การศึกษามาตรการความมั่นคงปลอดภัยทางไซเบอร์ต่อสถาบันการเงิน

พ.จ.อ.ปรมัตถ์ ไวรักษ์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาศิลปศาสตรมหาบัณฑิต
สาขาวิชาอาชญาวิทยาและงานยุติธรรม ภาควิชาสังคมวิทยาและมานุษยวิทยา
คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2562

A STUDY OF CYBERSECURITY MEASURES IN FINANCIAL INSTITUTIONS

Cpo.1 Poramat Viruk

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Arts in Criminology and Criminal Justice
Department of Sociology and Anthropology
FACULTY OF POLITICAL SCIENCE
Chulalongkorn University
Academic Year 2019

หัวข้อวิทยานิพนธ์	การศึกษามาตรการความมั่นคงปลอดภัยทางไซเบอร์ต่อสถาบันการเงิน
โดย	พ.จ.อ.ปรมัตถ์ ไวรักษ์
สาขาวิชา	อาชญาวิทยาและงานยุติธรรม
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	รองศาสตราจารย์ ดร.สุมนทิพย์ จิตสว่าง

คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาศิลปศาสตรมหาบัณฑิต

..... คณบดีคณะรัฐศาสตร์
(รองศาสตราจารย์ ดร.เอก ตั้งทรัพย์วัฒนา)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(รองศาสตราจารย์ ดร.จุฑารัตน์ เอื้ออำนวย)

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

..... กรรมการภายนอกมหาวิทยาลัย
(ดร.กฤษฎิ์ เดชารักษ์)

ปรมัตถ์ ไวรักษ์ : การศึกษามาตรการความมั่นคงปลอดภัยทางไซเบอร์ต่อสถาบันการเงิน. (A STUDY OF CYBERSECURITY MEASURES IN FINANCIAL INSTITUTIONS) อ.ที่ปรึกษาหลัก : รศ. ดร.สุมนทิพย์ จิตสว่าง

วิทยานิพนธ์นี้มีวัตถุประสงค์เพื่อศึกษาบทบาทของธนาคารกลางของไทยในการกำกับดูแลสถาบันการเงินต่อการบังคับใช้มาตรการความมั่นคงปลอดภัยไซเบอร์และศึกษาถึงแนวทางการสร้างความร่วมมือระหว่างกลุ่มสถาบันการเงิน โดยใช้รูปแบบการวิจัยเชิงคุณภาพ เก็บข้อมูลด้วยเทคนิคการวิจัยเอกสารร่วมกับการสัมภาษณ์เชิงลึก จากกลุ่มตัวอย่าง 3 กลุ่ม แบ่งเป็น ผู้ปฏิบัติงานในด้านเทคโนโลยีสารสนเทศกลุ่มสถาบันการเงิน ผู้ปฏิบัติงานจากสายงานกระบวนการยุติธรรมหรือสายกฎหมาย และผู้เชี่ยวชาญอิสระด้านการจัดการความมั่นคงปลอดภัยทางไซเบอร์

ผลการศึกษา พบว่า 1) บทบาทที่สำคัญของธนาคารกลางของไทย คือ การวางกรอบแนวทางการรับมือภัยคุกคามไซเบอร์ โดยมีการกำหนดเป็นมาตรการและนโยบายต่าง ๆ ร่วมกับการตรวจสอบกำกับดูแล และการเผยแพร่ความรู้ให้แก่ภาคประชาชน 2) ธนาคารกลางของไทยมีการสร้างความร่วมมือกับกลุ่มสถาบันการเงินและองค์กรอื่น ๆ ทั้งภายในประเทศและต่างประเทศ เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์ที่เกิดขึ้น ซึ่งจะก่อให้เกิดทักษะความรู้ใหม่ ๆ ในการร่วมมือกันแก้ปัญหาภัยคุกคามไซเบอร์

ข้อเสนอแนะจากการศึกษานี้สามารถแบ่งได้เป็น 2 ด้าน คือ ด้านการปฏิบัติการ สถาบันการเงินควรมีการฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์ ไปพร้อมกับการสร้างความตระหนักรู้ให้แก่ภาคประชาชนในเชิงรุก รวมทั้งสร้างเครือข่ายด้านเทคโนโลยีสารสนเทศในภาคการเงิน ด้านการออกนโยบาย เสนอให้เพิ่มบทลงโทษสถาบันการเงินจากการไม่ปฏิบัติตามมาตรการที่บังคับใช้ และเสนอให้มีการสร้างความร่วมมือกับภาครัฐปรับหลักสูตรการเรียนการสอนให้มีบทเรียนเกี่ยวกับภัยคุกคามไซเบอร์และมาตรการความมั่นคงปลอดภัยทางไซเบอร์

สาขาวิชา อาชญาวิทยาและงานยุติธรรม ลายมือชื่อนิสิต .....

ปีการศึกษา 2562 ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

5980971724 : MAJOR CRIMINOLOGY AND CRIMINAL JUSTICE
KEYWORD: Cyber Threat, Cyber Security, Central Bank, Financial Institution
Poramat Viruk : A STUDY OF CYBERSECURITY MEASURES IN FINANCIAL INSTITUTIONS . Advisor: Assoc. Prof. SUMONTHIP CHITSAWANG, Ph.D.

The purpose of this study is to conduct research on the role of the central bank of Thailand in supervising financial institutions on an enforcement of cyber security measures and studying guidelines for establishing cooperation between financial institutions. This research primarily utilized the qualitative method of documentary research combined with in-depth interview from three samples groups, which included information technology operators in financial institutions, officers in administration of justice or legal and independent experts in cyber security management.

The key findings of this study show that: 1) The important role of central bank of Thailand is designing a framework to deal with cyber threats. The measures and policies are defined in conjunction with monitoring, supervising and disseminating cyber knowledge to the public sector. 2) The central bank of Thailand collaborates with financial institutions and other organizations both domestically and overseas to share knowledge and to build skills for solving cyber threats.

The suggestions from this study divided into 2 areas. In operation area, financial institutions should practice regularly to cope with threats along with proactively raising awareness to the public sector, in addition to building networks of information technology in the financial sector. In policy area, the central bank should increase penalties for non-compliance with their measures and collaborate with the government to include more lessons about cyber threats and cyber security measures into school curriculum.

Field of Study:	Criminology and Criminal Justice	Student's Signature .....
Academic Year:	2019	Advisor's Signature .....

กิตติกรรมประกาศ

สิ่งแรกที่ผู้วิจัยอยากกล่าวขอบคุณ คงเป็นคณาจารย์สาขาวิชาอาชญาวิทยาและงานยุติธรรมทุกท่าน ที่ได้มอบโอกาสให้ผู้วิจัยได้เข้ามาศึกษาในสถาบันอันทรงเกียรติแห่งนี้ โดยเฉพาะอย่างยิ่ง รองศาสตราจารย์ ดร.สุมนทิพย์ จิตสว่าง ที่กรุณารับเป็นอาจารย์ที่ปรึกษาในวิทยานิพนธ์เล่มนี้ อีกทั้งยังเป็นผู้ที่ดึงผู้วิจัยออกมาจากหลุมแห่งความท้อแท้และสิ้นหวัง ให้กลับมาเดินอยู่ในทิศทางถูกต้อง จนทำให้งานวิจัยสำเร็จไปได้ด้วยดี

ขอขอบคุณ รองศาสตราจารย์ ดร.จุฑารัตน์ เอื้ออำนวย ผู้กำหนดแนวทางในการวิจัย และเป็นผู้ที่คอยชี้ทางออกจากความมืดมนได้อยู่เสมอ

ขอขอบคุณ ดร.กฤษฎ์ เดชารักษ์ ที่สละเวลามาเป็นกรรมการร่วมในงานวิจัยครั้งนี้ และเป็นผู้ที่ทำให้งานวิจัยเล่มนี้มีความสมบูรณ์มากยิ่งขึ้น

ขอขอบคุณ เจ้าหน้าที่ภาควิชาสังคมวิทยาและมานุษยวิทยาทุกท่าน โดยเฉพาะ คุณกนกพร รักท้วม สำหรับความเสียสละ ที่คอยตามดูแล ตามแก้ไขปัญหาในทุกเรื่อง

ขอขอบคุณ ผู้ให้ข้อมูลทุกท่าน ที่ผู้วิจัยไม่อาจจะเอ่ยนามในที่นี้ ขอให้ทุกท่านได้รับรู้เอาไว้ว่าข้อมูลอันมีค่าของทุกท่านเป็นส่วนหนึ่งของงานวิจัยเล่มนี้

ขอขอบคุณ คุณปัญจรีย์ ไชยจรูญโชติ ผู้ที่อยู่เคียงข้างผู้วิจัย ผู้ที่ต้องคอยรองรับความทุกข์ใจของผู้วิจัยเอาไว้โดยตลอด อีกทั้งยังคอยสนับสนุนในทุกเรื่องเสมอมา

ขอขอบคุณ แรงใจจากครอบครัวที่เชียงใหม่ ผู้คอยส่งกำลังใจที่อาจไม่ได้มาเป็นคำพูดแต่สัมผัสได้ด้วยใจ

ท้ายสุด ผู้วิจัยหวังว่าข้อมูลในงานวิจัยครั้งนี้ จะเป็นประโยชน์กับผู้ที่มีความสนใจในอาชญากรรมไซเบอร์ หรือ อย่างน้อยก็อาจช่วยให้ได้จุดประกายแนวคิด เพื่อนำไปต่อยอดในงานวิจัยต่อไปในอนาคต

ปรมัตถ์ ไวรักษ์

สารบัญ

หน้า

สารบัญตาราง

สารบัญรูปภาพ

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญของปัญหา

“อาชญากรรมเปรียบเสมือนภาพสะท้อนสภาพสังคมที่เป็นอยู่” หรืออาจกล่าวได้ในอีกทางหนึ่งว่า “อาชญากรรมเป็นผลผลิตทางสังคมที่ถูกสร้างขึ้นจากผู้คนในสังคม” ในอดีตปัญหาอาชญากรรมที่เกิดขึ้นในสังคมมนุษย์ไม่ได้มีรูปแบบที่หลากหลายมากนัก รูปแบบปัญหาอาชญากรรมที่เกิดขึ้นโดยทั่วไปจะเป็นอาชญากรรมพื้นฐาน อาทิ การลักทรัพย์ การชิงทรัพย์ การปล้นทรัพย์ การฆาตกรรม การข่มขืน ซึ่งแตกต่างจากปัจจุบันที่ปัญหาอาชญากรรมมีการผสมผสานรูปแบบที่หลากหลายและมีความสลับซับซ้อนมากยิ่งขึ้น ตามการเปลี่ยนแปลงของสภาพสังคมที่มีความเลื่อนไหลอย่างไม่หยุดนิ่ง ซึ่งในทางอาชญาวิทยาได้มีการเรียกอาชญากรรมรูปแบบใหม่ ๆ ที่เกิดขึ้นในยุคนี้ว่า “อาชญากรรมร่วมสมัย” (Contemporary Crimes)

