไซเบอร์ที่กล่าวมาข้างต้นนั้น เกี่ยวข้องกับปัญหาที่สำคัญแบ่งได้เป็น 3 ประเด็นดังนี้

1) คนหรือบุคลากรไม่เพียงพอ ปัจจุบันหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศทั้งด้านสาธารณสุขและสาธารณูปโภค ยังขาดแคลนบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ที่มีความรู้ความเข้าใจความเชี่ยวชาญเชิงเทคนิค ส่งผลให้หลายองค์กรต้องเผชิญกับปัญหาบุคลากรไม่เพียงพอต่อการรองรับภาระงานในส่วนนี้ โดยเฉพาะหน่วยงานภาครัฐที่มีงบประมาณด้านการจ้างแรงงานที่ต่ำกว่าหน่วยงานเอกชน

2) เทคโนโลยีที่ล้าสมัย ปัญหาของระบบ อุปกรณ์ และมาตรฐานทางเทคโนโลยีไม่มีประสิทธิภาพมากพอที่จะรองรับและป้องกันภัยคุกคามในรูปแบบใหม่ๆที่มากขึ้นในปัจจุบัน ด้วยงบประมาณที่มีอยู่อย่างจำกัดและมีความเหลื่อมล้ำกันระหว่างองค์กร ปัญหาสำคัญมากๆคือ ความไม่สอดคล้องกันระหว่างความต้องการจัดซื้ออุปกรณ์ของ Vendor กับงบประมาณที่ได้รับการสนับสนุนจากภาครัฐ ดังนั้นการลงทุนทางด้าน Cybersecurity ที่ผ่านมาอาจจะไม่ได้ตอบโจทย์ที่แท้จริง

3) กฎหมายไม่ครอบคลุม พ.ร.บ. ไซเบอร์ 2562 ที่ประกาศออกมาเพื่อใช้เป็นกรอบกฎหมายที่ใหญ่ที่สุดที่จะเป็นแนวทางควบคุมให้เกิดความปลอดภัย ซึ่งโดยธรรมชาติของ พ.ร.บ. ไซเบอร์ 2562 ไม่ได้มีลักษณะเป็นการบังคับ แต่เป็นในลักษณะของแนวทาง (Guideline) ที่ให้หน่วยงานโครงสร้างพื้นฐานทางสารสนเทศและหน่วยงานที่สำคัญมีแนวทางที่เรียกว่า baseline หรือว่าแนวทางขั้นต่ำในการปฏิบัติเท่านั้น เนื่องจาก ไม่มีคำว่าบังคับหรือบทลงโทษที่ชัดเจน ทำให้คนทั่วไปเข้าใจว่าขอความร่วมมือหรือสมัครใจที่จะปฏิบัติตามเท่านั้น

5.1.2 ผลกระทบจากภัยคุกคามทางไซเบอร์

จากเหตุการณ์ภัยคุกคามไซเบอร์ที่โจมตีหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานด้านยุติธรรม ส่งผลกระทบต่อองค์กรดังนี้

(1) ด้านระบบสารสนเทศและเครือข่าย เช่น อินเตอร์เน็ต (Internet) เครื่องแม่ข่าย (Server) ฮาร์ดแวร์และซอฟต์แวร์ (Hardware/Software) ทำให้ระบบการทำงานล่าช้า หยุดชะงักหรือไม่สามารถใช้งานได้ แต่ผลกระทบในภาพรวมอยู่ในระดับต่ำ ที่องค์กรยังสามารถจัดการแก้ไขปัญหาได้ทันท่วงที

(2) ด้านข้อมูลสารสนเทศ ส่งผลให้องค์กรไม่สามารถเข้าถึงข้อมูลได้ ความสมบูรณ์และความพร้อมใช้งานของข้อมูลไม่เต็มประสิทธิภาพหรือมีข้อมูลบางอย่างหายไป แต่ยังรักษาความลับของข้อมูลที่สำคัญได้ ยกตัวอย่างกรณีการโจมตีทางไซเบอร์ที่โรงพยาบาลสระบุรี มีข้อมูลรายบุคคลของคนไข้ที่รั่วไหลออกไป เช่น ชื่อ สกุล ซึ่งเป็นข้อมูลทั่วไป แต่ไม่กระทบต่อข้อมูลด้านสุขภาพ

(3) ด้านการให้บริการ คือ ผลกระทบต่อความพึงพอใจของผู้มีส่วนได้ส่วนเสียในการรับบริการ เช่น หน่วยงานที่มีพันธกิจร่วมกัน คู่ค้า คู่ความร่วมมือ ลูกค้า รวมถึงประชาชนทั่วไปที่ใช้บริการจากหน่วยงานนั้นๆ โดยเฉพาะการให้บริการผ่านเว็บไซต์ และแอปพลิเคชัน ทำให้เกิดความล่าช้าหรือเกิดความเข้าใจผิดในการรับบริการ เป็นต้น

(4) ด้านความมั่นคงปลอดภัย ส่งผลกระทบต่อมาตรการในการรับมือและมาตรฐานทางเทคโนโลยีที่มีอยู่ในองค์กรอาจไม่ครอบคลุมและป้องกันการถูกโจมตีทางไซเบอร์ได้เท่าที่ควร กระทบต่อภาพลักษณ์และชื่อเสียง ส่งผลให้เห็นถึงความบกพร่องของมาตรการและวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์

(5) ด้านการกำกับดูแล จากภัยคุกคามไซเบอร์ที่เข้าโจมตีองค์กรบ่อยครั้ง และข้อมูลข่าวสารที่ได้รับจากผลกระทบหน่วยงานอื่นๆที่เกี่ยวข้อง ส่งผลให้ผู้บริหารระดับสูงขององค์กรเร่งปรับปรุงนโยบาย แผนยุทธศาสตร์องค์กร การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และการบริหารความเสี่ยง โดยคำนึงถึงผู้มีส่วนได้ส่วยเสียเป็นสำคัญ เพื่อกำหนดแนวปฏิบัติให้ครอบคลุมทุกภาคส่วนทั้งในเชิงนโยบายและเชิงเทคนิค

(6) ด้านบุคลากร ส่งผลในแง่การรับรู้และความตระหนักของพนักงานทุกระดับชั้นในแต่ละหน่วยงาน ซึ่งทำให้ทราบว่ายังขาดบุคลากรที่มีความเชี่ยวชาญและขาดการตระหนักรู้ถึงการป้องกันรับมือภัยคุกคามไซเบอร์

5.1.3 สาเหตุของปัญหาสถานการณ์ภัยคุกคามทางไซเบอร์

ปัญหาที่เกิดขึ้นในเรื่องภัยคุกคามทางไซเบอร์แบ่งออกเป็น 2 ส่วน ได้แก่ ด้านวิชาการหรือทฤษฎี และด้านการบริหารจัดการ ซึ่งหากเป็นด้านวิชาการ ตัวอย่างเช่น การเกิดรูรั่วหรือช่องโหว่ ต้องมีการตรวจสอบระบบปฏิบัติการหรือ Operation System และลักษณะของการถูกโจมตี แต่ปัญหาส่วนใหญ่เกิดจากด้านบริหารจัดการ โดยเฉพาะในองค์กร ปัญหาที่เป็นประเด็นสำคัญ

คือ Social Engineering ซึ่งเป็นเทคนิคการหลอกลวงที่เป็นพื้นฐานทางจิตวิทยา เพื่อให้เหยื่อเปิดเผยข้อมูลส่วนบุคคล หรือข้อมูลที่เป็นความลับขององค์กร เช่น ข้อมูลรหัสบัตรเครดิต ข้อมูลบัญชีผู้ใช้และรหัสผ่านของบริการต่างๆของเหยื่อ โดยที่ผู้ไม่ประสงค์ดีไม่จำเป็นต้องใช้เทคโนโลยีเข้ามาเกี่ยวข้องเลยแม้แต่น้อย แต่หากเป็นกลยุทธ์และวิธีการอันแยบยลที่ทำให้คนตกเป็นเหยื่อแบบไม่ทันตั้งตัว ดังนั้น องค์กรจึงจำเป็นต้องสร้างให้บุคลากรมีความตระหนักรู้หรือ Awareness ที่สำคัญไปกว่านั้นคือการสร้างนิสัยหรือที่เรียกว่า Habit Forming ตัวอย่างเช่น กรณีการใส่หมวกกันน็อค แต่บางคนไม่ใส่เพราะอาจมองข้ามสิ่งที่จำเป็นสำหรับตนเองไปเนื่องด้วยยังไม่มีเหตุกาณ์ใดมากระตุ้นให้ต้องทำสิ่งนี้ ดังนั้นการบังคับใช้อาจไม่เพียงพอและไม่ได้ผล จึงต้องเป็นการสร้างนิสัย หรือ Habit Forming ให้กับบุคคลในการเฝ้าระวังเพื่อรับมือเหตุการณ์ไม่คาดคิดที่อาจจะเกิดขึ้นในอนาคต

5.2 โครงสร้างการกำกับดูแลด้านเทคโนโลยีดิจิทัลขององค์กร การขับเคลื่อนด้วยนโยบายและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ในการบริหารจัดการ

ปัจจุบันหลายองค์กรในประเทศไทยเริ่มมีสภาวะตื่นตัวกับสถานการณ์ภัยคุกคามไซเบอร์ที่เกิดขึ้นตามรายงานข่าวและสื่อโซเชียลต่าง ๆ ไม่เว้นแต่ละวัน หลายองค์กรต้องเผชิญเหตุการณ์ภัยคุกคามกับองค์กรของตนเอง หรือแม้ที่เกิดขึ้นกับหน่วยงานที่มีการทำงานร่วมกันในการดำเนินงาน สิ่งนี้เป็นตัวกระตุ้นที่ทำให้องค์กรต่างๆหันมาทบทวนนโยบาย แผนยุทธศาสตร์ และแนวทางในการปฏิบัติงานในองค์กร และที่สำคัญไปกว่านั้นคือ หน่วยงานโครงสร้างพื้นฐานทางสารสนเทศที่สำคัญในประเทศไทย มีการปรับปรุงโครงสร้างองค์กร โดยเฉพาะด้านเทคโนโลยีดิจิทัล มีการแก้ไขทั้งในส่วนของบทบาทหลัก (Key Role) กระบวนการทำงาน (Process) และผลลัพธ์ของงาน (Output) อาทิ การประปาส่วนภูมิภาค และองค์กรที่มีแนวโน้มจะปรับปรุงโครงสร้าง อาทิ การไฟฟ้าส่วนภูมิภาค เพื่อรองรับลักษณะงานในด้านการรับมือและเฝ้าระวังภัยคุกคามทางไซเบอร์ตามแนวทางการกำกับดูแลของ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 และกฎหมายอื่นที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์

ในส่วนของมาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานควบคุมดูแลและการบริหารจัดการในหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศสอดรับกับปัจจัยที่สำคัญในการประเมินความมั่นคงปลอดภัยทางไซเบอร์ทั้งหมด 5 ด้าน ได้แก่

5.2.1 มาตรการทางกฎหมาย (Legal Measures)

แม้ว่าประเทศไทยมีกฎหมายอาญา (Criminal Legislation) ที่เกี่ยวกับการควบคุมการกระทำความผิดทางคอมพิวเตอร์ และมีกฎระเบียบและการปฏิบัติตามกฎระเบียบ (Regulation and Compliance) คือ การมีกฎที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์เฉพาะเรื่อง เช่น กฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์ กฎหมายการคุ้มครองข้อมูลส่วนบุคคล และกฎหมายการใช้ลายเซ็นอิเล็กทรอนิกส์ เป็นต้น อย่างไรก็ตาม กรอบของกฎหมายอย่าง พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ที่ใช้อยู่ในปัจจุบัน อาจยังไม่ครอบคลุมและชัดเจน โดยเฉพาะแนวทางมาตรฐานด้านเทคโนโลยีที่นำมาใช้ให้เกิดประสิทธิภาพต่อหน่วยงาน การบังคับใช้ แนวทางปฏิบัติตลอดจนการประสานงานเพื่อรายงานสถานกาณ์ และบทลงโทษ ภาครัฐจึงทบทวนและปรับปรุงแนวทางแก้ไขโดยการประกาศหลักเกณฑ์เพิ่มเติมจากคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ออกมาเป็นระยะๆ

5.2.2 มาตรการทางเทคนิค (Technical Measures)