โดยสังคมในยุคปัจจุบันเป็นสังคมที่ถูกขับเคลื่อนด้วยเทคโนโลยีคอมพิวเตอร์หรือที่เรียกกันว่า “ยุคแห่งเทคโนโลยีสารสนเทศ” การเปลี่ยนแปลงทางสังคมดังกล่าวได้ก่อให้เกิดอาชญากรรมในรูปแบบใหม่ที่เรียกว่า อาชญากรรมไซเบอร์ (Cyber Crime) ในประเด็นปัญหาอาชญากรรมไซเบอร์กำลังเป็นกระแสที่ถูกกล่าวถึงในแวดวงการศึกษาอาชญาวิทยา เนื่องด้วยสถานการณ์ในปัจจุบันปัญหาอาชญากรรมไซเบอร์ กำลังขยายตัวเป็นวงกว้างและทวีความรุนแรงอย่างรวดเร็วจนก่อให้เกิดผลกระทบไปยังสังคมทั่วโลก ด้วยจุดเด่นของรูปแบบลักษณะของอาชญากรรมไซเบอร์ ที่มีรูปแบบการโจมตีที่หลากหลายและมีความสลับซับซ้อนด้วยเทคนิคคอมพิวเตอร์อยู่ภายในตัว อีกทั้งยังมีการเปลี่ยนแปลงรูปแบบเทคนิคการโจมตีอยู่อย่างสม่ำเสมอ ตามการพัฒนาเทคโนโลยีคอมพิวเตอร์ อาชญากรไซเบอร์จะค้นหาวิธีการใหม่ ๆ เพื่อเข้าโจมตีเหยื่อโดยเสาะแสวงหาจากช่องโหว่ทางเทคโนโลยีคอมพิวเตอร์ที่ถูกเปิดทิ้งไว้อย่างไม่ตั้งใจ

ในอีกด้านของปัญหา การศึกษาถึงแนวทางการป้องกันอาชญากรรมไซเบอร์ ถูกนำมาเป็นประเด็นให้เหล่านักอาชญาวิทยาต้องกลับมาขบคิดถึงสาเหตุของปัญหาที่แท้จริง เพื่อแสวงหาแนวทางป้องกันอาชญากรรมทางไซเบอร์ที่เหมาะสม ซึ่งในปัจจุบันแนวทางป้องกันที่ถูกนำมากล่าวถึง คือ “มาตรการความมั่นคงปลอดภัยทางไซเบอร์” (Cyber Security Measures) โดยมาตรการดังกล่าวได้ถูกหยิบยกเป็นแนวทางหลักที่สังคมส่วนใหญ่ต่างเห็นพ้องต้องกัน จะเห็นได้จากองค์กรต่าง ๆ ได้มีการ

กำหนดมาตรการนี้ขึ้นเพื่อใช้ในองค์กรของตัวเอง รวมไปถึงการรวมกลุ่มในการกำหนดมาตรการร่วมกันจากองค์กรที่มีลักษณะทางสภาพแวดล้อมที่คล้ายคลึงกัน

อย่างไรก็ตามภายในหน่วยงานหรือองค์กรทั่วโลก ส่วนใหญ่ยังขาดการวางมาตรการจัดการปัญหาที่มีประสิทธิภาพเพียงพอต่อการป้องกันภัยคุกคามทางไซเบอร์ โดยเฉพาะอย่างยิ่งในกลุ่มสถาบันการเงินทั่วโลกที่กำลังตกเป็นเป้าหมายสำคัญของเหล่าอาชญากรไซเบอร์ หนทางในการแก้ไขปัญหาดังกล่าวจึงจำเป็นที่จะต้องมีการเร่งจัดการมาตรการความมั่นคงปลอดภัยทางไซเบอร์ภายในองค์กรสถาบันการเงินเหล่านี้ เพื่อทำการปิดช่องโหว่ทางเทคโนโลยีคอมพิวเตอร์ อีกทั้งยังเป็นการเตรียมความพร้อมรับมือภัยคุกคามทางไซเบอร์ที่กำลังสร้างความปั่นป่วนให้กับสังคมไปทั่วโลก

บทเรียนสำคัญจากในอดีตที่ผ่านมาที่เกิดจากสถาบันการเงินหลายแห่ง ได้ขาดการตระหนักรู้ถึงปัญหาภัยคุกคามทางไซเบอร์ จนละเลยต่อการจัดการระบบความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรให้มีประสิทธิภาพ ซึ่งเป็นเหตุให้ถูกกลุ่มอาชญากรไซเบอร์เข้าโจมตีจนสร้างความเสียหายให้กับสถาบันการเงิน ดังตัวอย่างกรณีศึกษาที่จะนำมากล่าวถึงต่อไปนี้

กรณีศึกษาแรกเป็นเหตุการณ์ที่เกิดขึ้นในทวีปเอเชีย โดยในช่วงต้นปี พ.ศ.2559 พบรายงานข่าวการถูกโจมตีทางไซเบอร์ของธนาคารกลางบังคลาเทศ ด้วยรูปแบบการลักลอบเจาะระบบเซิร์ฟเวอร์ โดยใช้มัลแวร์แฝงตัวเข้ามาในระบบพร้อมกับฝังตัวเก็บข้อมูลค้นหาช่องโหว่ของระบบจนสามารถเข้าโจมตีผ่านระบบที่มีชื่อว่า SWIFT (Society for Worldwide Interbank Financial Telecommunication) ซึ่งเป็นระบบโครงสร้างพื้นฐานทางการชำระเงิน ที่ใช้รองรับการโอนเงินมูลค่าสูงระหว่างประเทศและใช้ในการสื่อสารข้อมูลทางการเงินในธนาคารทั่วโลก ผลจากการตรวจสอบเพิ่มเติมในภายหลัง พบว่า การโจมตีเริ่มต้นจากการปล่อยมัลแวร์รูปแบบเฉพาะที่ถูกสร้างขึ้นมาโดยอาชญากรไซเบอร์ เข้าไปแฝงตัวอยู่ในระบบเซิร์ฟเวอร์ของธนาคาร เพื่อเก็บข้อมูลรูปแบบการโอนเงินพร้อมทั้งวางแผนปฏิบัติการ โดยเฝ้ารอคอยจนถึงช่วงเวลาที่เหมาะสมในการเข้าโจมตี จึงเริ่มปฏิบัติการสั่งโอนเงินจำนวนหลายสิบครั้งผ่านระบบ SWIFT ไปยังธนาคารกลางสหรัฐ สำนักงานนิวยอร์ก ที่ซึ่งธนาคารกลางของบังคลาเทศผูกบัญชีอยู่ กลุ่มอาชญากรไซเบอร์ได้สั่งให้โอนเงินจำนวนรวม 951 ล้านดอลลาร์สหรัฐ หรือกว่า 33,000 ล้านบาท ไปเข้าบัญชีส่วนบุคคลที่เปิดไว้กับธนาคารริซาล คอมเมอร์เชียล แบงก์ คอร์เปอเรชั่นในประเทศฟิลิปปินส์ ซึ่งหลังจากปฏิบัติการไปได้ช่วงระยะเวลาหนึ่งระบบได้ตรวจพบว่า มีคำสั่งหลายคำสั่งไม่สมบูรณ์และธนาคารกลางบังคลาเทศสามารถระงับคำสั่งที่ผิดปกติเหล่านั้นเอาไว้ได้ในบางส่วน เหตุการณ์ดังกล่าวคนร้ายจึงสามารถสั่งโอนเงินออกไปได้เพียง 101 ล้านดอลลาร์สหรัฐ หรือประมาณ 3,000 ล้านบาท โดยจำนวนเงินทั้งหมดนั้น

ได้ถูกสั่งจ่ายออกไปยังธนาคารอีกหลายแห่ง จากการตรวจสอบพบว่า มีการสั่งโอนเงินไปยังธนาคารในบังคลาเทศ จำนวน 20 ล้านดอลลาร์ หรือ 70 ล้านบาท ซึ่งถูกทางการอายัดเอาไว้ได้ในภายหลัง ในขณะที่จำนวนเงินอีก 81 ล้านดอลลาร์สหรัฐ หรือกว่า 2,800 ล้านบาท สามารถโอนไปยังธนาคารในฟิลิปปินส์ได้สำเร็จ ก่อนทยอยถอนออกไปได้ 58 ล้านดอลลาร์สหรัฐ หรือกว่า 2,000 ล้านบาท ในส่วนที่เหลืออีก 22.85 ล้านดอลลาร์สหรัฐ ทางการสามารถสั่งระงับธุรกรรมทางการเงินเอาไว้ได้ทัน จำนวนเงินที่ถอนไปได้มีการส่งต่อไปฟอกเงินในคาสิโนที่ซึ่งกฎหมายฟอกเงินของฟิลิปปินส์ไม่สามารถบังคับใช้ได้ โดยการโจมตีในครั้งนี้ได้สร้างความเสียหายไปกว่า 81 ล้านดอลลาร์สหรัฐ[1] เครื่องมือสำคัญที่อาชญากรไซเบอร์ใช้ในการโจมตีครั้งนี้ เป็นมัลแวร์ที่มีรูปแบบเฉพาะที่ถูกสร้างมาเพื่อแฝงตัวเข้าไปอยู่ในระบบเซิร์ฟเวอร์ ซึ่งตัวมัลแวร์ชนิดนี้สามารถลบร่องรอยของการกระทำผิด โดยทำการปรับเปลี่ยนข้อมูลและลบประวัติการทำธุรกรรมที่ปลอมแปลงไปจนหมด รวมไปถึงสั่งให้เครื่องพิมพ์ไม่พิมพ์ข้อมูลธุรกรรมที่ปลอมแปลงลงไป นอกจากนี้มัลแวร์ดังกล่าวยังสามารถดักจับและทำลายข้อความที่ยืนยันการโอนเงิน ส่งผลให้ไม่สามารถตรวจจับการถูกโจมตีในครั้งนี้ได้เลย[2] ในส่วนระบบความมั่นคงปลอดภัยทางไซเบอร์ของธนาคารกลางบังคลาเทศที่ใช้เชื่อมต่อกับระบบ SWIFT นั้น ตรวจพบว่ามีช่องโหว่อยู่หลายจุด อาทิ การเปิดให้สามารถเชื่อมต่อเข้าถึงระบบได้จากภายนอก การใช้รหัสผ่านที่สามารถคาดเดาได้ง่าย รวมไปถึง ไม่มีการติดตั้งระบบไฟร์วอล (Firewall) ที่เปรียบเสมือนกำแพงป้องกันการโจมตีทางไซเบอร์ ซึ่งการที่ไม่มีระบบไฟร์วอลนั้นก่อให้เกิดช่องโหว่ที่ทำให้ถูกลักลอบปล่อยมัลแวร์เข้ามาในระบบ อีกทั้งยังมีการตรวจพบว่าหนึ่งในสาเหตุที่ทำให้ระบบมีช่องโหว่อาจเกิดจากบุคลากรภายในองค์กร ได้เข้ามามีส่วนเกี่ยวข้องต่อการโจมตีในครั้งนี้ด้วย[3]

ลำดับต่อมาเป็นกรณีศึกษาที่เกิดขึ้นในฝั่งทวีปยุโรป ในช่วงกลางปีเดียวกันหลังจากเหตุการณ์โจมตีธนาคารกลางบังคลาเทศได้เพียงไม่กี่เดือน ได้มีการรายงานข่าวว่า ธนาคารแห่งหนึ่งในประเทศยูเครนถูกโจมตีทางไซเบอร์ โดยเข้าโจมตีจากช่องโหว่ของระบบ SWIFT เช่นเดียวกับรูปแบบวิธีการที่ใช้โจมตีในธนาคารกลางบังคลาเทศ ซึ่งอาชญากรไซเบอร์จะปล่อยมัลแวร์รูปแบบเฉพาะ เข้าไปฝังตัว

---

[1] Thai PBS News, **เผยบังคลาเทศก็เคยเจอแฮกเกอร์เจาะแบงก์ สูญเกือบ 3 พันล้าน** [ออนไลน์], 25 สิงหาคม 2559. แหล่งที่มา http://news.thaipbs.or.th/content/255180

[2] “แฮกเกอร์โจมตีแบงค์บังคลาเทศผ่านช่องทาง SWIFT ซอฟต์แวร์,” วารสารTransport Journal 19,804 (พฤษภาคม 2559): 16.

[3] ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต), **FBI เผย ธนาคารกลางบังคลาเทศถูกเจาะระบบ เหตุฝีมือคนในร่วมด้วย** [ออนไลน์], 11 พฤษภาคม 2559. แหล่งที่มา https://www.thaicert.or.th/newsbite/2016-05-11-01.html#2016-05-11-01

เก็บรวบรวมข้อมูลการโอนเงินในระบบ SWIFT ของธนาคารที่เป็นเป้าหมาย เมื่อสบโอกาสอาชญากรไซเบอร์จะส่งคำร้องขอโอนเงินที่ถูกปลอมแปลงขึ้นไปยังระบบ SWIFT เพื่อเริ่มการโอนเงินจากบัญชีของธนาคารเป้าหมาย ไปยังแหล่งเบิกจ่ายเงินที่ยากต่อการตรวจสอบ การโจมตีดังกล่าวส่งผลให้สามารถขโมยเงินออกไปได้กว่า 10 ล้านดอลลาร์[4]

ซึ่งในกรณีนี้ธนาคารกลางยูเครนได้ออกแถลงการณ์ว่า ได้อาศัยความร่วมมือกับทีมตอบสนองเหตุฉุกเฉินด้านคอมพิวเตอร์ (Computer Emergency Response Team – CERT) แบ่งปันข้อมูลการถูกโจมตีและแนวทางในการป้องกัน พร้อมทั้งได้ออกมาแจ้งเตือนกลุ่มสถาบันการเงินให้ยกระดับมาตรการป้องกันอาชญากรรมทางไซเบอร์ให้รัดกุมมากยิ่งขึ้น[5]

ลำดับถัดไปเป็นกรณีศึกษาที่เกิดขึ้นในประเทศไทย เหตุการณ์นี้เกิดขึ้นในช่วงเดือนสิงหาคม ปี พ.ศ.2559 ซึ่งธนาคารออมสินได้ตกเป็นเหยื่อรายล่าสุดที่ถูกโจมตีทางไซเบอร์ การโจมตีในครั้งนี้มีรายละเอียดรูปแบบการปฏิบัติการที่แตกต่างออกไป โดยอาชญากรไซเบอร์เลือกที่จะลักลอบเชื่อมต่อเข้าสู่ระบบเครือข่ายภายในของธนาคารออมสิน ผ่านทางตู้รับจ่ายเงินสดอัตโนมัติ (Automated Teller Machine - ATM) ด้วยวิธีการปลอมแปลงสร้างโปรแกรมเลียนแบบโปรแกรมที่ใช้อัพเดทซอฟต์แวร์ ทำให้ระบบคอมพิวเตอร์ภายในตู้เอทีเอ็มเข้าใจว่าเป็นการอัพเดทซอฟต์แวร์ แต่กลับส่งมัลแวร์ที่สร้างขึ้นมาเฉพาะเข้าสู่ระบบแทน เมื่อมัลแวร์ถูกปล่อยเข้าสู่ระบบจึงใช้บัตร ATM ที่มีโค้ดลับเฉพาะ ซึ่งจะทำงานร่วมกับมัลแวร์ที่ฝังอยู่ภายในเครื่อง เพื่อสั่งการให้เครื่อง ATM จ่ายเงินสดออกมา[6] ซึ่งเทคนิคการโจมตีในรูปแบบนี้มีชื่อเรียกว่า “แจ๊กพอตติ้ง เอทีเอ็ม” (Jackpotting ATM)[7] การถูกโจมตีในครั้งนี้ผู้บริหารธนาคารออมสินได้ออกมายอมรับว่า พบมัลแวร์ฝังอยู่ในระบบตู้เอทีเอ็มรวม 21 เครื่อง และตรวจพบเงินสูญหายไปกว่า 12 ล้านบาท[8]

---

[4] TechTalkThai, **แฮ็คระบบ SWIFT ธนาคารยูเครน ขโมยเงินไปกว่า 350 ล้านบาท** [ออนไลน์], 28 มิถุนายน 2559. แหล่งที่มา https://www.techtalkthai.com/ukranian-bank-swift-hacked/

[5] Reuters, **Ukraine central bank warns of new cyber-attack risk** [Online], 18 August 2017. Source https://www.reuters.com/article/us-cyber-ukraine-banking/ukraine-central-bank-warns-of-new-cyber-attack-risk-idUSKCN1AY0Y4

[6] TechTalkThai, **สรุปผลวิเคราะห์มัลแวร์ที่โจมตีตู้ ATM ธนาคารออมสินจาก NCR** [ออนไลน์], 31 สิงหาคม 2559. แหล่งที่มา https://www.techtalkthai.com/malware-attack-in-thailand-by-ncr/

[7] “ไขปริศนา ‘มัลแวร์’ ตัวร้าย ดูดเงิน ‘เอทีเอ็ม’,” มติชน (25 สิงหาคม 2559): 9.

[8] “ออมสินรับถูกแฮกเอทีเอ็ม 12 ล. โดนไวรัส200ตู้-สั่งปิดบริการชี้แก๊งยูเครน-ควบคุมจากสวิส ธปท.มึนสกัดล้วงอีแบงก์ยาก,” มติชน (24 สิงหาคม 2559): 1,7,12.

รวมไปถึงในอีกฝั่งของโลกอย่างประเทศสหรัฐอเมริกาก็ตกเป็นเหยื่อการถูกโจมตีทางไซเบอร์ด้วยเช่นกัน โดยมีการรายงานข่าวที่กล่าวถึงการโจมตีทางไซเบอร์ด้วยรูปแบบ “แจ๊กพอตติ้ง เอทีเอ็ม” ในหลากหลายพื้นที่ แต่ไม่ได้กล่าวชี้ชัดถึงชื่อธนาคารที่ตกเป็นเหยื่อและจำนวนเงินที่สูญหายไป[9] วิธีการโจมตีในรูปแบบดังกล่าว สอดคล้องกับเหตุการณ์ที่ธนาคารออมสิน ได้ถูกโจมตีดังที่กล่าวไว้ข้างต้น การโจมตีในครั้งนี้ทำให้ธนาคารที่ให้บริการผ่านตู้เอทีเอ็ม ต้องกลับมาทบทวนวิธีการในการป้องกันการถูกโจมตีด้วยวิธีการลักษณะนี้อีกครั้ง

จากกรณีศึกษาที่ได้ยกตัวอย่างมาประกอบ จะเห็นได้ว่าอาชญากรรมไซเบอร์ได้แพร่กระจายขยายตัวด้วยรูปแบบการโจมตีที่หลากหลายไปยังสังคมทั่วโลก พร้อมทั้งสร้างความเสียหายที่ส่งผลกระทบไปยังสังคมในหลากหลายมิติ ทั้งในมิติของเศรษฐกิจ สังคม และการเมือง ซึ่งมิติทางด้านเศรษฐกิจที่อาจเป็นส่วนที่ได้รับผลกระทบต่อการโจมตีมากที่สุด โดยในมิติของเศรษฐกิจกลุ่มสถาบันการเงินถือได้ว่าเป็นกลุ่มที่มีบทบาทสำคัญในการขับเคลื่อนเศรษฐกิจการเงินของประเทศ เมื่อกลุ่มสถาบันการเงินตกอยู่ในสภาวะที่สุ่มเสี่ยงต่อการตกเป็นเหยื่ออาชญากรรมไซเบอร์ ระบบเศรษฐกิจของประเทศจึงหลีกหนีไม่พ้นที่จะตกอยู่ในสภาวะที่สุ่มเสี่ยงไปด้วยเช่นกัน กลุ่มสถาบันการเงินจึงมีความจำเป็นที่จะต้องเร่งสร้างมาตรการความมั่นคงปลอดภัยทางไซเบอร์ เพื่อต่อต้านการถูกโจมตีได้อย่างทันท่วงที มีประสิทธิภาพ และสามารถกู้คืนระบบให้กลับมาสู่สภาวะปกติ ภายในระยะเวลาที่เหมาะสม

ซึ่งในปัจจุบันกลุ่มสถาบันการเงินในประเทศไทย ได้เรียกคืนความเชื่อมั่นที่มีต่อสถาบันการเงินจากกลุ่มผู้บริโภค ด้วยการเตรียมความพร้อมในการรับมือปัญหาภัยคุกคามทางไซเบอร์ที่กำลังถาโถมเข้ามา โดยกลุ่มสถาบันการเงิน 15 แห่ง ได้รวมตัวกันจัดตั้งกลุ่มความร่วมมือสถาบันการเงินภายใต้ชื่อ “ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร” (Thailand Banking Sector & Computer Emergency Response Team -TB-CERT) เพื่อสร้างความร่วมมือในการดูแลความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและเพื่อเป็นการเตรียมความพร้อมในการรับมือกับปัญหาอาชญากรรมไซเบอร์ ซึ่งสอดรับกับนโยบายของสถาบันการเงินยุคใหม่ที่ต้องการนำเอาเทคโนโลยีคอมพิวเตอร์มาใช้ในการให้บริการทางการเงินให้มากยิ่งขึ้น โดยการจัดตั้งกลุ่มดังกล่าวได้รับการสนับสนุนจากสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) และมีการ

[9] “โจรไฮเทคพุ่งเป้า เจาะเอทีเอ็มทั่วโลก,” โพสต์ทูเดย์ (28 สิงหาคม 2559): 3.

ควบคุมกำกับดูแลจากธนาคารแห่งประเทศไทย (ธปท.)[10] ซึ่งจะเข้ามาควบคุมในฐานะธนาคารกลางที่มีบทบาทหน้าที่ในการกำกับดูแลสถาบันการเงินให้มีความมั่นคง พร้อมทั้งดูแลบริหารจัดการความเสี่ยงในภาพรวมของสถาบันการเงินให้ครอบคลุมและมีประสิทธิภาพตามหลักเกณฑ์มาตรฐานสากล

จากประเด็นปัญหาที่กล่าวมาทั้งหมด ทำให้ผู้วิจัยเกิดความสนใจที่จะศึกษาในประเด็นปัญหาในมิติของการป้องกันอาชญากรรมไซเบอร์ โดยพุ่งเป้าไปที่การศึกษาถึงมาตรการความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งเป็นมาตรการตามหลักเกณฑ์สากลที่สถาบันการเงินได้นำมาปรับใช้ เพื่อเป็นเกราะป้องกันปัญหาอาชญากรรมไซเบอร์ รวมไปถึงการศึกษาถึงแนวทางการสร้างความร่วมมือระหว่างกลุ่มสถาบันการเงินด้วยกันในการป้องกันปัญหาอาชญากรรมไซเบอร์

1.2 คำถามวิจัย

ธนาคารกลางของไทยมีบทบาทในการกำกับดูแลสถาบันการเงินต่อการบังคับใช้มาตรการความมั่นคงปลอดภัยทางไซเบอร์อย่างไร สถาบันการเงินมีการสร้างความร่วมมือระหว่างกลุ่มในการป้องกันปัญหาอาชญากรรมไซเบอร์อย่างไร และควรมีการกำหนดมาตรการป้องกันอาชญากรรมทางไซเบอร์ที่เหมาะสมสำหรับประเทศไทยอย่างไร

1.3 วัตถุประสงค์ของการวิจัย

1.3.1 เพื่อศึกษาบทบาทธนาคารกลางของไทยในการกำกับดูแลสถาบันการเงินต่อการบังคับใช้มาตรการความมั่นคงปลอดภัยทางไซเบอร์

1.3.2 เพื่อศึกษาวิเคราะห์แนวทางการสร้างความร่วมมือระหว่างกลุ่มสถาบันการเงินในการกำหนดมาตรการป้องกันอาชญากรรมไซเบอร์

1.3.3 เพื่อเสนอแนะแนวทางการกำหนดมาตรการป้องกันอาชญากรรมไซเบอร์ที่เหมาะสม

1.4 ขอบเขตของการวิจัย

การวิจัยครั้งนี้ผู้วิจัยมีขอบเขตในการศึกษาจากเฉพาะกลุ่มตัวอย่างธนาคารกลางของไทยและกลุ่มสถาบันการเงินที่อยู่ภายใต้การกำกับดูแล คือ กลุ่มธนาคารพาณิชย์ที่จดทะเบียนภายในประเทศ

---

[10] “เก็บเบี้ยใต้ถุนร้าน: ผุดศูนย์ป้องกันไซเบอร์กันแบงก์เสียหาย สร้างความมั่นใจลูกค้า,” วารสารดอกเบี้ย 37, 436 (ตุลาคม 2560): 70-71.