มีการจัดตั้งหน่วยงานระดับชาติเพื่อตอบสนองเหตุการณ์ที่ละเมิดความมั่นคงปลอดภัยทางไซเบอร์ (CIRT (Computer incident Response Team), CIRT (Computer Emergency Response Team)) หรือ CSIRT (Computer Security incident Response Team) และหลายหน่วยงานมีการศึกษาและนำมาตรฐานทางเทคโนโลยีมาใช้ โดยการพิจารณาจากคณะกรรมการด้านบริหารภายในของแต่ละหน่วยงาน เช่น กรอบ NIST Cyber Security Framework และมาตรฐานทางเทคโนโลยี ISO/IEC 27001 รวมทั้งการออกใบรับรอง (Certifications) มาตรฐานเหล่านี้ แต่สำหรับบางหน่วยงานอาจไม่สามารถตัดสินใจลงทุนเองได้ เนื่องจากมีงบประมาณอยู่อย่างจำกัด ซึ่งต้องขึ้นอยู่กับการให้ความสำคัญด้านความมั่นคงปลอดภัยของผู้บริหารระดับสูงและการพิจารณาการจัดสรรเงินทุนหรืองบประมาณที่เพียงพอจากภาครัฐในการจัดหามาตรฐานทางเทคโนโลยีที่นำมาใช้เพื่อรองรับการตอบสนองต่อภัยคุกคามทางไซเบอร์

5.2.3 มาตรการการจัดโครงสร้างองค์กร (Organizational Measures)

หลายองค์กรนำกฎหมายหลักและกฎหมายรองของภาครัฐ มาปรับใช้เพื่อจัดทำและปรับปรุงนโยบาย (Policy) มีแผนด้านการกำกับดูแล (Roadmap for Governance) มีแนวทาง

ปฏิบัติ (Guidelines) และหน่วยงานผู้รับผิดชอบ (Responsible Agency) การเทียบเคียงกับหน่วยงานระดับชาติ (National Benchmarking) แต่เนื่องด้วยบางหน่วยงานเพิ่งริเริ่มจัดตั้งจากรัฐบาลเพื่อดูแลและจัดการด้านความมั่นคงปลอดภัยไซเบอร์ จึงทำให้ยังขาดแผนรองรับสถานการณ์ฉุกเฉินและแนวปฏิบัติที่ชัดเจน

5.2.4 การพัฒนาศักยภาพบุคลากร (Capacity Building)

มีการกำหนดมาตรฐานในการพัฒนาบุคลากร (Standardization Development) แผนการพัฒนาบุคลากร (Manpower Development Plan) การให้การรับรองแก่ผู้เชี่ยวชาญ (Professional Certification) การให้การรับรองหน่วยงาน (Agency Certification) การสร้างความตระหนักรู้ (Awareness) โดยเฉพาะหน่วยงานภาคการเงินการธนาคาร แต่หลายหน่วยงานยังขาดบุคลากรที่มีความเชี่ยวชาญในด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ทำให้การรับมือภัยคุกคามยังไม่มีประสิทธิภาพเท่าที่ควร ทั้งนี้เนื่องมาจากตามแผนการรับมือภัยไซเบอร์นั้น องค์กรควรจัดให้มีบุคลากรในการเฝ้าระวังสถานการณ์แบบ 24 ชั่วโมง 7 วันหรือ 24*7 เพื่อให้เป็นไปตามข้อปฏิบัติของศูนย์ปฏิบัติการ Security Operation Center (SOC) และควรเป็นผู้ที่ผ่านการอบรมและผ่านการรับรองด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)

5.2.5 การสร้างความร่วมมือ (Cooperation)

ประกอบด้วย การสร้างความร่วมมือระหว่างรัฐ (Intra-State Cooperation) การสร้างความร่วมมือระหว่างหน่วยงาน (Intra-Agency Cooperation) ความร่วมมือภาครัฐและภาคเอกชน (Public-private partnerships (PPP)) การสร้างความร่วมมือระหว่างประเทศ (International Cooperation) เป็นต้น ซึ่งประเทศไทยเอง มีศูนย์ประสานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์แห่งชาติ (NCERT) ซึ่งอยู่ภายในสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ทำหน้าที่ในการประสานงานและถ่ายทอดข้อมูลข่าวสารด้านไซเบอร์ให้กับหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศและหน่วยงานควบคุมหรือกำกับดูแล ตลอดจนหน่วยงานภาครัฐที่เกี่ยวข้อง โดยมุ่งเน้นการสร้างความตระหนักรู้ให้กับบุคลากรและประชาชนในการรับมือภัยคุกคามทางไซเบอร์

5.3 ประสิทธิภาพการรับมือภัยคุกคามทางไซเบอร์ขององค์กรในประเทศไทย

ความมั่นคงปลอดภัยไซเบอร์ ถือว่ามีความสำคัญอย่างยิ่งในการปกป้องทรัพยากรของประเทศ ทว่า การที่จะทำให้เทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัยจะต้องมีการบริหารจัดการและการกำกับดูแลที่ดี รวมไปถึงกระบวนการในการดำเนินการอย่างเป็นระบบ และกระบวนการเหล่านั้นได้ถูกกำหนดเอาไว้เป็นมาตรฐานที่เป็นที่ยอมรับ โดยมีองค์กรหรือสถาบันที่มีชื่อเสียงเป็นผู้กำหนดเกณฑ์และแนวทางในการปฏิบัติ ทั้งนี้ ประเทศไทยเองต่างตระหนักถึงภัยคุกคามทางไซเบอร์ที่เกิดจากความเป็นพลวัตของเทคโนโลยีอยู่ตลอดเวลา โดยมีการประเมินความเสี่ยงภัยไซเบอร์ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่ครอบคลุมทั้งในระดับนโยบาย การจัดการองค์กรและเทคโนโลยี เพื่อเฝ้าระวังและรับมือภัยคุกคามทางไซเบอร์ ซึ่งแต่ละประเทศสามารถเลือกมาตรฐานที่มีความเหมาะสมกับประเทศของตน และอาจเพิ่มเติมหรือยกเว้นการปฏิบัติในบางส่วนได้หากมีเหตุผลเพียงพอ

อย่างไรก็ตาม การจัดการความมั่นคงปลอดภัยไซเบอร์ในภาพรวมของประเทศไทยยังไม่มีประสิทธิภาพเท่าที่ควร เนื่องด้วยความมั่นคงปลอดภัยบนโลกไซเบอร์นั้น ไม่ได้เป็นเพียงแค่การจัดการที่เกี่ยวกับภัยคุกคามภายนอก (External Threat) และภัยคุกคามภายใน (Internal Threat) ไม่ว่าจะเกิดขึ้นด้วยเหตุบังเอิญ (Accidental) หรือมีสาเหตุมาจากผู้ไม่ประสงค์ดี ทั้งหมดนี้ล้วนก่อให้เกิดความเสี่ยงที่สำคัญต่อภาคธุรกิจขององค์กรทั้งสิ้น ดังนั้น การรักษาความปลอดภัยบนระบบเครือข่ายอย่างมีประสิทธิภาพ จึงเป็นกุญแจสำคัญในการป้องกันการสูญหายของข้อมูลและเป็นการเตรียมความพร้อมในการรับมือเพื่อจัดการกับปัญหาจากภัยคุมคามทางไซเบอร์ ที่อาจจะกลายเป็นอาชญากรรมรูปแบบใหม่ได้ในอนาคต

5.4 ข้อเสนอแนะ

จากปัญหาและผลกระทบที่เกิดขึ้นจากสถานการณ์ภัยคุกคามทางไซเบอร์ทั้งในด้านการขาดแคลนบุคลากร ความไม่พร้อมด้านมาตรฐานทางเทคโนโลยี และความไม่ชัดเจนของกฎหมายที่มีอยู่ นำไปสู่ข้อเสนอแนะเชิงนโยบายและข้อเสนอแนะเชิงปฏิบัติการ ดังนี้

5.4.1 ข้อเสนอแนะเชิงนโยบาย

จากการศึกษาสถานการณ์ภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของประเทศไทยนั้น แนวทางการกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์

ควรที่จะสามารถออกนโยบาย (Enact Policies) และกลยุทธ์ลดความเสี่ยงขององค์กรที่ควบคุมได้ทั้งภายในและทั่วทั้งเครือข่าย เพื่อให้องค์กรสามารถดำเนินการได้โดยลดแรงเสียดทานและความเสี่ยงต่างๆให้น้อยที่สุด รวมทั้งประเด็นด้านมาตรการทางกฎหมาย อาจไม่ใช่แค่เพื่อแก้ปัญหาในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ แต่ควรให้ความสำคัญในเรื่องมาตรการเสริมสร้างจิตสำนึกและความตระหนักรู้ การพัฒนาสิทธิรับรู้ข้อมูลข่าวสารในกระบวนการธรรมรัฐไทย การออกมาตรการทางกฎหมายเพื่อการคุ้มครองข้อมูลส่วนบุคคลเป็นสำคัญและจำเป็นในระดับนโยบายของรัฐ (National Policy) ดังนี้

(1) ด้านกฎหมาย รัฐบาลควรออกกฎหมายที่ชัดเจนให้หน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศและองค์กรที่เกี่ยวข้อง เนื่องจากมีกฎหมายหลายฉบับที่ประกาศออกมา ตั้งแต่ปี พ.ศ.2544 แต่ยังไม่มีการอธิบายถึงตัวกฎหมายให้ชัดเจน และกฎหมายบางอย่างซ้ำซ้อนกัน โดยเฉพาะด้านไซเบอร์ ซึ่งมองว่ากฎหมายบางอย่างหากไม่มีการนำมาใช้ ควรประกาศยกเลิกหรือนำมาพิจารณาปรับปรุงและปรับให้ทันสมัยมากขึ้น และเนื่องด้วยการประกาศกฎหมายฉบับก่อนหน้าและฉบับปัจจุบันในด้านการป้องกันและรักษาความมั่นคงปลอดภัยไซเบอร์ ออกโดยหน่วยงานที่ต่างกัน แต่คนปฏิบัติตามกฎหมายเป็นคนกลุ่มเดียวกัน

(2) ด้านนโยบายการบริหารจัดการองค์กร

ภาครัฐ ควรหามิติที่ชัดเจนในการกำกับดูแลและการวัด ประเมินผล KPI ต้องชัดเจนและประเมินได้ว่าวัดแล้วดีขึ้นอย่างไร รวมถึงควรมีการถ่ายทอดสื่อสารให้กับคณะกรรมการระดับสูงสุดของแต่ละหน่วยงานได้ และควรมีการจัดตั้งคณะทำงานโดยเฉพาะที่ประสานงานทั้งหมดทุกด้านได้

องค์กร จะต้องเน้นการบริหารด้านการจัดสรรทรัพยากร ทั้งเรื่องของ เงิน คน และเวลา เรื่องของการจัดทำแผนนำทาง (Roadmap) และการจัดทำสถาปัตยกรรมองค์กร (Enterprise Architecture: EA) ควรต้องมีการปรับปรุงทุกปี ควรมีที่ปรึกษาหรือผู้เชี่ยวชาญและคณะกรรมการคอยติดตามให้คำแนะนำในเรื่องความปลอดภัย (Security) และต้องมีการประชุมเพื่อรับฟังความคิดเห็นจากพนักงานที่เกี่ยวข้องร่วมกันในการพัฒนาและมองถึงความเป็นไปได้ในอนาคต ซึ่งต้องให้ความสำคัญกับคนและการสื่อสารเป็นหลัก

(3) ด้านการสร้างความตระหนัก หน่วยงานกลางหรือภาครัฐควรปลูกฝังและสร้างความตระหนักเรื่องภัยไซเบอร์ตั้งแต่ระดับการศึกษาประถม มัธยม โดยมีนโยบายให้เพิ่มทักษะทางวิชาการด้านความปลอดภัยทางไซเบอร์เป็น 1 วิชาที่สำคัญที่ทุกโรงเรียนหรือสถาบันการศึกษาควรมี

การเรียนการสอนให้ทันต่อยุคดิจิทัล ยุคแห่งการสื่อสารและการแพร่หลายของอินเตอร์เน็ตโซเชียลต่างๆ เพราะจะเป็นการสร้างพฤติกรรมหรือสร้างลักษณะนิสัย (Habit forming) ให้คนตั้งแต่ระดับเยาว์วัยได้ตระหนักและเฝ้าระวังภัยคุกคามทางไซเบอร์ให้เป็นนิสัย จะทำให้ได้ผลอย่างทั่วถึงทุกพื้นที่การศึกษาทั่วประเทศ แก้ปัญหาได้อย่างมีประสิทธิภาพเนื่องจาก เด็กที่ได้รับความรู้ในด้านดิจิทัลนี้ ไม่ว่าเติบโตมาในสายอาชีพใด ก็จะมีความตระหนักและพฤติกรรมการระวังภัยอยู่เสมอ

(4) ด้านงบประมาณ รัฐบาลควรสนับสนุนงบประมาณให้หน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศและหน่วยงานที่เกี่ยวข้องมีงบประมาณเพียงพอต่อการนำไปใช้ในการพัฒนา ป้องกัน และรับมือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ ควรให้ความสำคัญในด้านความปลอดภัยเป็นอันดับแรก

(5) ด้านวิชาชีพ รัฐบาลหรือหน่วยงานที่มีส่วนในการจัดสรรคนในตลาดแรงงานควรกำหนดให้มีอาชีพด้านความมั่นคงปลอดภัยไซเบอร์ ที่เป็นวิชาชีพที่สามารถกำหนดอัตรากำลังและค่าแรงขั้นต่ำต่อพนักงานในการปฏิบัติงาน รวมถึงกำหนดในเรื่องของรายได้ กฎเกณฑ์ขั้นต่ำของอาชีพนี้เป็นอย่างไร ทั้งนี้ ในส่วนของใบรับรองวิชาชีพหรือหลักสูตรที่พนักงานได้ผ่านการอบรมและได้รับ Certificate ควรมีค่าตอบแทนให้พนักงานเนื่องจากการอบรมด้านความมั่นคงปลอดภัยไซเบอร์ค่อนข้างยากและซับซ้อนต่อการทำความเข้าใจ

(6) ด้านมาตรฐานทางเทคโนโลยี หน่วยงานกลางที่ออกกฎหมายแนวทางการปฏิบัติตาม พ.ร.บ. หรือประกาศ รวมถึงข้อบังคับใดๆที่เป็นแนวทางด้านความมั่นคงปลอดภัยไซเบอร์ควรมีกระบวนการด้านความมั่นคงปลอดภัยไซเบอร์ที่ชัดเจนในเรื่องของมาตรฐานต่างๆ มาประยุกต์ใช้ร่วมกัน ได้แก่ ISO/IEC 27001:2013 และ NIST Cyber security Framework เนื่องด้วยกฎหมายที่ประกาศออกมาไม่ได้ระบุถึงมาตรฐานสากลที่ชัดเจนให้หน่วยงานเลือกใช้ เพราะหลายหน่วยงานไม่มีความเชี่ยวชาญในด้านนี้เท่าที่ควร

5.4.2 ข้อเสนอแนะเชิงปฏิบัติการ

มาตรการทางกฎหมายและการดำเนินการบังคับใช้กฎหมาย ยากที่จะสัมฤทธิ์ผลถ้าไม่มีการสร้างความตระหนักรู้ การพัฒนาทักษะ ความรู้ ความเข้าใจ และเสริมสร้างจิตสำนึกของเจ้าหน้าที่ของรัฐและประชาชนควบคู่ไปกับการใช้มาตรการทางกฎหมาย เมื่อพิจารณาถึงประเด็นการแก้ไขปัญหาภัยคุกคามทางไซเบอร์ซึ่งนอกจากมิติของตัวบทกฎหมาย การบังคับใช้กฎหมาย การกำหนดมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ การนำนโยบายและมาตรการเหล่านี้ไปใช้ใน

องค์กรและสื่อสารให้บุคลากรในองค์กรปฏิบัติตามอย่างเคร่งครัด จะช่วยให้ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ดังนั้น การถ่ายทอดกระบวนการด้านการกำกับดูแลและการรับมือเพื่อปองกันภัยคุกคามทางไซเบอร์โดยใช้วิธีการวิจัยที่หลากหลายร่วมกัน จะช่วยตอบประเด็นข้อสงสัยดังกล่าวได้อย่างครอบคลุม และชัดเจน ทำให้เข้าใจปัญหาสาเหตุและความเสี่ยงภัยคุกคามทางไซเบอร์มากยิ่งขึ้น เพื่อประโยชน์ในการวิเคราะห์หาแนวทางการป้องกันและคาดการณ์ เหตุการณ์หรือแนวโน้มภัยคุกคามในอนาคตสำหรับกำหนดแนวนโยบายในการรับมือและป้องกันภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ในประเทศไทยต่อไป โดยแบ่งแยกประเด็นได้ดังนี้

(1) องค์กรควรพยายามลดจุดอ่อนหรือความเสี่ยงให้น้อยลงมากที่สุด เพื่อให้เกิดผลกระทบกับผู้มีส่วนได้ส่วนเสียให้อยู่ในระดับที่ต่ำที่สุด ควรมีผู้ที่ดูแลและรับมือภัยคุกคามแบบ 24 ชั่วโมง 7 วัน หรือ 24*7 เนื่องด้วยตอนนี้หลายหน่วยงานยังไม่สามารถดำเนินการได้เอง เนื่องจากจำนวนพนักงานที่มีความเชี่ยวชาญด้านไซเบอร์มีอยู่อย่างจำกัด

(2) ควรมีการจัดทำ SOC หรือจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์ในองค์กร เพราะจะทำให้การจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ได้อย่างมีประสิทธิภาพ

(3) ควรให้หน่วยงานฝึกซ้อมการรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้นได้ในอนาคต เพราะสิ่งที่จะหยุดเหตุได้คือการรับมือกับเหตุนั้นๆ เป็นเรื่องสำคัญ ซึ่งหลายหน่วยงานยังไม่แนวปฏิบัติหรือแผนการรับมือในส่วนนี้

(4) บุคลากรในองค์กรและผู้มีส่วนได้ส่วนเสียควรได้รับการอบรมและสร้างความตระหนักรู้ให้ได้มากที่สุด เช่น ผู้ใช้งานระบบ (User) ผู้ดูแลระบบ (Administrator) ผู้บริหาร (Executive) คู่ค้า (Counterparty) คู่ความร่วมมือ (Partnership) หน่วยงานภายนอก (Outsource)

(5) ควรได้รับการจัดสรรงบประมาณในการซื้อเครื่องมือหรืออุปกรณ์ เช่น เครื่อง CCTV อย่างไรก็ตาม ควรต้องมีการจัดสรรกำลังคนในส่วนนี้ไว้ด้วย เนื่องจากต้องมีผู้ที่คอย monitor ระบบอยู่ตลอดเวลาและเป็นเรื่องของสิทธิ์ในการเข้าถึงระบบ

(6) ด้านการพัฒนาบุคลากร พร้อมกับการปฏิบัติงานเชิงรับของระบบและภัยคุกคาม รวมถึงการปฏิบัติงานเชิงรุกในการตรวจหาและหยุดยั้งภัยคุกคาม ซึ่งองค์กรต้องมีการพัฒนาบุคลากรให้สามารถดำเนินการคืนสภาพเมื่อมีภัยคุกคามทางไซเบอร์ที่ประกอบด้วย การระบุความเสี่ยง การป้องกันความเสี่ยง การตรวจจับภัยคุกคาม การตอบสนองต่อภัยคุกคาม และการกู้คืน พร้อม

ทั้งมีการเรียนรู้จากกรณีภัยคุกคามต่างๆ ที่เกิดขึ้น เพื่อให้องค์กรมีความสามารถในการคืนสภาพได้ทางไซเบอร์ที่รวดเร็ว ลดผลกระทบและความเสียหายที่จะเกิดขึ้นจากองค์กร

(7) หน่วยงานด้านกระบวนการยุติธรรม ซึ่งเป็นหน่วยงานที่อาจตกเป็นเป้าหมายที่สำคัญของแฮกเกอร์หรืออาชญกรได้นั้น ควรให้ความสำคัญกับการวางแผนและรับมือภัยคุกคามทางไซเบอร์ให้ดีที่สุด เพื่อไม่ให้เกิดผลกระทบต่อความมั่นคงปลอดภัยของประเทศชาติในอนาคต

5.4.3 ข้อจำกัดในการวิจัย

การวิจัยเรื่องนี้ อยู่ในช่วงของสถานการณ์การแพร่ระบาดของโรคติดเชื้อไวรัสโคโรนา 2019 (COVID-19) ส่งผลให้กระบวนการวิจัยในขั้นตอนของการเก็บรวบรวมข้อมูลล่าช้าและต้องปรับเปลี่ยนตามสถานการณ์การแพร่ระบาดดังกล่าว โดยการวิจัยเชิงคุณภาพ ซึ่งเป็นการสัมภาษณ์ผู้ปฏิบัติงานระดับผู้บริหารที่เป็นกลุ่มตัวอย่าง โดยปรับเลี่ยนไปใช้การสัมภาษณ์ทางออนไลน์เป็นบางส่วน ส่งผลให้บรรยากาศในการสนทนาขาดความสัมพันธ์ระหว่างผู้วิจัยและผู้ให้ข้อมูล การตอบข้อซักถามเป็นไปอย่างกระชับในบางกรณีที่สิ่งแวดล้อมไม่เอื้ออำนวย ข้อมูลที่ได้อาจจะไม่รอบด้านและครอบคลุมในประเด็นอื่น ๆ ที่เกี่ยวข้อง ดังนั้น ในการวิจัยครั้งต่อไป เมื่อเกิดสถานการณ์ที่ไม่สามารถดำเนินการวิจัยได้ตามแบบแผนที่กำหนด จึงควรมีการเตรียมมาตรการรองรับและออกแบบการวิจัยให้มีสอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป โดยไม่ให้มีผลกระทบต่อกระบวนการเก็บรวมรมข้อมูลการวิจัย

5.4.4 ข้อควรระวังในการนำงานวิจัยไปใช้

การวิจัยเรื่อง แนวทางการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ขององค์กรในยุคดิจิทัล เป็นงานวิจัยริเริ่มฉบับแรกซึ่งยังไม่เคยมีการศึกษาเกี่ยวกับแนวทางการกำกับดูแลเพื่อรับมือภัยคุกคามทางไซเบอร์ที่อาจจะเกิดกับหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศด้านสาธารณูปโภค ทั้งในประเทศและต่างประเทศ การทบทวนวรรณกรรมเกี่ยวกับปัญหาภัยคุกคามทางไซเบอร์อาจจะยังไม่ครบถ้วนและรอบด้าน เนื่องจากเป็นลักษณะภัยคุกคามทางไซเบอร์มีความเป็นพลวัตและเกิดขึ้นในรูปแบบใหม่ได้ทุกเวลา ซึ่งต้องอาศัยการวิจัยต่อไปอีกในหลายประเด็นเพื่อเป็นการสร้างองค์ความรู้เกี่ยวกับการป้องกันและรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ใน

เชิงลึก ดังนั้น การนำงานวิจัยเรื่องนี้ไปใช้ในการอ้างอิง ควรใช้อย่างระมัดระวัง โดยต้องเพิ่มเติมข้อมูลสนับสนุนที่เกี่ยวข้องกับเรื่องนั้น ๆ

5.4.5 ข้อเสนอแนะสำหรับงานวิจัยครั้งต่อไป

งานวิจัยชิ้นนี้อาจมีข้อจำกัดหรือข้อบกพร่องอยู่บ้าง เนื่องจากผู้วิจัย ไม่สามารถศึกษาวิจัยหน่วยงานโครงสร้างพื้นฐานให้ครอบคลุมหรือมีความสมบูรณ์ได้ทุกด้าน ซึ่งผู้วิจัยเลือกเก็บข้อมูลวิจัยเฉพาะหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศเฉพาะด้านสาธารณสุข สาธารณูปโภค การเงินการธนาคาร แต่ยังมีหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศอื่นๆ อีก เช่น หน่วยงานด้านความมั่นคงของรัฐ หน่วยงานด้านบริการภาครัฐที่สำคัญ หน่วยงานด้านโทรคมนาคม หน่วยงานด้านขนส่งและโลจิสติกส์ เป็นต้น รวมถึงมีข้อจำกัดเรื่องขอบเขตเนื้อหาที่ศึกษา การเข้าถึงประชากรหรือการเลือกกลุ่มตัวอย่าง ตลอดจนระยะเวลาในการเก็บรวบรวมข้อมูลหรืองบประมาณ เป็นต้น ทั้งนี้ เพื่อให้งานวิจัยมีความสมบูรณ์หรือมีการพัฒนาต่อไป

บรรณานุกรม

ภาษาไทย

กรมพัฒนาสังคมและสวัสดิการ. (2563). *รูปแบบภัยคุกคามด้านไซเบอร์*. http://www.dsdw2016.dsdw.go.th/doc_pr/ndc_2560-2561/PDF/8498st/5.บทที่%203.pdf

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2561). *คู่มือการจัดตั้งซีเซิร์ต (Establishing a CSIRT)*. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน).

--------. (2563). *สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ: เกี่ยวกับ สกมช*. https://www.mdes.go.th/mission/detail/2481

กรุงเทพธุรกิจ. (2563). ต่างประเทศ: โจมตีทางไซเบอร์' สงครามตัวแทนสหรัฐ-อิหร่าน. *กรุงเทพธุรกิจ*. https://www.bangkokbiznews.com/world/861631

--------. (2564). คอลัมนิสต์: ยุทธศาสตร์ความมั่นคงไซเบอร์ของสิงคโปร์. *กรุงเทพธุรกิจ*. https://www.bangkokbiznews.com/blogs/columnist/114696

กสทช. (2558). *คู่มือ Cyber security สำหรับประชาชน*. สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.).