และกลุ่มสถาบันการเงินเฉพาะกิจ จำนวน 5 แห่ง ทั้งนี้ไม่รวมถึง กลุ่มธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารต่างประเทศ กลุ่มผู้ให้บริการทางการเงินที่ไม่ใช่สถาบันการเงิน กลุ่มบริษัทบริหารสินทรัพย์ กลุ่มบริษัทเงินทุน และกลุ่มบริษัทเครดิตฟองซิเอร์ รวมไปถึงการเก็บข้อมูลจากกลุ่มผู้ปฏิบัติงานสายงานด้านกระบวนการยุติธรรม และผู้เชี่ยวชาญด้านการจัดการความมั่นคงปลอดภัยทางไซเบอร์ โดยจะมีระยะเวลาในการศึกษาตั้งแต่เดือนมกราคม 2561 ถึงเดือนสิงหาคม 2563

1.5 รูปแบบการวิจัย

การศึกษาวิจัยในครั้งนี้ผู้วิจัยใช้แนวทางการศึกษาในรูปแบบการวิจัยเอกสาร(Documentary Research) และการวิจัยเชิงคุณภาพ (Qualitative Research) มาศึกษาถึงบทบาทรูปแบบธนาคารกลางในการกำกับดูแลสถาบันการเงินต่อการบังคับใช้มาตรการป้องกันอาชญากรรมทางไซเบอร์ พร้อมทั้งศึกษาวิเคราะห์ถึงประเด็นปัญหาเพื่อให้เกิดความเข้าใจอย่างถ่องแท้ ในการกำหนดมาตรการป้องกันอาชญากรรมทางไซเบอร์และการสร้างความร่วมมือระหว่างกลุ่มสถาบันการเงิน เพื่อสรุปเป็นข้อเสนอแนะแนวทางเชิงนโยบายที่เหมาะสมสำหรับการวางมาตรการป้องกันอาชญากรรมทางไซเบอร์ของกลุ่มสถาบันการเงิน โดยข้อมูลที่ได้จากการศึกษาทั้งหมดจะถูกนำมาสรุปเป็นรายงานวิจัยฉบับสมบูรณ์ พร้อมนำเสนอในงานสัมมนาทางวิชาการหรือตีพิมพ์เป็นบทความวิชาการต่อไป

1.6 การเก็บรวบรวมข้อมูลการวิจัย

เพื่อให้งานวิจัยสามารถตอบโจทย์ปัญหาได้อย่างครบถ้วนถูกต้องตรงประเด็น มีความน่าเชื่อถือ มีความลุ่มลึกทางวิชาการ ด้วยการมองภาพของปัญหาจากมุมมองที่หลากหลาย ซึ่งแต่ละมุมมองนั้นจะมีความเชื่อมโยงต่อกันกับประเด็นปัญหาในหลากหลายมิติ ผู้วิจัยจึงได้เลือกใช้วิธีการผสมผสานเครื่องมือในเก็บรวบรวมข้อมูล ดังนี้

1.6.1 การวิจัยเอกสาร (Documentary Research)

ผู้วิจัยจะใช้วิธีการวิจัยเอกสารในการศึกษาค้นคว้าข้อมูลที่อยู่ในรูปแบบข้อมูลทุติยภูมิ (Secondary Data) ซึ่งจะเป็นข้อมูลที่รวบรวมมาจากหนังสือวิชาการ เอกสาร สื่อสิ่งพิมพ์ สื่อดิจิตอล สื่อสังคมออนไลน์และงานวิจัยที่เกี่ยวข้องต่าง ๆ และนำข้อมูลเหล่านั้นมาสังเคราะห์เป็นข้อมูลเชิงพรรณนาในรูปแบบบทปริทัศน์วรรณกรรม ประกอบการนำเสนอในการศึกษาบททบทวนวรรณกรรม

อีกทั้งยังนำมาใช้ในการศึกษาเพิ่มเติมข้อมูล ในประเด็นบทบาทและรูปแบบในการกำกับดูแลสถาบันการเงินต่อการบังคับใช้มาตรการป้องกันอาชญากรรมทางไซเบอร์

1.6.2 การสัมภาษณ์เชิงลึก (In-depth Interview)

ผู้วิจัยจะใช้การเก็บข้อมูลด้วยการสัมภาษณ์เชิงลึกจากผู้ให้ข้อมูลสำคัญ (Key Informants) ด้วยเทคนิคการสุ่มกลุ่มตัวอย่างแบบเจาะจง (Purposive Sampling) จำนวน 2 ราย และใช้เทคนิคการสุ่มกลุ่มตัวอย่างแบบสโนว์บอล (Snowball Sampling) จำนวน 10 ราย โดยอาศัยการแนะนำจากผู้ให้ข้อมูลชุดแรก ส่งต่อข้อมูลแบบต่อเนื่องจากกลุ่มเครือข่ายข้อมูล ทั้งนี้กลุ่มผู้ให้ข้อมูลต้องมาจากกลุ่มเป้าหมายที่มีความรู้เฉพาะด้านมาตรการความมั่นคงปลอดภัยทางไซเบอร์หรือมีประสบการณ์ที่เกี่ยวข้องกับประเด็นคำถามวิจัย อาทิ ผู้ปฏิบัติงานด้านกำกับดูแลตรวจสอบเทคโนโลยีสารสนเทศกลุ่มสถาบันการเงิน ผู้ปฏิบัติงานในการควบคุมดูแลระบบความมั่นคงปลอดภัยทางไซเบอร์ ผู้ปฏิบัติงานในด้านกระบวนการยุติธรรม และผู้เชี่ยวชาญด้านการจัดการความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้เพื่อให้ได้ข้อมูลเชิงคุณภาพจากหลากหลายมุมมองครอบคลุมทุกมิติของคำถามวิจัย

1.7 ผู้ให้ข้อมูลสำคัญและวิธีการคัดเลือก

การคัดเลือกผู้ให้ข้อมูลนั้น ผู้วิจัยจะแบ่งออกเป็นสองขั้นตอน

ในขั้นตอนแรก การคัดเลือกผู้ให้ข้อมูลสำคัญผู้วิจัยเลือกใช้เทคนิคการสุ่มกลุ่มตัวอย่างแบบเจาะจง (Purposive Sampling) โดยเริ่มต้นจากผู้ปฏิบัติงานในด้านกำกับดูแลตรวจสอบเทคโนโลยีสารสนเทศของธนาคารแห่งประเทศไทย จำนวน 2 ราย

ในขั้นตอนที่สอง จะใช้เทคนิคการสุ่มกลุ่มตัวอย่างแบบสโนว์บอล (Snowball Sampling) จำนวน 10 ราย ซึ่งคัดเลือกมาจากกลุ่มบุคคลที่ได้รับการแนะนำจากผู้ให้ข้อมูลชุดแรก โดยกลุ่มตัวอย่างนั้นจะต้องมีความเกี่ยวข้องกับการจัดการปัญหาความมั่นคงปลอดภัยทางไซเบอร์หรือมีส่วนร่วมในการออกนโยบาย แผนยุทธศาสตร์ กฎเกณฑ์ ข้อบังคับต่าง ๆ ในกลุ่มสถาบันการเงิน ซึ่งประกอบด้วยบุคลากรจากหน่วยงานต่าง ๆ ได้แก่

1.7.1 ผู้ปฏิบัติงานในด้านเทคโนโลยีสารสนเทศกลุ่มสถาบันการเงิน

คัดเลือกมาจากผู้ที่ปฏิบัติงานในด้านกำกับดูแลตรวจสอบเทคโนโลยีสารสนเทศกลุ่มสถาบันการเงินของธนาคารแห่งประเทศไทย โดยผู้ข้อมูลจะต้องอยู่ในคณะทำงานในการยกร่าง Cyber

Resilience Assessment Framework ซึ่งเป็นหลักเกณฑ์ที่ออกมาใช้การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน จำนวน 3 ราย

คัดเลือกจากผู้ที่ปฏิบัติงานในการควบคุมดูแลระบบความมั่นคงปลอดภัยทางไซเบอร์จากกลุ่มตัวอย่างสถาบันการเงิน จำนวน 2 ราย

1.7.2 ผู้ปฏิบัติงานจากสายงานกระบวนการยุติธรรมหรือสายกฎหมาย

คัดเลือกจากเจ้าหน้าที่ตำรวจที่มีความรู้ความเชี่ยวชาญในด้านการบังคับใช้กฎหมายเทคโนโลยีสารสนเทศจากกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ จำนวน 1 ราย

คัดเลือกจากผู้เชี่ยวชาญด้านกฎหมายเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับสถาบันการเงินจากสำนักงานอัยการสูงสุด จำนวน 1 ราย

1.7.3 ผู้เชี่ยวชาญอิสระด้านการจัดการความมั่นคงปลอดภัยทางไซเบอร์

คัดเลือกจากผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางไซเบอร์จากผู้ที่มีประสบการณ์ ผลงานวิชาการหรือนำเสนอแนวคิดขับเคลื่อนการจัดการความมั่นคงปลอดภัยทางไซเบอร์ที่ได้รับการยอมรับจากสังคม จำนวน 1 ราย

ผู้เชี่ยวชาญจากสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) ซึ่งเป็นหน่วยงานที่มีบทบาทในการสนับสนุนให้ทุกภาคส่วนตระหนักถึงปัญหาอาชญากรรมไซเบอร์ พร้อมทั้งเผยแพร่ความรู้ในการจัดการความมั่นคงปลอดภัยทางไซเบอร์หรือแนวทางในการป้องกันอาชญากรรมไซเบอร์ให้กับสังคม จำนวน 1 ราย

รวมไปถึงผู้แทนจากศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคธนาคาร (TB-CERT) หน่วยงานเฉพาะกิจที่ถูกจัดตั้งขึ้นมาเพื่อยกระดับความร่วมมือในการดูแลความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและเตรียมความพร้อมรับมือกับภัยคุกคามไซเบอร์ให้กับกลุ่มสถาบันการเงิน จำนวน 1 ราย

1.8 การจัดทำเครื่องมือในการวิจัย

เพื่อให้การวิจัยได้มาซึ่งข้อมูลที่ครอบคลุมประเด็นคำถามวิจัยและได้รับเนื้อหาข้อมูลที่มีความเที่ยงตรงสมบูรณ์ตามวัตถุประสงค์ของการวิจัย ผู้วิจัยจึงได้เลือกใช้เทคนิคใช้การสัมภาษณ์เชิงลึกในรูปแบบการสัมภาษณ์แบบเป็นทางการ มาเป็นเครื่องมือที่ใช้ในการศึกษาและรวบรวมข้อมูล โดยในองค์ประกอบของแบบสัมภาษณ์ จะประกอบไปด้วย 3 ชุดคำถาม ดังนี้