กัลยา ชินาธิวร. (2562). *ปัจจัยความสำเร็จของสิงคโปร์: กรณีศึกษาเพื่อประกอบการพัฒนาแนวทางการดำเนินการตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทย*. กระทรวงการต่างประเทศ.

กาญจนา แก้วเทพ กิตติ กันภัย และสมสุข หินวิมาน. (2560). *สายธารแห่งนักคิดทฤษฎีเศรษฐศาสตร์การเมืองกับสื่อสารศึกษา*. อินทนิล.

ข่าวสดออนไลน์. (2565, 26 ตุลาคม). *กระอัก ออสเตรเลีย ถูกเจาะระบบซ้ำ ข้อมูลสุขภาพรั่วไหล 4 ล้านคน*. https://www.khaosod.co.th/around-the-world-news/news_7334192

ไซเบอตรอน. (2565). *CYBER 911: ศูนย์ปฏิบัติการเฝ้าระวังรักษาความปลอดภัยทางไซเบอร์ยุค New Normal*. https://cybertron.co.th/cyber-911/

ณภัทร เรืองนภากุล. (2564, 15 สิงหาคม). *ความเป็นพลเมืองยุคดิจิทัลกับการรับมือด้านมืดออนไลน์ในวิถีปรกติใหม่*. https://erp.mju.ac.th/acticleDetail.aspx?qid=1198

ณัฐวี อุตกฤษฎ์. (2555). การวางแผนรองรับเหตุการณ์ฉุกเฉินเพื่อความมั่นคงสารสนเทศในองค์กร. *วารสารเทคโนโลยีสารสนเทศ*, *8*(2), 64-72.

ดิเรกฤทธิ์ บุษยธนากรณ์. (2563). *แบบจำลองการคาดคะเนปัจจัยที่เป็นข้อบ่งชี้ลักษณะอาชญากรรมลูกผสมในสังคมไทย*. [วิทยานิพนธ์ปรัชญาดุษฎีบัณฑิต, จุฬาลงกรณ์มหาวิทยาลัย]. Chulalongkorn University Intellectual Repository(CUIR). http://cuir.car.chula.ac.th/bitstream/123456789/76413/1/6181360024

เดลินิวส์. (2563, 9 กันยายน). แฮกเกอร์ส่ง 'มัลแวร์' เรียกค่าไถ่ รพ.สระบุรี 6.3 หมื่นล้าน. *เดลินิวส์*. https://d.dailynews.co.th/regional/794273/

ทีมมายด์อินไซต์. (2564, 7 กันยายน). *[Extreme History] Stuxnet Worm ไวรัสตัวแรกที่ถูกใช้เป็นอาวุธไซเบอร์ (แต่ช่วยหยุดสงครามโลกไว้ได้)*. https://www.extremeit.com/extreme-history-stuxnet/

ทีเอ็นเอ็น. (2563). *โรงพยาบาลสระบุรี ถูกไวรัสโจมตี เรียกค่าไถ่ 6.3 หมื่นล้านรับมือ*. https://www.tnnthailand.com/content/54304

ไทยรัฐออนไลน์. (2565, 23 มิถุนายน). *เทคโนโลยี: Microsoft เผยรัสเซียยกระดับการโจมตีทางไซเบอร์ต่อชาติพันธมิตรยูเครน*. https://www.thairath.co.th/news/tech/2426840

--------. (2565, 28 มิถุนายน). *เทคโนโลยี: แฮกเกอร์รัสเซีย อ้างความรับผิดชอบการโจมตีทางไซเบอร์ในประเทศลิทัวเนีย.* https://www.thairath.co.th/news/tech/2430730

ธนาคารแห่งประเทศไทย. (2562). "*กรอบการประเมินความพร้อมด้าน Cyber Resilience*". https://www.bot.or.th/content/dam/bot/fipcs/documents/FOG/2562/ThaiPDF/25620272.pdf

นคร เสรีรักษ์. (2548). *การคุ้มครองข้อมูลส่วนบุคคล: ข้อเสนอเพื่อการพัฒนาสิทธิรับรู้ข้อมูล ข่าวสารในกระบวนการธรรมรัฐไทย*. [วิทยานิพนธ์ปรัชญาดุษฎีบัณฑิต, มหาวิทยาลัยธรรมศาสตร์].

นัทธมน เพชรกล้า. (2564). *การรับมือของภาครัฐกับการก่อการร้ายทางไซเบอร์ในประเทศไทย.* [วิทยานิพนธ์ปรัชญาดุษฎีบัณฑิต, จุฬาลงกรณ์มหาวิทยาลัย]. Chulalongkorn University Intellectual Repository (CUIR). https://cuir.car.chula.ac.th/handle/123456789/80926

บริษัทโทรคมนาคมแห่งชาติ จำกัด (มหาชน). (2565, 18 กุมภาพันธ์). *สรุปสถิติภัยคุกคามปี 2564 จากศูนย์ปฏิบัติการ CSOC ของ NT cyfence*. https://www.cyfence.com/article/ntcyfence-csoc-summary-2021/

--------. (2565, 24 มีนาคม). *ศูนย์* CSOC *คืออะไร มีความสำคัญอย่างไรในด้าน* Cybersecurity *กับองค์กร.* https://www.cyfence.com/article/what-is-a-csoc-center-and-why-is-it-important-to-cybersecurity/

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. 2564. (2564, 23 สิงหาคม). *ราชกิจจานุเบกษา*. เล่ม 138 ตอนพิเศษ 194 ง. หน้า 14-15.

ประชาชาติธุรกิจ. (2564, 3 กรกฎาคม). *"เอสโตเนีย" กับการป้องกัน สงครามไซเบอร์*. https://www.prachachat.net/ict/news-703725

ปริญญา หอมอเนก. (2561). *Strategy to Cybersecurity 4.0*. ห้างหุ้นส่วนจำกัด โรงพิมพ์วัชรินทร์พี.พี.

--------. (2561, 8 สิงหาคม). คอลัมนิสต์: ทางแก้ปัญหาการโจมตีทางไซเบอร์ด้วย *3* วินัยที่ควรปฏิบัติ. *กรุงเทพธุรกิจ*. https://www.bangkokbiznews.com/blogs/columnist/120162

--------. (2562). *ความมั่นคงปลอดภัยไซเบอร์ของชาติ ปัญหาอธิปไตยไซเบอร์ ผลกระทบต่อความมั่นคงของชาติในระยะยาวและแนวทางการกำหนดยุทธศาสตร์ชาติ* [เอกสารวิจัยส่วนบุคคล] วิทยาลัยป้องกันราชอาณาจักร.

--------. (2564, 2 มกราคม). *ผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ของชาติ: ปัญหาอธิปไตยไซเบอร์และแนวทางการกำหนดยุทธศาสตร์ชาติ ตอนที่ 3*. https://itgthailand.wordpress.com/tag/national-cybersecurity/

ผู้จัดการออนไลน์. (2563, 9 กันยายน). ภาคกลาง-ตะวันออก: ผอ.รพ.สระบุรี แจงโจรไซเบอร์แฮกข้อมูล รพ.สระบุรี เรียกค่าไถ่ข้อมูลคนไข้. *ผู้จัดการ*. https://mgronline.com/local/detail/9630000092463

--------. (2564, 7 กันยายน). รพ.เพชรบูรณ์แจงยิบ มือมืดแฮกข้อมูลผู้ป่วยแค่ 10,000 กว่าชื่อ สั่งปิดกั้นคนนอกเข้าถึงอินเทอร์เน็ตแล้ว. *ผู้จัดการ*. https://mgronline.com/local/detail/9640000088648

พรชัย ขันตี และคณะ. (2543). *ทฤษฎีและงานวิจัยทางอาชญาวิทยา*. สำนักพิมพ์บุคเน็ท จำกัด.

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. (2562, 27 พฤษภาคม). *ราชกิจจานุเบกษา*. เล่ม 136 ตอนที่ 69 ก. หน้า 20-51.

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. (2562, 27 พฤษภาคม). *ราชกิจจานุเบกษา*. เล่ม 136 ตอนที่ 69 ก. หน้า 52-95.

ไพรัตน์ พงศ์พานิชย์. (2561, 7 สิงหาคม). นิวส์รูมวิเคราะห์: การโจมตีทางไซเบอร์ บทเรียนจากสิงคโปร์. *มติชน*. https://www.matichon.co.th/newsroom-analysis/news_1076346

เมธาพร ธรรมศิริ และ ศิรภัสสรศ์ วงศ์ทองดี. (2565). ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากร ในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร Cyber Security Awareness of

Employees in One Private Company in Bangkok Area. *วารสารวิชาการไทยวิจัยและการจัดการ Thai Research and Management Journal*, *3*(2), 13.

ราม โชติคุต. (2554, 1 ธันวาคม). *มองรุสโซในฐานะนักวิพากษ์สังคมสมัยใหม่* (*Rousseau as The Modern Social Critic)*. https://v-siam.blogspot.com/2011/12/rousseau-as-modern-social-critic.html

วัชรวรรณ ดวงสะเก็ด. (2555). *ความพร้อมของเทศบาลตำบลในจังหวัดเชียงใหม่ต่อการรับถ่ายโอนงานทะเบียนราษฎร* [ภาคนิพนธ์ รป.ม., มหาวิทยาลัยเชียงใหม่].

วิลาส วิถีไพร. (2561). *การพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเตอร์เน็ตประสานสรรพสิ่ง THE DEVELOPMENT OF CYBERSECURITY FRAMEWORK FOR INTERNET OF THINGS* [สารนิพนธ์วิทยาศาสตรมหาบัณฑิต, มหาวิทยาลัยศรีปทุม].

ศรีสมบัติ โชคประจักษ์ชัด. (2561). *ตำรา เหยื่ออาชญากรรม : สิทธิและการช่วยเหลือเยียวยา*. สำนักพิมพ์คณะรัฐมนตรีและราชกิจจานุเบกษา.

ศิวลีย์ สิริโรจน์บริรักษ์. (2558). การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security). *บทความวิชาการสถาบันวิชาการป้องกันประเทศ*. กระทรวงกลาโหม.

สรรสิริ สิริสันตคุปต์. (2565, 12 เมษายน). *การโจมตีโครงสร้างพื้นฐานที่สำคัญของประเทศ ในสถานการณ์ความขัดแย้ง ยูเครน รัสเซีย*. https://www.cioworldbusiness.com/sansiri-sirisantakupt-attacks-on-the-countrys-critical-infrastructure-in-the-conflict-situation-ukraine-russia/

สาวตรี สุขศรี. (2560). อาชญากรรมคอมพิวเตอร์/ไซเบอร์กับทฤษฎีอาชญาวิทยา. วารสารนิติศาสตร์, *46*(2).

สำนักข่าวอินโฟเควสท์. (2564, 9 มิถุนายน). *In Focus: Cyber Attack – คลื่นใต้น้ำแห่งยุคดิจิทัลที่ต้องจับตามอง*. https://www.infoquest.co.th/2021/94874

สำนักงานตำรวจแห่งชาติ. (2565). *การรับแจ้งความทางออนไลน์คดีอาชญากรรมทางเทคโนโลยี*. https://www.thaipoliceonline.com/

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2564, 8 มิถุนายน). *CS101 ความมั่นคงปลอดภัยไซเบอร์เบื้องต้น.* https://www.etda.or.th/th/Useful-Resource/Knowledge-Sharing/Articles/Cybersecurity-101.aspx

--------. (2565). *สถิติภัยคุกคามประจำปี 2560-2564*. https://www.cyfence.com/article/2021-threat-statistics-summary-from-csoc-by-nt-cyfence/

สำนักงานเลขาธิการวุฒิสภา. (2561). *รายงานของคณะกรรมาธิการวิสามัญ พิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... พิจารณา ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....* สภานิติบัญญัติแห่งชาติ.

สำนักงานสภาความมั่นคงแห่งชาติ. (2561). *ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.2560 – 2564 (National Cybersecurity Strategy 2017 – 2021)*. สำนักพิมพ์คณะรัฐมนตรีและราชกิจจานุเบกษา.

สำนักงานสภาพัฒนาเศรษฐกิจและสังคมแห่งชาติ. (2561). *แผนแม่บทภายใต้ยุทธศาสตร์ชาติ*. http://nscr.nesdb.go.th

สุมนทิพย์ จิตสว่าง. (2562). *เอกสารประกอบการสอน วิชา "2403313 อาชญาวิทยา (Criminology)"*. https://drive.google.com/ file/d/1V9A2a5ulbJlXnl03qD_ vgzMR9pDEW3yh/view

อนาวิล แก้วสะอาด และ ณัฐวี อุตกฤษฎ์. (2564). แนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร. *วารสารสถาบันวิชาการป้องกันประเทศ*, *12*(1), 6-20.

อัญรัตน์ จันทร์เจริญสุข. (2552). *เทคนิคการจารกรรมข้อมูลสารสนเทศผ่านทางกระบวนการ ทางสังคม กรณีศึกษา ธนาคารพาณิชย์แห่งหนึ่ง* [สารนิพนธ์วิทยาศาสตร มหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์].

อัศว์ณุต แสงทองดี และญาณพล ยั่งยืน. (2563). แนวทางการรับมือและการรับแจ้งเหตุของตำรวจต่อกรณีมัลแวร์เรียกค่าไถ่. *วารสารสหศาสตร์*, *21*(1). คณะสังคมศาสตร์และมนุษยศาสตร์.

อีวาน พอร์ทเตอร์. (2565). การโจมตี *DDoS* คืออะไรและจะป้องกันมันได้อย่างไรในปี *2022*. https://th.safetydetectives.com/blog/what-is-a-ddos-attack-th/

เอซิสออนไลน์. (2564). *"บทวิเคราะห์กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ระดับโลก" – NIST's Framework for Improving Critical Infrastructure Cybersecurity "โอกาส ภัยคุกคาม และ ความเสี่ยงที่ผู้บริหารองค์กรต้องตระหนัก"*. www.acisonline.net/?p=4036&lang=th

ไอซาก้า. (2555). *COBIT 5 : กรอบการดำเนินงานทางธุรกิจสำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร. ISACA.* http://audit.sat.or.th/v2project/object/Download_File/COBIT-5_res_tha_1213.pdf

ภาษาต่างประเทศ

Appadurai, A. (1990). Disjuncture and Difference in the Global Cultural Economy. *Theory Culture & Society*, *7*, 295-310.

Back, S. L., J. (2020). Cyber-situational crime prevention and the breadth of cybercrimes among higher education institutions. *International Journal of Cybersecurity Intelligence and Cybercrime*, *3*(2), 25-47. https://www.doi.org/10.52306/RGWS2555

Beck, U. (1992). *Risk Society: Towards a New Modernity*. Sage publications Ltd, London.

Belani, G. (2020). *5 Cybersecurity Threats to Be Aware of in 2020*. IEEE. https://www.computer.org/publications/tech-news/trends/5-cybersecurity-threats-to-be-aware-of-in-2020

Bevis, J. (2007, June 26). *Xtreme Social Engineering-combating the Insider Security ThreatA Security Awareness Exercise*. https://jtbevis. files.wordpress.com/2007/09/article-social-eng-v-7921

Brantingham, P. L., & Brantingham, P. J. (1993). Nodes, paths and edges: Considerations on the complexity of crime and the physical environment. *Journal of Environmental Psychology*, *13*(1), 3-28.

--------. (1995). Criminality of place. *European Journal on Criminal Policy and Research*, *3*(3), 5-26.

Bronitt, S., & Gani, M. (2005). *Cyber-Crime in the 21st Century: Windows on Australian Law*. Hong Kong University Press. p141-167.

Bucci, S. (2012). Cyber Security Evangelist and Subject Matter Expert Consultant. *The Washington Post*.

CISA. (2019, April 11). *Protecting Against Malicious Code*. https://www.cisa.gov/uscert/ncas/tips/ST18-271

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*, 588-608.

Crowdstrike. (2021). *The 2021 Crowdstrike global Threat Report*. https://go.crowdstrike.com/crowdstrike global-threat-report-2021.html

Cyber Security Plan. (2020, September 14). *Spade Ransomware*. https://www.cybersecurityplan.org/spade-ransomware/+&cd=4&hl=en&ct=clnk&gl=th

DQinstitute. (2022). *Digital Citizenship*. https://www.dqinstitute.org/dq-framework

Ellul, J. (1964). *The Technological Society*. New York: A Vintage Book.

Felson, M., & Clarke, R. V. (1998). Opportunity Makes the Thief: Practical Theory for Crime Prevention. *Home Office Police Research Series*, *98*, 1-36.

Fruhwirth, C., & Mannisto, T. (2099). *"Improving CVSS-based vulnerability prioritization and response with context information"*. IEEE Computer Society Washington, DC, USA. https://ieeexplore.ieee.org/document/5314230

Giddens, A. (1996). *In Defence of Sociology; Essays, Interpretations and Rejoinders*. Cambridge: Polity Press.

Global Cyber Security Capacity Centre. (2016). *Cybersecurity Capacity Maturity Model for Nations (CMM)*. University of Oxford.

Global Cybersecurity Index. (2015). *The Global Cybersecurity Index and Cyber Wellness Profiles Report*. http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

International Telecommunication Union (ITU). (2021). *The Global Cybersecurity Index (GCI)*. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx

Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology*, *1*, 1-6.

Kabay, M. E. (2008). *A Brief History of Computer Crime: An Introduction for Students*. School of Graduate Studies: Norwich University.

Karatzogianni, A. (2009). *Cyber Conflict and Global Politics*. https://www.researchgate.net/publication/259850763_Cyber_Conflict_and_Global_Politics

Kusnadi IH., H. M. (2020). Digital Cohesion in Era of Pandemic COVID-19 in Indonesia. *International Journal of Engineering Research and Technology*, *13*, 1775-1779.

Lindau, K. (2012). *"Cyber Security in Estonia: Lessons from the Year 2007 Cyberattack"* [Master's thesis, Tallinn University].

Marion, J. B., Hill and Nancy E. . (2016). *Introduction to Cybercrime*. California: ABC – CLIO LLC.

Moonsun, C. A. (2016). Concept Analysis of Digital Citizenship for Democratic Citizenship Education in the Internet Age. *Theory & Research in Social Education*, *44*, 565-607.

News., T. (2016, February 11). *What does social networking mean?* https://www.modify.in.th/14244

Nichol, J., & Georgia, R. (2009). *Conflict in August 2008: Context and Implications for U.S. Interests*. Congressional Research Service.

NIST. (2021). *CYBERSECURITY FRAMEWORK*. https://www.nist.gov/cyberframework

Parker, D. B. (1976). *Crime by Computer*. New York: Charles Scribner's Sons.

Peiser, J. (2021, February 9). *A Hacker Broke into a Florida Town's Water Supply and Tried to Poison it with Lye, Police Said*. https://www.washingtonpost.com/nation/2021/02/09/oldsmar-water-supply-hack-florida

Phantawornchai, J. (2018). *Guidelines for Cyber Resilience Development Framework in Cloud Computing* [Thematic, Sripatum University].

Rajasekharaiah K.M, C. S. D., Sudarshan E. (2020). *Cyber Security Challenges and its Emerging Trends on Latest Technologies*. IOP Publishing.

Sakchareonkul, N. (2019). *The Preparation of Thai Public Officials for Digital Government* [Thesis, Chulalongkorn University].

Satter, R. (2017, July 7). *What makes a cyberattack? Experts lobby to restrict the term*. https://apnews.com/2c25d7da76f4409bae7daf063c071420

Swedberg, J. (2018). *"Successful Cybersecurity Strategy," Credit Union Management*. https://cumanagement.com/acgi/login?destination=/articles/2018/11/successful-cybersecurity-strategy

Teeraratchakarn, V. (2019). *Exploring Network Vulnerabilities for Corporate Security Operations* [Thesis, Chulalongkorn University].

The Institute of Internal Auditors. (2013). IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control [Brochure]. *Altamonte Springs*. Florida, USA.

TRPC. (2015). *Public data at risk: Cyber Threats to the Networked Government*. http://apps.bangkok.go.th/info_gidsedbkk/bmainfo/data_DDS/document/cyber_threats.pdf

Wall, S. (2020, August 14). *Void Crypt Ransomware Actively Spreading in the Wild*. https://securitynews.sonicwall.com/xmlpost/voidcrypt-ransomware-actively-spreading-in-the-wild

Werner, E., & Henry, S. (1995). *Criminological Theory*. Texas: Harcourt Brace College Publisher.

Whiteside, T. (1978). *Computer Capers: Tales of Electronic Thievery, Embezzlement, and Fraud Ty Crowell Co*.

Zhuang, R., Alexandru, G., Bardas, Scott A., Deloach, & Ou, X. (2015). *A Theory of Cyber Attacks Conference Paper*. https://www.researchgate.net/publication/301419837_A_Theory_of_Cyber_Attacks

ภาคผนวก

ภาคผนวก ก ใบรับรองโครงการวิจัย

คณะกรรมการพิจารณาจริยธรรมการวิจัยในคน กลุ่มสหสถาบัน ชุดที่ 2 สังคมศาสตร์ มนุษยศาสตร์ และศิลปกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
อาคารจามจุรี 1 ชั้น 1 ห้อง 114 ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน กรุงเทพมหานคร 10330
โทรศัพท์: 02-218-3210 Email: curec2.ch1@chula.ac.th

COA No. 110/66

ใบรับรองโครงการวิจัย

โครงการวิจัยที่ 660031 แนวทางการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ขององค์กรในยุคดิจิ
ผู้วิจัยหลัก นางสาว ชรินทร์ทิพย์ ปั้นสุวรรณ
หน่วยงาน คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

คณะกรรมการพิจารณาจริยธรรมการวิจัยในคน กลุ่มสหสถาบัน ชุดที่ 2 สังคมศาสตร์ มนุษยศาสตร์ และศิลปกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย พิจารณาจริยธรรมการวิจัยโดยยึดหลัก ของ Declaration of Helsinki, the Belmont report, CIOMS guidelines และ The international conference on harmonization – Good clinical practice (ICH-GCP) อนุมัติให้ดำเนินการศึกษาวิจัยเรื่องดังกล่าวได้

ลงนาม ..... **ลงนาม** .....

(รองศาสตราจารย์ ดร. นวลน้อย ตรีรัตน์) (อาจารย์ ดร. ศยามล เจริญรัตน์)

ประธานคณะกรรมการ กรรมการและเลขานุการ

รูปแบบการพิจารณาทบทวน: แบบลดขั้นตอน

วันที่รับรอง: 18 มีนาคม 2566 **วันหมดอายุ:** 17 มีนาคม 2567

เอกสารที่คณะกรรมการรับรอง

1. เอกสารข้อมูลสำหรับกลุ่มตัวอย่างผู้มีส่วนร่วมในการวิจัย
2. หนังสือยินยอมเข้าร่วมในการวิจัย
3. ประวัติผู้วิจัย (CV)
4. เครื่องมือที่ใช้ในการวิจัย

เงื่อนไข

1. ผู้วิจัยรับทราบว่าเป็นการผิดจริยธรรม หากดำเนินการเก็บข้อมูลการวิจัยก่อนได้รับการอนุมัติจากคณะกรรมการพิจารณาจริยธรรมการวิจัยฯ
2. หากใบรับรองโครงการวิจัยหมดอายุ การดำเนินการวิจัยต้องยุติ เมื่อต้องการต่ออายุต้องขออนุมัติใหม่ล่วงหน้าไม่ต่ำกว่า 1 เดือน พร้อมส่งรายงานความก้าวหน้าการวิจัย
3. ต้องดำเนินการวิจัยตามที่ระบุไว้ในโครงการวิจัยอย่างเคร่งครัด
4. ใช้เอกสารข้อมูลสำหรับกลุ่มตัวอย่าง/ผู้มีส่วนร่วมในการวิจัย ใบยินยอมของกลุ่มตัวอย่างหรือผู้มีส่วนร่วมในการวิจัย และเอกสารชี้แจงเข้าร่วมวิจัย (ถ้ามี) เฉพาะที่ประทับตราคณะกรรมการเท่านั้น
5. หากเกิดเหตุการณ์ไม่พึงประสงค์ร้ายแรงในสถานที่เก็บข้อมูลที่ขออนุมัติจากคณะกรรมการ ต้องรายงานคณะกรรมการภายใน 5 วันทำการ
6. หากมีการเปลี่ยนแปลงการดำเนินการวิจัย ให้ส่งคณะกรรมการพิจารณารับรองก่อนดำเนินการ
7. โครงการวิจัยไม่เกิน 1 ปี ส่งแบบรายงานสิ้นสุดโครงการวิจัย (AF 03-13) และบทคัดย่อผลการวิจัยภายใน 30 วัน เมื่อโครงการวิจัยเสร็จสิ้น สำหรับโครงการวิจัยที่เป็นวิทยานิพนธ์ให้ส่งบทคัดย่อผลการวิจัยภายใน 30 วัน เมื่อโครงการวิจัยเสร็จสิ้น ทั้งนี้เพื่อเป็นหลักฐานในการปิดโครงการ
8. โครงการวิจัยที่ได้รับการอนุมัติโครงการโดยการพิจารณาทบทวนแบบการเร่งรัด (Exemption review) ปฏิบัติตามเงื่อนไข ข้อ 1,6 และ 7 เท่านั้น

Digital Certificate

เลขที่โครงการวิจัย 660031
วันที่รับรอง 18 มี.ค. 2566
วันที่หมดอายุ 17 มี.ค. 2567

ภาคผนวก ข แบบสัมภาษณ์ กลุ่มที่ 1 สำหรับบุคลากรระดับบริหารและเจ้าหน้าที่เฝ้าระวังและรับมือภัยคุกคามทางไซเบอร์ หน่วยงานโครงสร้างพื้นฐานสารสนเทศด้านสาธารณสุขและสาธารณูปโภค

แบบสัมภาษณ์ กลุ่มที่ 1 สำหรับบุคลากรระดับบริหารและเจ้าหน้าที่เฝ้าระวังและรับมือภัยคุกคามทางไซเบอร์ หน่วยงานโครงสร้างพื้นฐานสารสนเทศด้านสาธารณสุขและสาธารณูปโภค

ดุษฎีนิพนธ์ เรื่อง แนวทางการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ขององค์กรในยุคดิจิทัล
(Guidelines on Corporate Governance for Responding to Cybersecurity Threats in the Digital Age)

วันที่..... เดือน..... พ.ศ. 2566 สถานที่.....