1.8.1 ชุดคำถามที่ 1 กลุ่มผู้ปฏิบัติงานในด้านเทคโนโลยีสารสนเทศกลุ่มสถาบันการเงิน

ประเด็นคำถาม บทบาทและรูปแบบการกำกับดูแลสถาบันการเงินต่อการบังคับใช้มาตรการป้องกันอาชญากรรมทางไซเบอร์ การสร้างความร่วมมือระหว่างกลุ่มสถาบันการเงินในการป้องกันปัญหาอาชญากรรมไซเบอร์ และแนวทางการกำหนดมาตรการป้องกันอาชญากรรมทางไซเบอร์ที่เหมาะสม

1.8.2 ชุดคำถามที่ 2 กลุ่มผู้ปฏิบัติงานจากสายงานกระบวนการยุติธรรมหรือสายกฎหมาย

ประเด็นคำถาม การบังคับใช้กฎหมายเทคโนโลยีสารสนเทศต่อปัญหาอาชญากรรมไซเบอร์และแนวทางในการปรับปรุงกฎหมายในภาคการเงินเพื่อรองรับปัญหาอาชญากรรมไซเบอร์

1.8.3 ชุดคำถามที่ 3 ผู้เชี่ยวชาญอิสระด้านการจัดการความมั่นคงปลอดภัยทางไซเบอร์

ประเด็นคำถาม บทบาทในการสนับสนุนมาตรการความมั่นคงปลอดภัยทางไซเบอร์ให้กับสถาบันการเงินไทย

1.9 การวิเคราะห์ข้อมูล

ข้อมูลที่ได้มาจากการวิจัยเอกสารและการสัมภาษณ์เชิงลึก จะถูกนำมาวิเคราะห์ข้อมูลด้วยวิธีการวิเคราะห์เชิงเนื้อหา (Content Analysis) เพื่อจัดกลุ่มข้อมูลตรวจสอบความถูกต้อง ความครบถ้วนของข้อมูลที่ถูกรวบรวมมาและคัดแยกประเด็นที่ไม่เกี่ยวข้องกับการวิจัยออกไป เพื่อให้ได้ข้อมูลที่มีเนื้อหาที่ตรงประเด็นกับคำถามวิจัยที่ได้ตั้งไว้

1.10 จริยธรรมของการวิจัย

ผู้วิจัยได้ตระหนักถึงจริยธรรมการวิจัย (Research Ethics) ซึ่งงานวิจัยจะต้องดำเนินงานวิจัยโดยตั้งอยู่บนพื้นฐานของจริยธรรมและหลักวิชาการที่เหมาะสม[11] จึงต้องมีการได้รับการยินยอมในการเผยแพร่ข้อมูลจากผู้ให้ข้อมูลทั้งหมด ในส่วนของการสัมภาษณ์ผู้วิจัยจะทำการชี้แจงแนวทางการวิจัยรวมถึงหลักจริยธรรมในการวิจัยแก่ผู้ให้ข้อมูล โดยในงานวิจัยจะไม่มีการเปิดเผยข้อมูลชื่อนามสกุลที่แท้จริงของผู้ให้ข้อมูล รวมไปถึงชื่อองค์กรที่มีความเกี่ยวข้อง เพื่อไม่ให้ผลในทางลบหรือเกิดความเสียหายแก่องค์กร ซึ่งข้อมูลทั้งหมดที่อยู่ในงานวิจัยจะต้องได้รับความยินยอมจากผู้ให้ข้อมูล

[11] อัศวิน แสงพิกุล, “จริยธรรมการวิจัย,” วารสารสุทธิปริทัศน์ 27,81 (มกราคม-มีนาคม 2556): 136-146.

1.11 ระยะเวลาทำการวิจัย

ในการศึกษาวิจัยการวิจัยครั้งนี้ผู้วิจัยใช้ระยะเวลาในการศึกษา ตั้งแต่เดือนพฤศจิกายน 2561 จนถึง เดือนสิงหาคม 2563

1.12 นิยามศัพท์

มาตรการความมั่นคงปลอดภัยทางไซเบอร์ หมายถึง แนวทางการปฏิบัติที่ออกมาบังคับใช้ในป้องกันอาชญากรรมไซเบอร์ภายในกลุ่มสถาบันการเงิน ซึ่งจะอยู่ในรูปแบบของแผนยุทธศาสตร์ แนวนโยบาย แนวทางการปฏิบัติ กรอบการดำเนินงาน กรอบแนวคิดด้านการรักษาความปลอดภัย การบริหารจัดการความเสี่ยง ระเบียบหลักเกณฑ์ ข้อบังคับทางกฎหมาย การฝึกอบรม การประกันภัย และการจัดการระบบเทคโนโลยีสารสนเทศ

สถาบันการเงิน หมายถึง กลุ่มธนาคารพาณิชย์ที่จดทะเบียนภายในประเทศและกลุ่มสถาบันการเงินเฉพาะกิจที่อยู่ภายใต้การกำกับดูแลของธนาคารกลางไทยเท่านั้น ซึ่งไม่รวมถึง กลุ่มธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารต่างประเทศ กลุ่มผู้ให้บริการทางการเงินที่ไม่ใช่สถาบันการเงิน กลุ่มบริษัทบริหารสินทรัพย์ กลุ่มบริษัทเงินทุน และกลุ่มบริษัทเครดิตฟองซิเอร์

ธนาคารกลางของไทย หมายถึง ธนาคารแห่งประเทศไทย

อาชญากรรมไซเบอร์ หมายถึง การประกอบอาชญากรรมที่ได้นำเอาเทคโนโลยีคอมพิวเตอร์มาเป็นเครื่องมือในการกระทำความผิด หรือใช้วิธีการใดก็ตามที่สร้างความเสียหายต่อระบบคอมพิวเตอร์ โดยจะส่งผลกระทบต่อสถาบันการเงินทั้งทางตรงและทางอ้อม อาทิ การใช้มัลแวร์ลักลอบเข้าสู่ระบบ การดักจับข้อมูล และการจารกรรมข้อมูลโดยใช้เทคนิควิศวกรรมสังคม

1.13 ประโยชน์ที่ได้รับ

1.13.1 ทำให้เข้าใจถึงบทบาทธนาคารกลางในการกำกับดูแลสถาบันการเงินต่อการบังคับใช้มาตรการความมั่นคงปลอดภัยทางไซเบอร์

1.13.2 ทำให้เข้าใจถึงแนวทางการสร้างความร่วมมือระหว่างกลุ่มสถาบันการเงินในการกำหนดมาตรการป้องกันอาชญากรรมทางไซเบอร์

1.13.3 ทำให้ได้ข้อเสนอแนะแนวทางการกำหนดมาตรการป้องกันอาชญากรรมไซเบอร์ที่เหมาะสม

บทที่ 2
การทบทวนวรรณกรรม

การศึกษาวิจัยในครั้งนี้ ผู้วิจัยได้ทบทวนวรรณกรรมที่เกี่ยวข้อง จากแนวคิด ทฤษฎีต่าง ๆ ที่ได้รวบรวมจากหนังสือวิชาการ เอกสาร สื่อสิ่งพิมพ์ สื่อดิจิตอล สื่อสังคมออนไลน์ และงานวิจัยที่เกี่ยวข้อง มาสังเคราะห์เป็นกรอบแนวคิดประกอบการนำเสนอ สำหรับแนวทางที่ใช้ศึกษา ผู้วิจัยจะนำเอาวิธีการศึกษาในมุมมองเชิงพรรณนา (Descriptive Approach)[1] มาสังเคราะห์เป็นบทปริทัศน์วรรณกรรม (Literature Review) ในรูปแบบของบทความเชิงพรรณนา โดยมีกรอบแนวคิดทฤษฎีที่เกี่ยวข้องในการวิจัย ดังนี้

1. แนวคิดเกี่ยวกับปัญหาอาชญากรรมไซเบอร์และความสัมพันธ์กับอาชญากรรมเศรษฐกิจ
2. แนวคิดการป้องกันอาชญากรรมไซเบอร์และมาตรการความมั่นคงปลอดภัยทางไซเบอร์
3. แนวคิดเกี่ยวกับมาตรการของสถาบันการเงินต่อการป้องกันอาชญากรรมไซเบอร์
4. งานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดเกี่ยวกับอาชญากรรมไซเบอร์และความสัมพันธ์กับอาชญากรรมเศรษฐกิจ

“อาชญากรรมไซเบอร์” เป็นปรากฏการณ์ทางสังคมที่ถือกำเนิดขึ้นจากการพัฒนาเทคโนโลยีคอมพิวเตอร์ ปฏิเสธไม่ได้ว่าในปัจจุบันเทคโนโลยีคอมพิวเตอร์ ได้เข้ามาเป็นส่วนหนึ่งในชีวิตประจำวันของกลุ่มคนส่วนใหญ่ในสังคม ไม่ว่าจะเป็นในระดับปัจเจกบุคคลที่ใช้เทคโนโลยีคอมพิวเตอร์ผ่านอุปกรณ์สมาร์ท ดีไว (Smart Devices) ที่เป็นตัวเชื่อมต่อกับระบบอินเทอร์เน็ต เข้ามาช่วยเหลือกิจกรรมส่วนตัวต่าง ๆ และในระดับกลุ่มที่ใหญ่ขึ้นจากสังคมรอบตัวที่นำเอาเทคโนโลยีคอมพิวเตอร์เข้ามาเป็นตัวช่วยเสริมกิจกรรมทางสังคมในหลากหลายด้าน จะเห็นได้ว่าเทคโนโลยีคอมพิวเตอร์นั้นไม่ได้เป็นสิ่งที่อยู่ไกลตัว แต่กลับเข้ามาอยู่รอบตัวของเราโดยที่เราไม่ทันรู้ตัว การพัฒนาเทคโนโลยีคอมพิวเตอร์ในยุคปัจจุบัน ถูกพัฒนาอยู่บนพื้นฐานของระบบอินเทอร์เน็ต ซึ่งในรอบปีที่ผ่านมาได้มีกระแสสังคมกล่าวถึงแนวคิดในการใช้เทคโนโลยีคอมพิวเตอร์เชื่อมต่อทุกสิ่งรอบตัวเข้าสู่ ระบบอินเทอร์เน็ต ซึ่งมีชื่อที่เรียกกันโดยทั่วไปในสังคมว่า “แนวคิดอินเทอร์เน็ตแห่งสรรพสิ่ง” (The

[1] จุฑารัตน์ เอื้ออำนวย, “การบริหารงานยุติธรรม: วิธีการศึกษา วิเคราะห์ และเปรียบเทียบการบริหารงานยุติธรรม,” (เอกสารประกอบการเรียน สาขาอาชญาวิทยาและงานยุติธรรม ภาควิชาสังคมวิทยาและมานุษยวิทยา คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2560).