คำชี้แจง : แบบสัมภาษณ์ชุดนี้ประกอบไปด้วยคำถามทั้งหมด 4 ส่วน ดังนี้

ส่วนที่ 1 : ข้อมูลหน่วยงาน

ส่วนที่ 2 : สถานการณ์ภัยคุกคามไซเบอร์และผลกระทบต่อองค์กร

ส่วนที่ 3 : โครงสร้างการกำกับดูแลด้านเทคโนโลยีดิจิทัลขององค์กร การขับเคลื่อนการดำเนินการตามนโยบายและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ในการบริหารจัดการของภาครัฐ

ส่วนที่ 4 : แนวทางการเตรียมแผนการรับมือและป้องกันภัยคุกคามความมั่นคงปลอดภัยไซเบอร์และการกำกับดูแลการบริหารจัดการที่ดีด้านเทคโนโลยีดิจิทัลในองค์กร

คำอธิบาย :

การกำกับดูแลองค์กร (Corporate Governance) หมายถึง การบริหารจัดการองค์กร การกำกับ การติดตาม การควบคุม และการดูแล ผู้ที่ได้รับมอบหมายอำนาจหน้าที่ให้ไปทำหน้าที่ทางการบริหาร เพื่อให้ทรัพยากรขององค์กรได้นำไปใช้อย่างมีประสิทธิภาพ ประสิทธิผล ตรงตามเป้าหมายอย่างคุ้มค่า โปร่งใส ตรวจสอบได้ ทั้งนี้เพื่อให้เกิดประโยชน์สูงสุดแก่ผู้มีส่วนได้ส่วนเสียทุกฝ่ายอย่างเป็นธรรม

ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) หมายถึง กระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อให้องค์กรปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบทั้งทางอิเล็กทรอนิกส์และทางกายภาพ ความปลอดภัยของระบบและเครือข่ายที่ใช้ในการเก็บ เข้าถึง

ประมวล และกระจายข้อมูล ทั้งนี้รวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม และความผิดต่างๆ

การรับมือ (Coping) หมายถึง จัดการ ต้านทาน กำราบ และเป็นการจัดเป็นลำดับขั้นตอนโดยแยกแยะหมวดหมู่มักจะทำแบบเป็นคู่ ๆ เช่น มีปัญหาเป็นศูนย์ หรือมีอารมณ์เป็นศูนย์ สู้หรือหนี โดยการรู้คิดหรือโดยพฤติกรรม

ส่วนที่ 1 ข้อมูลหน่วยงาน

1.1 ชื่อหน่วยงาน/ข้อมูลทั่วไป.....

1.2 ท่านมีประสบการณ์การทำงานที่เกี่ยวข้องกับด้านการกำกับดูแล ป้องกัน รับมือ และเฝ้าระวังภัยคุกคามทางไซเบอร์อย่างไร

.....

.....

ส่วนที่ 2 สถานการณ์ภัยคุกคามทางไซเบอร์และผลกระทบต่อองค์กร

2.1 องค์กรของท่านเคยประสบกับปัญหาสถานการณ์ภัยคุกคามทางไซเบอร์รูปแบบใดบ้าง และมีลักษณะอย่างไร

.....

.....

2.2 จากสถานการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศที่สำคัญในประเทศไทยด้านสาธารณสุขและด้านสาธารณูปโภค เช่น ภัยคุกคามจากการเจาะระบบฐานข้อมูล เป็นต้น ส่งผลกระทบต่อองค์กรท่านอย่างไร

2.2.1 ด้านระบบสารสนเทศและเครือข่าย

.....

.....

2.2.2 ด้านข้อมูลสารสนเทศ

.....

.....

2.2.3 ด้านการให้บริการ

.....

.....

2.2.4 ด้านความมั่นคงปลอดภัย

.....

.....

2.2.5 ด้านการกำกับดูแล

.....

.....

2.2.6 ด้านอื่นๆ

.....

.....

2.2.7 ระดับความรุนแรงของสถานการณ์ภัยคุกคามทางไซเบอร์

.....

.....

ส่วนที่ 3 : โครงสร้างการกำกับดูแลด้านเทคโนโลยีดิจิทัลขององค์กร การขับเคลื่อนการดำเนินการตามนโยบายและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ในการบริหารจัดการของภาครัฐ

3.1 โครงสร้างการกำกับดูแลด้านเทคโนโลยีดิจิทัลขององค์กร มีหน่วยงานที่เกี่ยวข้องด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และมีบทบาทหน้าที่การกำกับดูแลอย่างไร

3.1.1 ด้านกฎหมาย

.....

.....

.....

3.1.2 ด้านเทคโนโลยี

.....

.....

.....

3.1.3 ด้านการประสานงานระหว่างหน่วยงานในประเทศหรือต่างประเทศ

.....

.....

.....

3.2 มาตรการต่างๆ เช่น นโยบาย กฎหมาย แผนปฏิบัติการ ระเบียบ ข้อบังคับ ของภาครัฐ สอดคล้องกับการแก้ไขสถานการณ์ภัยคุกคามทางไซเบอร์ขององค์กรอย่างไร

.....

.....

3.3 การปฏิบัติงานตามนโยบายและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ มีขั้นตอนและองค์ประกอบอย่างไรเพื่อให้เป็นไปตามกฎเกณฑ์ในการบริหารจัดการของภาครัฐ

.....

.....

ส่วนที่ 4 : แนวทางการเตรียมแผนการรับมือและป้องกันภัยคุกคามความมั่นคงปลอดภัยไซเบอร์และการกำกับดูแลการบริหารจัดการที่ดีด้านเทคโนโลยีดิจิทัลในองค์กร

4.1 ท่านประสบปัญหาและอุปสรรคในการป้องกันภัยคุกคามความมั่นคงปลอดภัยไซเบอร์หรือไม่ อย่างไร

.....

.....

4.2 มีแนวทางอย่างไรในการกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัลขององค์กร เช่น นโยบาย แผนยุทธศาสตร์ มาตรการต่างๆ

.....

.....

4.3 มีแนวทางอย่างไรการบริหารจัดการความเสี่ยงด้านเทคโนโลยีดิจิทัล เช่น การตรวจสอบช่องโหว่ วิเคราะห์และประเมินความเสี่ยงหรือโอกาสที่จะเกิดปัญหาภัยคุกคามทางไซเบอร์

.....

.....

4.4 การให้ความร่วมมือและการประสานงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศระหว่างหน่วยงานภาครัฐมีวิธีการอย่างไร และมีประสิทธิภาพมากน้อยอย่างไร

.....

.....

4.5 มีการนำกรอบการดำเนินงานตามมาตรฐานสากลและการนำเทคโนโลยีดิจิทัล เช่น การจัดตั้งศูนย์ปฏิบัติการไซเบอร์เฝ้าระวังและตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ มาใช้ในการรับมือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์อย่างไร

.....

.....

4.6 มีแผนการปฏิบัติการขององค์กรที่มีความสอดคล้องกับ กฎหมาย ระเบียบ ข้อบังคับและมาตรฐานต่างๆ ที่เกี่ยวข้องกับการพัฒนาเทคโนโลยีดิจิทัล เช่น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เป็นต้น โดยแสดงให้เห็นถึงแผนงาน/โครงการที่ชัดเจนเป็นรูปธรรมอย่างไร

.....

.....

4.7 มีการจัดทำแผนปฏิบัติงาน คู่มือ แนวทางการรับมือภัยคุกคามทางไซเบอร์ขององค์กรอย่างไร และมีการถ่ายทอดสื่อสารกระบวนการบริหารจัดการความมั่งคงปลอดภัยด้านเทคโนโลยีดิจิทัลแก่ผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างไร

.....

.....

4.8 มีการกำหนดตัวชี้วัดในการติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (outcome) ของกระบวนการจัดทำแผนปฏิบัติการดิจิทัลและแผนปฏิบัติการประจำปีขององค์กรในการรับมือภัยคุกคามทางไซเบอร์หรือไม่ อย่างไร

.....

.....

4.9 มีการสร้างความตระหนักรู้ด้านการเฝ้าระวังภัยคุกคามทางไซเบอร์และวิธีการรับมือ ป้องกัน แก้ไข ให้กับบุคลากรในองค์กรอย่างไร

.....

.....

4.10 ท่านมีข้อเสนอแนะเชิงนโยบายและเชิงปฏิบัติการอย่างไรต่อการเตรียมความพร้อมในการรับมือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์

.....

.....

เลขที่โครงการวิจัย 660031
วันที่รับรอง 18 มี.ค. 2566
วันที่หมดอายุ 17 มี.ค. 2567

ภาคผนวก ค แบบสัมภาษณ์ กลุ่มที่ 2 สำหรับบุคลากรระดับบริหารกำหนดนโยบายและยุทธศาสตร์ ด้านการกำกับดูแลเทคโนโลยีดิจิทัลและความมั่นคงปลอดภัยทางไซเบอร์

แบบสัมภาษณ์ กลุ่มที่ 2 สำหรับบุคลากรระดับบริหารกำหนดนโยบายและยุทธศาสตร์

ด้านการกำกับดูแลเทคโนโลยีดิจิทัลและความมั่นคงปลอดภัยทางไซเบอร์

ดุษฎีนิพนธ์ เรื่อง แนวทางการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ขององค์กรในยุคดิจิทัล

(Guidelines on Corporate Governance for Responding to Cybersecurity Threats

in the Digital Age)

วันที่..... เดือน..... พ.ศ. 2566 สถานที่.....

คำชี้แจง : แบบสัมภาษณ์ชุดนี้ประกอบไปด้วยคำถามทั้งหมด 4 ส่วน ดังนี้

ส่วนที่ 1 : ข้อมูลหน่วยงาน

ส่วนที่ 2 : สถานการณ์ภัยคุกคามไซเบอร์และผลกระทบต่อองค์กร

ส่วนที่ 3 : โครงสร้างการกำกับดูแลด้านเทคโนโลยีดิจิทัลขององค์กร การขับเคลื่อนการดำเนินการตามนโยบายและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ในการบริหารจัดการของภาครัฐ

ส่วนที่ 4 : แนวทางการเตรียมแผนการรับมือและป้องกันภัยคุกคามความมั่นคงปลอดภัยไซเบอร์และการกำกับดูแลการบริหารจัดการที่ดีด้านเทคโนโลยีดิจิทัลในองค์กร

คำอธิบาย :

การกำกับดูแลองค์กร (Corporate Governance) หมายถึง การบริหารจัดการองค์กร การกำกับ การติดตาม การควบคุม และการดูแล ผู้ที่ได้รับมอบหมายอำนาจหน้าที่ให้ไปทำหน้าที่ทางการบริหาร เพื่อให้ทรัพยากรขององค์กรได้นำไปใช้อย่างมีประสิทธิภาพ ประสิทธิผล ตรงตามเป้าหมายอย่างคุ้มค่า โปร่งใส ตรวจสอบได้ ทั้งนี้เพื่อให้เกิดประโยชน์สูงสุดแก่ผู้มีส่วนได้ส่วนเสียทุกฝ่ายอย่างเป็นธรรม

ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) หมายถึง กระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อให้องค์กรปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบทั้งทางอิเล็กทรอนิกส์และทางกายภาพ ความปลอดภัยของระบบและเครือข่ายที่ใช้ในการเข้าถึง

ประมวล และกระจายข้อมูล ทั้งนี้รวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม และความผิดต่างๆ

การรับมือ (Coping) หมายถึง จัดการ ต้านทาน กำราบ และเป็นการจัดเป็นลำดับขั้นตอนโดยแยกแยะหมวดหมู่มักจะทำแบบเป็นคู่ ๆ เช่น มีปัญหาเป็นศูนย์ หรือมีอารมณ์เป็นศูนย์ สู้หรือหนี โดยการรู้คิดหรือโดยพฤติกรรม

ส่วนที่ 1 ข้อมูลหน่วยงาน

1.1 ชื่อหน่วยงาน/ข้อมูลทั่วไป.....