Internet of Things) แนวคิดดังกล่าวเป็นการนำเสนอแนวทางสร้างสังคมที่สามารถเชื่อมโยงทุกสิ่งเอาไว้ด้วยกัน การเชื่อมต่ออินเทอร์เน็ตเข้าสู่วัตถุรอบตัวเรา จะทำให้เรามองเห็นความสัมพันธ์ระหว่างคน เครื่องจักรกล และสิ่งของด้วยมุมมองที่ลุ่มลึกกว่าเดิม อีกทั้งยังก่อให้เกิดชุดของฐานข้อมูลขนาดใหญ่ (Big Data) ที่แสดงให้เห็นถึงความสัมพันธ์กันของทุกสรรพสิ่งในระดับที่สูงขึ้นจากเดิม หากย้อนกลับไปพิจารณาถึงเทคโนโลยีคอมพิวเตอร์ในช่วง 10 ปี ที่ผ่านมาเปรียบเทียบกับในปัจจุบัน จะเห็นถึงพัฒนาการของเทคโนโลยีคอมพิวเตอร์ที่ก้าวล้ำเกินกว่าที่ได้คาดการณ์เอาไว้ กรอบแนวคิดดังกล่าวจึงดูเหมือนจะไม่ใช่เรื่องที่ดูเพ้อฝันเกินจริงเหมือนกับนิยายวิทยาศาสตร์ แต่เป็นสิ่งที่กำลังเกิดขึ้นจริงแล้วในสังคม

แนวคิดดังกล่าวข้างต้นสอดคล้องกับสิ่งที่ Samuel Greengard ได้หยิบยกมานำเสนอในมุมมองต่าง ๆ ไว้ได้อย่างน่าสนใจภายในหนังสือ “อินเทอร์เน็ตแห่งสรรพสิ่ง” ซึ่งเนื้อหาภายในหนังสือมีการกล่าวถึง ความพยายามของกลุ่มคนในยุคสมัยปัจจุบันที่ต้องการนำเอาแนวคิดอินเทอร์เน็ตแห่งสรรพสิ่งเข้ามาเปลี่ยนแปลงสังคม โดยถูกคาดการณ์ว่าจะเข้ามาทำหน้าที่เป็นโครงสร้างพื้นฐานสำหรับการใช้ชีวิตประจำวันและการงานของผู้คนในสังคมทั้งหมดในอนาคตอันใกล้[2]

อย่างไรก็ตาม การพัฒนาเทคโนโลยีคอมพิวเตอร์นั้นก็ไม่ได้มีแต่ด้านดีเพียงอย่างเดียว ผลเสียและผลกระทบที่ตามมาจากการพัฒนาเทคโนโลยีคอมพิวเตอร์ ก่อให้เกิดปัญหาอาชญากรรมไซเบอร์ตามขึ้นมาอย่างหลีกเลี่ยงไม่ได้ โดย Samuel Greengard ยังได้กล่าวต่อไปถึงสาเหตุของปัญหาดังกล่าว โดยให้เหตุผลว่าปัญหามาจากช่องโหว่ของระบบอินเทอร์เน็ต ที่ขาดการออกแบบระบบความมั่นคงปลอดภัยทางไซเบอร์ที่เหมาะสมมาตั้งแต่เริ่มต้น ซึ่งสถานการณ์ในปัจจุบันผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางไซเบอร์เสมือนกำลังเล่นไล่จับกับอาชญากรไซเบอร์ เมื่อมีภัยคุกคามหรือจุดบกพร่องในรูปแบบใหม่ ๆ ทีมจัดการความมั่นคงปลอดภัยทางไซเบอร์ก็จะสืบเสาะหารอยรั่วและรีบอุดรูรั่วนั้นทันที สถานการณ์นี้ทำให้เกิดเครื่องมือ วิธีการ และเทคนิคที่ผสมผสานกัน ซึ่งเป็นที่ทราบกันดีว่า ไม่มีวิธีการใดวิธีการหนึ่งที่จะสามารถแก้ไขปัญหาได้อย่างเบ็ดเสร็จ โดยในทุกวันนี้การจัดการความมั่นคงปลอดภัยทางไซเบอร์ต้องใช้การผสมผสานเครื่องมือทั้งไฟร์วอลล์ ระบบตรวจจับมัลแวร์ การรักษาความปลอดภัยที่อุปกรณ์ปลายทาง การเข้ารหัส ระบบจัดการพาสเวิร์ด รวมทั้งการเฝ้าระวังเครือข่ายและวิธีการอื่น ๆ ร่วมไปด้วยกัน[3]

---

[2] ซามูเอล กรีนการ์ด, The Internet of Things: อินเทอร์เน็ตแห่งสรรพสิ่ง แปลโดยทีปกร วุฒิพิทยามงคล (กรุงเทพฯ: สำนักพิมพ์ โอเพ่นเวิลด์ส, 2560). หน้า 12.

[3] เรื่องเดียวกัน หน้า 146-147.

สถานการณ์ในปัจจุบันปัญหาอาชญากรรมไซเบอร์ได้เพิ่มพูนจำนวนและความรุนแรงมากขึ้นเรื่อย ๆ ซึ่งจะเห็นได้จากจำนวนตัวเลขสถิติการก่ออาชญากรรมทางไซเบอร์ทั่วโลก ที่ยังคงเดินหน้าสร้างสถิติเพิ่มจำนวนสูงขึ้นเรื่อย ๆ ในทุกวินาทีที่หมุนไปจะมีการโจมตีทางไซเบอร์บนพื้นที่โลกไซเบอร์อยู่ตลอดเวลา โดยสามารถติดตามได้จากแหล่งข้อมูลสาธารณะที่น่าเชื่อถือ ในที่นี้ผู้วิจัยจะขอยกตัวอย่างรายงานสถานการณ์สถิติการโจมตีทางไซเบอร์บนเว็บไซต์ของบริษัทแคสเปอร์สกี้[4] บริษัทผู้ผลิตซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์จากประเทศรัสเซีย โดยในรายงานสถิติบนเว็บไซต์จะแสดงการรายงานข้อมูลการตรวจจับการโจมตีทางไซเบอร์จากโปรแกรมแอนตี้ไวรัส ที่ติดตั้งอยู่บนระบบเครื่องคอมพิวเตอร์ของผู้ใช้บริการทั่วโลก ซึ่งจะมีการรายงานผลข้อมูลตัวเลขด้วยระบบเรียลไทม์ (Real-Time System) เพื่อแสดงให้เห็นถึงรายละเอียดการเคลื่อนไหวของข้อมูลตัวเลขการถูกโจมตีในระดับวินาที

ตัวอย่างสถิติข้อมูลจากแหล่งข้อมูลดังกล่าว ณ วันที่ 15 กันยายน 2561 ได้มีการรายงานข้อมูลไว้ว่า ประเทศที่ถูกโจมตีทางไซเบอร์มากที่สุด 5 อันดับแรก คือ เวียดนาม รัสเซีย เยอรมัน สหรัฐอเมริกา และจีน ตามลำดับ ในส่วนของประเทศไทยนั้นมีการถูกโจมตีทางไซเบอร์ติดอยู่ในอันดับที่ 15 ของโลก ซึ่งยังถือว่าอยู่ในระดับที่สูง โดยประเภทของไวรัสคอมพิวเตอร์ที่เข้ามาโจมตีในประเทศไทยสูงที่สุดประจำเดือน สิงหาคม 2561 มีชื่อเรียกว่า“HACKTOOL.WIN64.HACKKMS” มีสัดส่วนการเข้าโจมตีอยู่ที่ 33.42 % ของจำนวนไวรัสคอมพิวเตอร์ทั้งหมด จากการเก็บรวบรวมจำนวนตัวเลขสถิติที่เก็บได้เฉพาะในประเทศไทยมีอัตราเฉลี่ยการตรวจจับการโจมตีอยู่ที่ประมาณ 180,000 – 200,000 ครั้งต่อวัน

ลำดับ	ชื่อไวรัสคอมพิวเตอร์	สัดส่วนการโจมตี
1	HACKTOOL.WIN64.HACKKMS	33.42 %
2	DANGEROUSOBJECT.MULTI.GENERIC	10.87 %
3	TROJAN.WINLNK.STARTER	6.20 %
4	TROJAN.WINLNK.RUNNER	4.50 %
5	TROJAN.SCRIPT.GENERIC	3.13 %

ตารางที่ 1 สัดส่วนไวรัสคอมพิวเตอร์ที่ถูกปล่อยเข้ามาโจมตีทางไซเบอร์ในประเทศไทย

[4] Kaspersky Lab, **Cyberthreat Real-Time Map** [Online], 26 December 2017. Source https://cybermap.kaspersky.com

อย่างไรก็ตามสถิติการโจมตีที่แสดงอยู่บนเว็บไซต์เป็นเพียงการเก็บข้อมูลจากผู้ใช้บริการซอฟต์แวร์แคสเปอร์สกี้เพียงเท่านั้น แต่ยังมีข้อมูลที่ไม่ได้ถูกเก็บรวบรวมไว้หรือไม่สามารถเก็บรวบรวมไว้เป็นสถิติได้ ซึ่งเป็นสิ่งที่เป็นข้อจำกัดหลักในการนำเอาสถิติมาใช้ในการศึกษาวิจัย อีกทั้งข้อมูลเหล่านี้ในหลายองค์กรมักจะยอมปกปิดตัวเลขการถูกโจมตีเอาไว้เป็นความลับ เพื่อที่จะรักษาชื่อเสียงและความเชื่อมั่นขององค์กรไว้ ปัญหาการจัดเก็บข้อมูลทางสถิติยังคงเป็นประเด็นที่ถูกตั้งคำถามถึงแม้ว่าจะมีการจำกัดขอบเขตในการศึกษาแล้วก็ตาม แต่ก็ยังไม่สามารถจัดเก็บข้อมูลได้อย่างสมบูรณ์จากปัญหาข้างต้นส่งผลให้การศึกษาวิจัยในปัจจุบัน ทำได้เพียงจัดเก็บข้อมูลทางสถิติให้ได้ใกล้เคียงกับข้อมูลที่แท้จริงให้มากที่สุด โดยจำนวนตัวเลขสถิติที่ยังคงแอบซ่อนอยู่หลังฉากเหล่านี้ ในการศึกษาอาชญาวิทยาให้คำนิยามว่าเป็น “ตัวเลขมืดของอาชญากรรม” (The Dark Figure of Crime)[5]

2.1.1 นิยามของอาชญากรรมไซเบอร์

นอกเหนือจากปัญหาด้านการจัดเก็บข้อมูลด้านสถิติแล้วนั้น ปัญหาการให้คำนิยามจำกัดความอาชญากรรมไซเบอร์ ดูเหมือนจะเป็นประเด็นที่มีต้องกลับมาทบทวนกันอีกครั้ง เนื่องจากปัจจุบันอาชญากรรมไซเบอร์ได้ปรับเปลี่ยนรูปแบบไปจากในอดีต เป็นอาชญากรรมที่ไม่ได้มีรูปแบบตายตัว มีการปรับเปลี่ยนรูปแบบอยู่เสมอตามการพัฒนาเทคโนโลยีคอมพิวเตอร์ ส่งผลให้การให้คำนิยามที่ชัดเจนครอบคลุมเป็นไปด้วยความยากลำบาก แต่ถึงกระนั้นก็ตามได้มีการให้คำนิยามจากบรรดานักวิชาการและองค์กรที่มีส่วนเกี่ยวข้องไว้อย่างหลากหลาย

เริ่มต้นจากการให้คำนิยามในยุคแรกของปัญหาอาชญากรรมไซเบอร์ หรือ ในช่วงปีพุทธศักราช 2519 นำโดย Don B. Parker ชาวสหรัฐอเมริกา ผู้ที่ได้ชื่อว่าเป็นบิดาแห่งอาชญากรรมคอมพิวเตอร์ (ชื่อเรียกอาชญากรรมไซเบอร์ในยุคนั้น) ได้นิยามถึงถึงการกระทำความผิดทางคอมพิวเตอร์ไว้ในหนังสือ Crime by Computer ไว้ว่า