1.2 ท่านมีประสบการณ์การทำงานที่เกี่ยวข้องกับด้านการกำกับดูแล ป้องกัน รับมือ และเฝ้าระวังภัยคุกคามทางไซเบอร์อย่างไร

.....

.....

ส่วนที่ 2 สถานการณ์ภัยคุกคามทางไซเบอร์และผลกระทบต่อองค์กร

2.1 องค์กรของท่านเคยประสบกับปัญหาสถานการณ์ภัยคุกคามทางไซเบอร์รูปแบบใดบ้าง และมีลักษณะอย่างไร

.....

.....

2.2 จากสถานการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศที่สำคัญในประเทศไทยด้านสาธารณสุขและด้านสาธารณูปโภค เช่น ภัยคุกคามจากการเจาะระบบฐานข้อมูล เป็นต้น ส่งผลกระทบต่อองค์กรท่านอย่างไร

2.2.1 ด้านระบบสารสนเทศและเครือข่าย

.....

.....

2.2.2 ด้านข้อมูลสารสนเทศ

.....

.....

2.2.3 ด้านการให้บริการ

.....

.....

2.2.4 ด้านความมั่นคงปลอดภัย

.....

.....

2.2.5 ด้านการกำกับดูแล

.....

.....

2.2.6 ด้านอื่นๆ

.....

.....

2.2.7 ระดับความรุนแรงของสถานการณ์ภัยคุกคามทางไซเบอร์

.....

.....

ส่วนที่ 3 : โครงสร้างการกำกับดูแลด้านเทคโนโลยีดิจิทัลขององค์กร การขับเคลื่อนการดำเนินการตามนโยบายและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ในการบริหารจัดการของภาครัฐ

3.1 โครงสร้างการกำกับดูแลด้านเทคโนโลยีดิจิทัลขององค์กร มีหน่วยงานที่เกี่ยวข้องด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และมีบทบาทหน้าที่การกำกับดูแลอย่างไร

3.1.1 ด้านกฎหมาย

.....

.....

.....

3.1.2 ด้านเทคโนโลยี

.....

.....

.....

3.1.3 ด้านการประสานงานระหว่างหน่วยงานในประเทศหรือต่างประเทศ

.....

.....

.....

3.2 มาตรการต่างๆ เช่น นโยบาย กฎหมาย แผนปฏิบัติการ ระเบียบ ข้อบังคับ ของภาครัฐ สอดคล้องกับการแก้ไขสถานการณ์ภัยคุกคามทางไซเบอร์ขององค์กรอย่างไร

.....

.....

3.3 การปฏิบัติงานตามนโยบายและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ มีขั้นตอนและองค์ประกอบอย่างไรเพื่อให้เป็นไปตามกฎเกณฑ์ในการบริหารจัดการของภาครัฐ

.....

.....

ส่วนที่ 4 : แนวทางการเตรียมแผนการรับมือและป้องกันภัยคุกคามความมั่นคงปลอดภัยไซเบอร์และการกำกับดูแลการบริหารจัดการที่ดีด้านเทคโนโลยีดิจิทัลในองค์กร

4.1 ท่านประสบปัญหาและอุปสรรคในการป้องกันภัยคุกคามความมั่นคงปลอดภัยไซเบอร์หรือไม่ อย่างไร

.....

.....

4.2 มีแนวทางอย่างไรในการกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัลขององค์กร เช่น นโยบาย แผนยุทธศาสตร์ มาตรการต่างๆ

.....

.....

4.3 มีแนวทางอย่างไรการบริหารจัดการความเสี่ยงด้านเทคโนโลยีดิจิทัล เช่น การตรวจสอบช่องโหว่ วิเคราะห์และประเมินความเสี่ยงหรือโอกาสที่จะเกิดปัญหาภัยคุกคามทางไซเบอร์

.....

.....

4.4 การให้ความร่วมมือและการประสานงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศระหว่างหน่วยงานภาครัฐมีวิธีการอย่างไร และมีประสิทธิภาพมากน้อยอย่างไร

.....

.....

4.5 มีการนำกรอบการดำเนินงานตามมาตรฐานสากลและการนำเทคโนโลยีดิจิทัล เช่น การจัดตั้งศูนย์ปฏิบัติการไซเบอร์เฝ้าระวังและตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ มาใช้ในการรับมือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์อย่างไร

.....

.....

4.6 มีแผนการปฏิบัติการขององค์กรที่มีความสอดคล้องกับ กฎหมาย ระเบียบ ข้อบังคับและมาตรฐานต่างๆ ที่เกี่ยวข้องกับการพัฒนาเทคโนโลยีดิจิทัล เช่น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เป็นต้น โดยแสดงให้เห็นถึงแผนงาน/โครงการที่ชัดเจนเป็นรูปธรรมอย่างไร

.....

.....

4.7 มีการจัดทำแผนปฏิบัติงาน คู่มือ แนวทางการรับมือภัยคุกคามทางไซเบอร์ขององค์กรอย่างไร และมีการถ่ายทอดสื่อสารกระบวนการบริหารจัดการความมั่งคงปลอดภัยด้านเทคโนโลยีดิจิทัลแก่ผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างไร

.....

.....

4.8 มีการกำหนดตัวชี้วัดในการติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (outcome) ของกระบวนการจัดทำแผนปฏิบัติการดิจิทัลและแผนปฏิบัติการประจำปีขององค์กรในการรับมือภัยคุกคามทางไซเบอร์หรือไม่ อย่างไร

.....

.....

4.9 มีการสร้างความตระหนักรู้ด้านการเฝ้าระวังภัยคุกคามทางไซเบอร์และวิธีการรับมือ ป้องกัน แก้ไข ให้กับบุคลากรในองค์กรอย่างไร

.....

.....

4.10 ท่านมีข้อเสนอแนะเชิงนโยบายและเชิงปฏิบัติการอย่างไรต่อการเตรียมความพร้อมในการรับมือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์

.....

.....

เลขที่โครงการวิจัย 660031
วันที่รับรอง 18 มี.ค. 2566
วันที่หมดอายุ 17 มี.ค. 2567

ภาคผนวก ง แบบสัมภาษณ์ กลุ่มที่ 3 สำหรับบุคลากรระดับบริหารด้านกระบวนการยุติธรรม

แบบสัมภาษณ์ กลุ่มที่ 3 สำหรับบุคลากรระดับบริหารด้านกระบวนการยุติธรรม

ดุษฎีนิพนธ์ เรื่อง แนวทางการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ขององค์กรในยุคดิจิทัล

(Guidelines on Corporate Governance for Responding to Cybersecurity Threats in the Digital Age)

วันที่..... เดือน..... พ.ศ. 2566 สถานที่.....

คำชี้แจง : แบบสัมภาษณ์ชุดนี้ประกอบไปด้วยคำถามทั้งหมด 4 ส่วน ดังนี้

ส่วนที่ 1 : ข้อมูลหน่วยงาน

ส่วนที่ 2 : สถานการณ์ภัยคุกคามไซเบอร์และผลกระทบต่อองค์กร

ส่วนที่ 3 : โครงสร้างการกำกับดูแลด้านเทคโนโลยีดิจิทัลขององค์กร การขับเคลื่อนการดำเนินการตามนโยบายและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ในการบริหารจัดการของภาครัฐ

ส่วนที่ 4 : แนวทางการเตรียมแผนการรับมือและป้องกันภัยคุกคามความมั่นคงปลอดภัยไซเบอร์และการกำกับดูลการบริหารจัดการที่ดีด้านเทคโนโลยีดิจิทัลในองค์กร

คำอธิบาย :

การกำกับดูแลองค์กร (Corporate Governance) หมายถึง การบริหารจัดการองค์กร การกำกับ การติดตาม การควบคุม และการดูแล ผู้ที่ได้รับมอบหมายอำนาจหน้าที่ให้ไปทำหน้าที่ทางการบริหาร เพื่อให้ทรัพยากรขององค์กรได้นำไปใช้อย่างมีประสิทธิภาพ ประสิทธิผล ตรงตามเป้าหมายอย่างคุ้มค่า โปร่งใส ตรวจสอบได้ ทั้งนี้เพื่อให้เกิดประโยชน์สูงสุดแก่ผู้มีส่วนได้ส่วนเสียทุกฝ่ายอย่างเป็นธรรม

ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) หมายถึง กระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อให้องค์กรปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบทั้งทางอิเล็กทรอนิกส์และทางกายภาพ ความปลอดภัยของระบบและเครือข่ายที่ใช้ในการเก็บ เข้าถึง

ประมวล และกระจายข้อมูล ทั้งนี้รวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม และความผิดต่างๆ

การรับมือ (Coping) หมายถึง จัดการ ต้านทาน กำราบ และเป็นการจัดเป็นลำดับขั้นตอนโดยแยกแยะหมวดหมู่มักจะทำแบบเป็นคู่ ๆ เช่น มีปัญหาเป็นศูนย์ หรือมีอารมณ์เป็นศูนย์ สู้หรือหนี โดยการรู้คิดหรือโดยพฤติกรรม

ส่วนที่ 1 ข้อมูลหน่วยงาน

1.1 ชื่อหน่วยงาน/ข้อมูลทั่วไป.....

1.2 ท่านมีประสบการณ์การทำงานที่เกี่ยวข้องกับด้านการกำกับดูแล ป้องกัน รับมือ และเฝ้าระวังภัยคุกคามทางไซเบอร์อย่างไร

.....

.....

ส่วนที่ 2 สถานการณ์ภัยคุกคามทางไซเบอร์และผลกระทบต่อองค์กร

2.1 องค์กรของท่านเคยประสบกับปัญหาสถานการณ์ภัยคุกคามทางไซเบอร์รูปแบบใดบ้าง และมีลักษณะอย่างไร

.....

.....

2.2 จากสถานการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศที่สำคัญในประเทศไทยด้านสาธารณสุขและด้านสาธารณูปโภค เช่น ภัยคุกคามจากการเจาะระบบฐานข้อมูล เป็นต้น ส่งผลกระทบต่อองค์กรท่านอย่างไร

2.2.1 ด้านระบบสารสนเทศและเครือข่าย

.....

.....

2.2.2 ด้านข้อมูลสารสนเทศ

.....

.....

2.2.3 ด้านการให้บริการ

.....

.....

2.2.4 ด้านความมั่นคงปลอดภัย

.....

.....

2.2.5 ด้านการกำกับดูแล

.....

.....

2.2.6 ด้านอื่นๆ

.....

.....

2.2.7 ระดับความรุนแรงของสถานการณ์ภัยคุกคามทางไซเบอร์

.....

.....

ส่วนที่ 3 : โครงสร้างการกำกับดูแลด้านเทคโนโลยีดิจิทัลขององค์กร การขับเคลื่อนการดำเนินการตามนโยบายและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ในการบริหารจัดการของภาครัฐ

3.1 โครงสร้างการกำกับดูแลด้านเทคโนโลยีดิจิทัลขององค์กร มีหน่วยงานที่เกี่ยวข้องด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และมีบทบาทหน้าที่การกำกับดูแลอย่างไร

3.1.1 ด้านกฎหมาย

.....

.....

.....

3.1.2 ด้านเทคโนโลยี

.....

.....

.....

3.1.3 ด้านการประสานงานระหว่างหน่วยงานในประเทศหรือต่างประเทศ

.....

.....

.....

3.2 มาตรการต่างๆ เช่น นโยบาย กฎหมาย แผนปฏิบัติการ ระเบียบ ข้อบังคับ ของภาครัฐ สอดคล้องกับการแก้ไขสถานการณ์ภัยคุกคามทางไซเบอร์ขององค์กรอย่างไร

.....

.....

3.3 การปฏิบัติงานตามนโยบายและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ มีขั้นตอนและองค์ประกอบอย่างไรเพื่อให้เป็นไปตามกฎเกณฑ์ในการบริหารจัดการของภาครัฐ

.....

.....

ส่วนที่ 4 : แนวทางการเตรียมแผนการรับมือและป้องกันภัยคุกคามความมั่นคงปลอดภัยไซเบอร์และการกำกับดูแลการบริหารจัดการที่ดีด้านเทคโนโลยีดิจิทัลในองค์กร

4.1 ท่านประสบปัญหาและอุปสรรคในการป้องกันภัยคุกคามความมั่นคงปลอดภัยไซเบอร์หรือไม่ อย่างไร

.....

.....

4.2 มีแนวทางอย่างไรในการกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัลขององค์กร เช่น นโยบาย แผนยุทธศาสตร์ มาตรการต่างๆ

.....

.....

4.3 มีแนวทางอย่างไรการบริหารจัดการความเสี่ยงด้านเทคโนโลยีดิจิทัล เช่น การตรวจสอบช่องโหว่ วิเคราะห์และประเมินความเสี่ยงหรือโอกาสที่จะเกิดปัญหาภัยคุกคามทางไซเบอร์

.....

.....

4.4 การให้ความร่วมมือและการประสานงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศระหว่างหน่วยงานภาครัฐมีวิธีการอย่างไร และมีประสิทธิภาพมากน้อยอย่างไร

.....

.....

4.5 มีการนำกรอบการดำเนินงานตามมาตรฐานสากลและการนำเทคโนโลยีดิจิทัล เช่น การจัดตั้งศูนย์ปฏิบัติการไซเบอร์เฝ้าระวังและตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ มาใช้ในการรับมือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์อย่างไร

.....

.....

4.6 มีแผนการปฏิบัติการขององค์กรที่มีความสอดคล้องกับ กฎหมาย ระเบียบ ข้อบังคับและมาตรฐานต่างๆ ที่เกี่ยวข้องกับการพัฒนาเทคโนโลยีดิจิทัล เช่น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เป็นต้น โดยแสดงให้เห็นถึงแผนงาน/โครงการที่ชัดเจนเป็นรูปธรรมอย่างไร

.....

.....

4.7 มีการจัดทำแผนปฏิบัติงาน คู่มือ แนวทางการรับมือภัยคุกคามทางไซเบอร์ขององค์กรอย่างไร และมีการถ่ายทอดสื่อสารกระบวนการบริหารจัดการความมั่งคงปลอดภัยด้านเทคโนโลยีดิจิทัลแก่ผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างไร

.....

.....

4.8 มีการกำหนดตัวชี้วัดในการติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (outcome) ของกระบวนการจัดทำแผนปฏิบัติการดิจิทัลและแผนปฏิบัติการประจำปีขององค์กรในการรับมือภัยคุกคามทางไซเบอร์หรือไม่ อย่างไร

.....

.....

4.9 มีการสร้างความตระหนักรู้ด้านการเฝ้าระวังภัยคุกคามทางไซเบอร์และวิธีการรับมือ ป้องกัน แก้ไข ให้กับบุคลากรในองค์กรอย่างไร

.....

.....

4.10 ท่านมีข้อเสนอแนะเชิงนโยบายและเชิงปฏิบัติการอย่างไรต่อการเตรียมความพร้อมในการรับมือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์

.....

.....

เลขที่โครงการวิจัย 660031
วันที่รับรอง 18 มี.ค. 2566
วันที่หมดอายุ 17 มี.ค. 2567

ภาคผนวก จ แบบสัมภาษณ์ กลุ่มที่ 4 สำหรับผู้ทรงคุณวุฒิ นักวิชาการและผู้เชี่ยวชาญ

แบบสัมภาษณ์ กลุ่มที่ 4 ผู้ทรงคุณวุฒิ นักวิชาการและผู้เชี่ยวชาญ

ดุษฎีนิพนธ์ เรื่อง แนวทางการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ขององค์กรในยุคดิจิทัล

(Guidelines on Corporate Governance for Responding to Cybersecurity Threats in the Digital Age)

วันที่..... เดือน..... พ.ศ. 2566 สถานที่.....

คำชี้แจง : แบบสัมภาษณ์ชุดนี้ประกอบไปด้วยคำถามทั้งหมด 4 ส่วน ดังนี้

ส่วนที่ 1 : ข้อมูลหน่วยงาน

ส่วนที่ 2 : สถานการณ์ภัยคุกคามไซเบอร์และผลกระทบต่อองค์กร

ส่วนที่ 3 : โครงสร้างการกำกับดูแลด้านเทคโนโลยีดิจิทัลขององค์กร การขับเคลื่อนการดำเนินการตามนโยบายและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ในการบริหารจัดการของภาครัฐ

ส่วนที่ 4 : แนวทางการเตรียมแผนการรับมือและป้องกันภัยคุกคามความมั่นคงปลอดภัยไซเบอร์และการกำกับดูแลการบริหารจัดการที่ดีด้านเทคโนโลยีดิจิทัลในองค์กร

คำอธิบาย :

การกำกับดูแลองค์กร (Corporate Governance) หมายถึง การบริหารจัดการองค์กร การกำกับ การติดตาม การควบคุม และการดูแล ผู้ที่ได้รับมอบหมายอำนาจหน้าที่ให้ไปทำหน้าที่ทางการบริหาร เพื่อให้ทรัพยากรขององค์กรได้นำไปใช้อย่างมีประสิทธิภาพ ประสิทธิผล ตรงตามเป้าหมายอย่างคุ้มค่า โปร่งใส ตรวจสอบได้ ทั้งนี้เพื่อให้เกิดประโยชน์สูงสุดแก่ผู้มีส่วนได้ส่วนเสียทุกฝ่ายอย่างเป็นธรรม

ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) หมายถึง กระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อให้องค์กรปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบทั้งทางอิเล็กทรอนิกส์และทางกายภาพ ความปลอดภัยของระบบและเครือข่ายที่ใช้ในการเก็บ เข้าถึง

ประมวล และกระจายข้อมูล ทั้งนี้รวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม และความผิดต่างๆ

การรับมือ (Coping) หมายถึง จัดการ ต้านทาน กำราบ และเป็นการจัดเป็นลำดับขั้นตอนโดยแยกแยะหมวดหมู่มักจะทำแบบเป็นคู่ ๆ เช่น มีปัญหาเป็นศูนย์ หรือมีอารมณ์เป็นศูนย์ สู้หรือหนี โดยการรู้คิดหรือโดยพฤติกรรม

ส่วนที่ 1 ข้อมูลหน่วยงาน

1.1 ชื่อหน่วยงาน/ข้อมูลทั่วไป.....

1.2 ท่านมีประสบการณ์การทำงานที่เกี่ยวข้องกับด้านการกำกับดูแล ป้องกัน รับมือ และเฝ้าระวังภัยคุกคามทางไซเบอร์อย่างไร

.....

.....

ส่วนที่ 2 สถานการณ์ภัยคุกคามทางไซเบอร์และผลกระทบต่อองค์กร

2.1 องค์กรของท่านเคยประสบกับปัญหาสถานการณ์ภัยคุกคามทางไซเบอร์รูปแบบใดบ้าง และมีลักษณะอย่างไร

.....

.....

2.2 จากสถานการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศที่สำคัญในประเทศไทยด้านสาธารณสุขและด้านสาธารณูปโภค เช่น ภัยคุกคามจากการเจาะระบบฐานข้อมูล เป็นต้น ส่งผลกระทบต่อองค์กรท่านอย่างไร

2.2.1 ด้านระบบสารสนเทศและเครือข่าย

.....

.....

2.2.2 ด้านข้อมูลสารสนเทศ

.....

.....

2.2.3 ด้านการให้บริการ

.....

.....

2.2.4 ด้านความมั่นคงปลอดภัย

.....

.....

2.2.5 ด้านการกำกับดูแล

.....

.....

2.2.6 ด้านอื่นๆ

.....

.....

2.2.7 ระดับความรุนแรงของสถานการณ์ภัยคุกคามทางไซเบอร์

.....

.....

ส่วนที่ 3 : โครงสร้างการกำกับดูแลด้านเทคโนโลยีดิจิทัลขององค์กร การขับเคลื่อนการดำเนินการตามนโยบายและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ในการบริหารจัดการของภาครัฐ

3.1 โครงสร้างการกำกับดูแลด้านเทคโนโลยีดิจิทัลขององค์กร มีหน่วยงานที่เกี่ยวข้องด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และมีบทบาทหน้าที่การกำกับดูแลอย่างไร

3.1.1 ด้านกฎหมาย

.....

.....

.....

3.1.2 ด้านเทคโนโลยี

.....

.....

.....

3.1.3 ด้านการประสานงานระหว่างหน่วยงานในประเทศหรือต่างประเทศ

.....

.....

.....

3.2 มาตรการต่างๆ เช่น นโยบาย กฎหมาย แผนปฏิบัติการ ระเบียบ ข้อบังคับ ของภาครัฐ สอดคล้องกับการแก้ไขสถานการณ์ภัยคุกคามทางไซเบอร์ขององค์กรอย่างไร

.....

.....

3.3 การปฏิบัติงานตามนโยบายและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ มีขั้นตอนและองค์ประกอบอย่างไรเพื่อให้เป็นไปตามกฎเกณฑ์ในการบริหารจัดการของภาครัฐ

.....

.....

ส่วนที่ 4 : แนวทางการเตรียมแผนการรับมือและป้องกันภัยคุกคามความมั่นคงปลอดภัยไซเบอร์และการกำกับดูแลการบริหารจัดการที่ดีด้านเทคโนโลยีดิจิทัลในองค์กร

4.1 ท่านประสบปัญหาและอุปสรรคในการป้องกันภัยคุกคามความมั่นคงปลอดภัยไซเบอร์หรือไม่ อย่างไร

.....

.....

4.2 มีแนวทางอย่างไรในการกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัลขององค์กร เช่น นโยบาย แผนยุทธศาสตร์ มาตรการต่างๆ

.....

.....

4.3 มีแนวทางอย่างไรการบริหารจัดการความเสี่ยงด้านเทคโนโลยีดิจิทัล เช่น การตรวจสอบช่องโหว่ วิเคราะห์และประเมินความเสี่ยงหรือโอกาสที่จะเกิดปัญหาภัยคุกคามทางไซเบอร์

.....

.....

4.4 การให้ความร่วมมือและการประสานงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศระหว่างหน่วยงานภาครัฐมีวิธีการอย่างไร และมีประสิทธิภาพมากน้อยอย่างไร

.....

.....

4.5 มีการนำกรอบการดำเนินงานตามมาตรฐานสากลและการนำเทคโนโลยีดิจิทัล เช่น การจัดตั้งศูนย์ปฏิบัติการไซเบอร์เฝ้าระวังและตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ มาใช้ในการรับมือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์อย่างไร

.....

.....

4.6 มีแผนการปฏิบัติการขององค์กรที่มีความสอดคล้องกับ กฎหมาย ระเบียบ ข้อบังคับและมาตรฐานต่างๆ ที่เกี่ยวข้องกับการพัฒนาเทคโนโลยีดิจิทัล เช่น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เป็นต้น โดยแสดงให้เห็นถึงแผนงาน/โครงการที่ชัดเจนเป็นรูปธรรมอย่างไร

.....

.....

4.7 มีการจัดทำแผนปฏิบัติงาน คู่มือ แนวทางการรับมือภัยคุกคามทางไซเบอร์ขององค์กรอย่างไร และมีการถ่ายทอดสื่อสารกระบวนการบริหารจัดการความมั่งคงปลอดภัยด้านเทคโนโลยีดิจิทัลแก่ผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างไร

.....

.....

4.8 มีการกำหนดตัวชี้วัดในการติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (outcome) ของกระบวนการจัดทำแผนปฏิบัติการดิจิทัลและแผนปฏิบัติการประจำปีขององค์กรในการรับมือภัยคุกคามทางไซเบอร์หรือไม่ อย่างไร

.....

.....

4.9 มีการสร้างความตระหนักรู้ด้านการเฝ้าระวังภัยคุกคามทางไซเบอร์และวิธีการรับมือ ป้องกัน แก้ไข ให้กับบุคลากรในองค์กรอย่างไร

.....

.....

4.10 ท่านมีข้อเสนอแนะเชิงนโยบายและเชิงปฏิบัติการอย่างไรต่อการเตรียมความพร้อมในการรับมือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์

.....

.....

เลขที่โครงการวิจัย 660031
วันที่รับรอง 18 มี.ค. 2566
วันที่หมดอายุ 17 มี.ค. 2567

ประวัติผู้เขียน

ชื่อ-สกุล	นางสาวชรินทร์ทิพย์ ปั้นสุวรรณ
วัน เดือน ปี เกิด	26 มีนาคม 2527
สถานที่เกิด	นครศรีธรรมราช
วุฒิการศึกษา	พ.ศ. 2549 มหาวิทยาลัยราชภัฏพระนคร พ.ศ. 2558 Brunel University London
ที่อยู่ปัจจุบัน	82/100 เฟส 8 ซอย 2/1 หมู่ 6 หมู่บ้านฟ้าปิยรมย์ ถนนลำลูกกา ตำบลบึงคำพร้อย อำเภอลำลูกกา จังหวัดปทุมธานี 12150
รางวัลที่ได้รับ	Computer Science with Merit (เกียรตินิยมอันดับ 2) Brunel University London