“การกระทำความผิดทางคอมพิวเตอร์ หรือ การใช้คอมพิวเตอร์ในทางที่ผิด (Computer abuse) สามารถตีความหมายได้แบบกว้าง คือ การกระทำใด ๆ ก็ตามที่ได้นำเอาเทคโนโลยีทางคอมพิวเตอร์ เข้าไปมีส่วนในการกระทำจนเป็นเหตุให้เหยื่อต้องได้รับความเสียหาย หรือ เกิดความสูญเสีย และการกระทำดังกล่าวนั้นเป็นการกระทำที่เกิดขึ้นโดยเจตนาของผู้กระ ทำความผิด หรือ

[5] LawTeacher, **The Dark Figure of Crime** [Online], 26 December 2017. Source https://www.lawteacher.net/free-law-essays/criminology/the-dark-figure-of-crime.php

กระทำไปเพื่อให้ได้รับประโยชน์จากการกระทำความผิดนั้น – 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."[6]

นอกจากการให้คำนิยามข้างต้นแล้ว ในปีพุทธศักราช 2522 ในขณะที่ Don B. Parker ได้ดำรงตำแหน่งเป็น Senior Computer Security Consultant ของ Stanford Research Institute International (SRI) เขาได้ร่วมกับทีมวิจัยเขียนคู่มือการออกกฎหมายควบคุมปัญหาอาชญากรรมบนคอมพิวเตอร์ (Computer Crime: Criminal Justice Resource Manual) ซึ่งในคู่มือเล่มดังกล่าวได้มีการให้นิยามถึงการกระทำความผิดทางคอมพิวเตอร์เอาไว้ว่า

"การกระทำใด ๆ ก็ตามที่กฎหมายได้ระบุไว้ว่าเป็นความผิด ซึ่งการกระทำนั้นเป็นการกระทำที่ต้องอาศัยความรู้ทางด้านเทคโนโลยีคอมพิวเตอร์ เพื่อประกอบความผิดนั้นให้สำเร็จลุล่วง - Any illegal act for which knowledge of computer technology is essential for its successful prosecution"[7]

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

---

[6] Don B. Parker, Crime by Computer (New York: Charles Scribner's Sons, 1976), p.12.

[7] วรณัฐ บุญเจริญ, "มาตรการทางกฎหมายของอาเซียนเพื่อการคุ้มครองและป้องกันอาชญากรรมทางคอมพิวเตอร์," (วิทยานิพนธ์ปริญญานิติศาสตรมหาบัณฑิต สำนักวิชานิติศาสตร์ มหาวิทยาลัยแม่ฟ้าหลวง,2557).

“อาชญากรรมไซเบอร์เป็นอาชญากรรมที่มีความเกี่ยวข้องกับคอมพิวเตอร์และเครือข่ายระบบคอมพิวเตอร์ โดยทั่วไปแล้วหมายถึงการกระทำที่อาชญากรใช้ระบบอินเทอร์เน็ต หรือ 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 systems to cause harm to others or some from of a disturbance.”[8]

โดยคำนิยามจำกัดความข้างต้นสอดคล้องกับความคิดเห็นของ Brian K. Payne ที่ได้กล่าวถึงในหนังสือ White - Collar Crime เอาไว้ว่า

“อาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์ หมายถึง ประเภทของอาชญากรรมที่มีความเกี่ยวข้องกับการใช้คอมพิวเตอร์ ในการกระทำความผิดตามกฎหมาย หรือ กระทำอันตรายอื่น ๆ ต่อระบบคอมพิวเตอร์ ซึ่งในกรณีนี้รวมถึงการที่ระบบคอมพิวเตอร์ตกเป็นเป้าหมายในการถูกโจมตี หรือ ระบบคอมพิวเตอร์ถูกนำมาใช้เป็นเครื่องมือในการประกอบอาชญากรรม หรือ การกระทำที่ส่งผลกระทบจนก่อให้เกิดอาชญากรรม – The terms computer crime and cybercrime refer to a range of computer – related behaviors that are criminally illegal or otherwise harmful. In case of computer crime, the computer is either a target of the offense or a tool for the crime or is incidental to the crime.”[9]

โดยสรุปผู้วิจัยขอให้คำนิยามจำกัดความอาชญากรรมไซเบอร์เอาไว้ว่า

“อาชญากรรมไซเบอร์ หมายถึง การประกอบอาชญากรรมที่ได้นำเอาเทคโนโลยีคอมพิวเตอร์มาเป็นเครื่องมือในการกระทำความผิด หรือ การกระทำความผิดใดก็ตามที่สร้างความเสียหายต่อระบบคอมพิวเตอร์ทั้งทางตรงและทางอ้อม โดยการกระทำนั้นกฎหมายได้ระบุไว้ว่าเป็นความผิด”

2.1.2 รูปแบบของอาชญากรรมไซเบอร์

จากเนื้อหาในส่วนการให้คำนิยามจำกัดความข้างต้น ทำให้เราทราบว่าอาชญากรรมไซเบอร์มีขอบเขตการจำกัดความที่กว้างครอบคลุมไปยังการกระทำผิดในหลากหลายรูปแบบ ด้วยเหตุนี้จึง

---

[8] Joshua B. Hill and Nancy E. Marion, Introduction to Cybercrime (California: ABC –CLIO LLC, 2016), p.5.

[9] Brian K. Payne, White - Collar Crime (California: SAGE Publication, Inc., 2017), p.165.

ต้องมีการจำแนกรูปแบบอาชญากรรมไซเบอร์ตามลักษณะการกระทำผิดต่าง ๆเพื่อใช้เป็นแนวทางในการศึกษาทำความเข้าใจในวิธีการของอาชญากรรมไซเบอร์แต่ละลักษณะ

โดยจากการศึกษาค้นคว้าข้อมูล พบว่า มีการแบ่งประเภทรูปแบบอาชญากรรมไซเบอร์ออกเป็นกลุ่มตามลักษณะของการกระทำผิด ดังนี้

ประเภทที่ 1 ลักษณะความผิดประเภทบุกรุกเข้าสู่ระบบคอมพิวเตอร์

การลักลอบเข้าสู่ระบบคอมพิวเตอร์ (Hacking) หมายถึง การเข้าสู่ระบบคอมพิวเตอร์โดยที่ไม่ได้รับอนุญาต หรือ การเข้าสู่ระบบคอมพิวเตอร์อย่างผิดกฎหมาย จากผู้กระทำความผิดที่มีความรู้ในทักษะด้านระบบคอมพิวเตอร์ ซึ่งถูกเรียกว่า แฮกเกอร์ (Hacker)[10] โดยสาเหตุที่เป็นปัจจัยกระตุ้นให้เกิดการกระทำของเหล่าแฮกเกอร์ จะเกิดขึ้นได้ทั้งจากความอยากทดลองอยากเรียนรู้ในระบบคอมพิวเตอร์ ซึ่งการสามารถเจาะเข้าสู่ระบบคอมพิวเตอร์ถือได้ว่าเป็นความท้าทายอย่างหนึ่งของเหล่าแฮกเกอร์ หรือ มาจากความต้องการแสวงหาผลประโยชน์ที่ได้จากการลักลอบเข้าสู่ระบบคอมพิวเตอร์ ซึ่งมักจะมารูปแบบของการจารกรรมข้อมูล (Data Espionage) ที่ถูกเก็บไว้บนระบบคอมพิวเตอร์ หรือ อยู่ในรูปแบบของการดักจับข้อมูล (Sniffing) ในระหว่างการส่งข้อมูล โดยเหยื่อมักจะไม่รู้ตัวว่าได้ถูกล้วงเอาข้อมูลส่วนตัวออกไป เหยื่อจะรู้ตัวก็ต่อเมื่อถูกนำเอาข้อมูลไปสร้างความเสียหายไปแล้ว

การก่อกวนระบบคอมพิวเตอร์ หมายถึง การกระทำใดก็ตามที่ก่อให้เกิดความผิดปกติต่อระบบคอมพิวเตอร์ เช่น การใช้มัลแวร์ (Malware) ตัวมัลแวร์เป็นรูปแบบโปรแกรมที่ถูกสร้างมาเพื่อแฝงตัวเข้าไปในระบบคอมพิวเตอร์ โดยจะหลบซ่อนอยู่ในระบบคอมพิวเตอร์ของเหยื่อ ซึ่งมัลแวร์ในปัจจุบันมีรูปแบบที่หลากหลายตามแต่จะกำหนดไว้ อาทิ กลุ่มสปายแวร์ (Spyware) จะทำหน้าที่ฝังตัวเก็บข้อมูลบนระบบคอมพิวเตอร์ แล้วส่งข้อมูลกลับมาให้กลุ่มแฮกเกอร์ ในบางกรณีอาจจะทำงานร่วมกับโปรแกรม Keyloggers เพื่อดักจับข้อมูลบนแป้นพิมพ์ โดยเฉพาะข้อมูลส่วนตัว รหัสผ่านอีเมล์ และข้อมูลการดำเนินธุรกรรมทางการเงินต่าง ๆ กลุ่มคอมพิวเตอร์ไวรัส (Virus) จะสร้างความผิดปกติบนระบบคอมพิวเตอร์ เพื่อก่อความรำคาญให้กับเหยื่อ กลุ่ม Ransomware จะสั่งการให้ระบบคอมพิวเตอร์ของเหยื่อหยุดการทำงานหรือเข้ารหัสในไฟล์งาน เพื่อเรียกค่าไถ่ในการปลดล็อคระบบคอมพิวเตอร์[11] กลุ่ม Rootkit จะสามารถเข้าควบคุมเครื่องคอมพิวเตอร์ หรือ เข้าใช้งานเครื่องที่ถูก

---

[10] Joshua B. Hill and Nancy E. Marion, Introduction to Cybercrime (California: ABC –CLIO LLC, 2016), p.61.

[11] Brian K. Payne, White - Collar Crime (California: SAGE Publication, Inc., 2017), p.167.

ติดตั้งได้จากระยะไกล อีกหนึ่งวิธีการก่อกวนระบบที่พบได้บ่อยครั้ง เป็นการโจมตีระบบด้วยวิธีการ Distributed denial-of-service (DDoS) การโจมตีด้วยวิธี DDoS จะพุ่งเป้าโจมตีไปยังเว็บไซต์หรือผู้ให้บริการโดยอาศัยการใช้อุปกรณ์คอมพิวเตอร์จำนวนมากเข้าใช้บริการในระบบพร้อม ๆ กัน ซึ่งจะส่งผลให้การจราจรบนระบบเซิฟเวอร์ไม่สามารถรองรับจำนวนผู้ให้บริการได้เพียงพอ จนเป็นเหตุให้เกิดความขัดข้องของระบบชั่วคราว[12]

ประเภทที่ 2 ลักษณะความผิดที่มีเป้าหมายเป็นผู้ใช้งานคอมพิวเตอร์

การใช้เทคนิควิศวกรรมสังคม (Social Engineering) หมายถึง กระบวนการที่ผู้กระทำผิดใช้ปฏิบัติการจิตวิทยาหลอกลวงเหยื่อ เพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลหรือข้อมูลสำคัญที่สามารถนำไปใช้แสวงหาประโยชน์ โดยอาศัยจุดอ่อนจากความรู้ไม่เท่าทันเล่ห์เหลี่ยมกลโกงอาชญากรซึ่งรูปแบบของเทคนิควิศวกรรมสังคมที่พบจะมีวิธีการที่หลากหลาย บางลักษณะจะมีการผสมผสานเทคนิคด้านคอมพิวเตอร์เอาไว้ ดังปรากฏให้เห็นในรูปแบบของการฟิชชิ่ง (Phishing) ที่จะใช้เล่ห์กลหลอกให้เหยื่อเปิดเผยข้อมูลส่วนตัวผ่านช่องทางที่ถูกปลอมแปลงขึ้นมีทั้งรูปแบบอีเมล์และเว็บไซต์ โดยเหยื่อมักจะถูกหลอกให้กรอกข้อมูลประเภทรหัสผ่านหรือรายละเอียดข้อมูลส่วนตัว[13] และเมื่อได้รับข้อมูลแล้วอาชญากรไซเบอร์จะนำข้อมูลที่ได้ไปปลอมแปลงตัวตน (Identity theft) หรือกระทำการอื่นใดที่สามารถนำเอาข้อมูลเหล่านั้นไปแสวงหาผลประโยชน์ในทางที่มิชอบ ลำดับต่อมาเป็นรูปแบบการค้นข้อมูลจากถังขยะ (Dumpster Diving) โดยมีจุดมีมุ่งหมายเพื่อค้นหาข้อมูลที่ได้จดบันทึกและถูกทิ้งเอาไว้ในถังขยะ ไม่ว่าจะเป็นรหัสผ่านเลขบัญชีธนาคาร หมายเลขโทรศัพท์ผู้ติดต่อ รวมไปถึงข้อมูลสำคัญอื่น ๆ โดยทั่วไปจะเลือกใช้วิธีนี้กับเหยื่อบุคคลเป้าหมายที่มีความสำคัญสูง ซึ่งในความหมายของการค้นข้อมูลถังขยะ มีการให้นิยามรวมไปถึงการค้นข้อมูลถูกเก็บเอาไว้ในอุปกรณ์บันทึกข้อมูลทางอิเล็กทรอนิกส์ชนิดต่าง ๆ อาทิ ฮาร์ดดิสก์ (Hard Disk) ยูเอสบีแฟลชไดรฟ์ (USB Flash Drive) การ์ดหน่วยความจำ (Memory card) นอกจากนี้ยังพบรูปแบบวิศวกรรมสังคมในบางลักษณะที่ไม่มีการใช้เทคนิคคอมพิวเตอร์เข้ามาเกี่ยวข้อง อาทิ การแอบสังเกตข้อมูล (Shoulder Surfing) โดยมีรูปแบบการกระทำจากการแอบสังเกตเหยื่อในจังหวะที่เปิดเผยข้อมูลสำคัญ ไม่ว่าจะเป็นการจดด้วยกระดาษหรือกรอกข้อมูลผ่านระบบคอมพิวเตอร์ อีกหนึ่งรูปแบบที่พบได้บ่อยครั้งเป็นการหลอกลวงทางโทรศัพท์ (Telephone) โดยผู้กระทำผิดจะสุ่มหมายเลขโทรศัพท์ไปหาเหยื่อและใช้ข้อความเสียง

---

[12] William Stallings, Effective Cybersecurity (Pearson Education, Inc., 2019), p.92.

[13] Gráinne Kirwan and Andrew Power, Cybercrime (Cambridge: Cambridge University Press., 2013), p.110.

อัตโนมัติหรือแอบอ้างเป็นเจ้าหน้าที่ของหน่วยงานต่าง ๆ เพื่อลวงถามข้อมูลหรือหลอกให้ไปทำธุรกรรมทางการเงิน โดยรูปแบบที่พบบ่อยครั้งจะเป็นการหลอกลวงจากความรู้ไม่เท่าทันของเหยื่อ โดยแอบอ้างว่าบัญชีธนาคารถูกอายัดหรือเป็นหนี้บัตรเครดิต แอบอ้างว่าบัญชีเข้าไปพัวพันกับการฟอกเงินหรือค้ายาเสพติด แอบอ้างเป็นเจ้าหน้าที่ธนาคารแจ้งว่าข้อมูลส่วนตัวได้หายไปขอให้ส่งข้อมูลให้อีกครั้ง อีกทั้งยังมีในรูปแบบการหากินกับความโลภของเหยื่อ โดยหลอกว่าเป็นผู้โชคดีได้รับเงินรางวัลจากการสุ่มหรือหลอกว่าได้รับการคืนเงินภาษีคืน โดยที่เหยื่อจะต้องโอนเงินเป็นค่าธรรมเนียมไปให้ก่อน ในรูปแบบที่ยกมากล่าวไว้ในข้างต้นทั้งหมดล้วนเป็นเทคนิควิศวกรรมสังคมที่สามารถพบเห็นได้โดยทั่วไปในสังคมปัจจุบัน

ประเภทที่ 3 ลักษณะกระทำความผิดประสงค์ผลต่อรัฐ (Cybercrimes on Governments)

การก่อการร้ายทางไซเบอร์ (Cyber terrorism) หมายถึง การโจมตีเคลื่อนไหวต่อต้านรัฐบาลด้วยรูปแบบวิธีปฏิบัติการเคลื่อนไหวในทางลับ โดยการเผยแพร่ข้อมูลข่าวสารผ่านระบบคอมพิวเตอร์หรือ ใช้มัลแวร์ปฏิบัติการโจมตีเข้าสู่ระบบคอมพิวเตอร์ ซึ่งในกระบวนการโจมตีเข้าสู่ระบบจะมีการวางแผนตระเตรียมการไว้ล่วงหน้า เป้าหมายของปฏิบัติการจะมุ่งเป้าไปที่การสร้างความเสียหายต่อหน่วยงานของรัฐ หรือ ผู้สนับสนุนของรัฐ อาทิ ภาคธุรกิจธนาคาร หน่วยงานทหาร โรงผลิตกระแสไฟฟ้า ระบบการประปา ระบบวิทยุการบิน ในการโจมตีจะส่งผลให้หน่วยงานดังกล่าวจำต้องยุติการให้บริการเป็นการชั่วคราว ผลกระทบที่ตามมาจากปฏิบัติการจะส่งผลให้ผู้คนสังคมเกิดความตื่นตระหนกหวาดกลัว สูญเสียความเชื่อมั่นในเรื่องของมาตรการความปลอดภัยของรัฐบาล[14]

2.1.3 ความสัมพันธ์กับอาชญากรรมเศรษฐกิจ

ปัญหาอาชญากรรมไซเบอร์ได้มีการขยายตัวเข้าสู่สังคมครอบคลุมในทุกมิติ ซึ่งผลจากการขยายตัวดังกล่าวนั้น ได้ก่อให้เกิดความสัมพันธ์ที่ทับซ้อนระหว่างอาชญากรรมไซเบอร์และอาชญากรรมในรูปแบบอื่น ๆ ไปพร้อมกัน โดยในการศึกษาวิจัยครั้งนี้ผู้วิจัยจะขอกล่าวถึงประเด็นความสัมพันธ์ระหว่างอาชญากรรมไซเบอร์และอาชญากรรมเศรษฐกิจเป็นเนื้อหาหลัก เพื่อเป็นการกระชับเนื้อหาให้อยู่ในกรอบตามที่ได้กำหนดไว้เป็นขอบเขตของการวิจัยเท่านั้น

---

[14] Joshua B. Hill and Nancy E. Marion, Introduction to Cybercrime (California: ABC –CLIO LLC, 2016), p.82.

อาชญากรรมเศรษฐกิจเป็นรูปแบบของอาชญากรรมจำพวกหนึ่งที่ได้รับผลกระทบจากการเข้ามาของอาชญากรรมไซเบอร์ ความเป็นมาของปัญหาอาชญากรรมเศรษฐกิจนั้นเริ่มถูกกล่าวถึงในสังคมราวตอนต้นศตวรรษที่ 19 โดยเริ่มต้นจากการเกิดขึ้นของอาชญากรรมรูปแบบใหม่ ๆ ที่เริ่มปรากฏให้เห็นในวงการธุรกิจการเงินการธนาคาร อาทิ ความผิดเกี่ยวกับเช็ค การฉ้อโกง การปลอมแปลงเอกสาร และการปลอมแปลงเงินตรา ซึ่งได้ส่งผลกระทบต่อระบบเศรษฐกิจในขณะนั้นเป็นอย่างมาก ประกอบกับในยุคสมัยดังกล่าวยังไม่มีการร่างกฎหมายที่สามารถนำมาบังคับใช้ควบคุมปัญหาอาชญากรรมเศรษฐกิจได้อย่างเหมาะสม ส่งผลให้นักวิชาการจากหลากหลายสาขา อาทิ นักอาชญาวิทยา นักสังคมวิทยา และนักกฎหมาย ได้เริ่มทำการศึกษาถึงต้นตอสาเหตุของปัญหาอาชญากรรมเศรษฐกิจที่เกิดขึ้น โดยนักอาชญาวิทยาที่มีชื่อเสียงที่สุดในยุคอย่าง Edwin Sutherland ได้ศึกษาและให้คำนิยามอาชญากรรมเศรษฐกิจเอาไว้ว่า “เป็นการกระทำความผิดทางอาญาหรือกฎหมายอื่น ๆ จากบุคคลที่มีสถานภาพทางเศรษฐกิจ โดยอาศัยความสัมพันธ์ทางอาชีพของเขาเหล่านั้นและความผิดดังกล่าวก่อให้เกิดความเสียหายต่อวงการธุรกิจตลอดจนระบบเศรษฐกิจของประเทศ”[15] จากคำนิยามข้างต้นชี้ให้เห็นว่า อาชญากรรมเศรษฐกิจมีการให้คำนิยามไว้แบบกว้าง ๆ ครอบคลุมการกระทำความผิดในทุกลักษณะที่มีส่วนเกี่ยวข้องและสร้างความเสียหายต่อระบบเศรษฐกิจ

อาชญากรรมเศรษฐกิจนั้น จัดว่าเป็นอาชญากรรมที่มีความเฉพาะตัว ผู้กระทำผิดจะเป็นผู้ที่มีความรู้ความสามารถเฉพาะทางในระดับสูง ซึ่งจะมีความแตกต่างจากอาชญากรรมในประเภทอื่น ๆ การกระทำความผิดทางเศรษฐกิจถูกเรียกในชื่อที่แตกต่างกัน ตามแต่ลักษณะรูปแบบการประกอบอาชญากรรม อาทิ อาชญากรรมคอปกขาว (White Collar Crime) อาชญากรรมทางธุรกิจ (Business Crime) อาชญากรรมทางการพาณิชย์ (Commercial Crime) และอาชญากรรมทางการเงิน (Financial Crime) ซึ่งการกระทำความผิดทั้งหมดข้างต้นล้วนมีความหมายอยู่ในลักษณะเดียวกัน คือ เป็นการประกอบความผิดโดยมีวัตถุประสงค์เพื่อให้ได้มาซึ่งผลกำไรหรือผลประโยชน์ทางเศรษฐกิจ โดยเป็นการกระทำผิดต่อกฎหมายเกี่ยวกับการพาณิชย์อันจะมีผลกระทบต่อระบบเศรษฐกิจและความมั่นคงของประเทศ เพื่อให้ครอบคลุมถึงการกระทำความผิดทางเศรษฐกิจทั้งหมด[16]

---

[15] ชญานิศ ภาชีรัตน์, “อาชญากรรมเศรษฐกิจที่เกี่ยวกับสถาบันการเงิน: ศึกษากรณีเปรียบเทียบมาตรการในการบังคับใช้กฎหมายของต่างประเทศและประเทศไทย,” (วิทยานิพนธ์ปริญญานิติศาสตรมหาบัณฑิต สาขาวิชานิติศาสตร์ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย,2543).

[16] วีระพงษ์ บุญโญภาส, อาชญากรรมทางเศรษฐกิจ (กรุงเทพ: สำนักพิมพ์นิติธรรม, 2549). หน้า 5-6.

จากการศึกษาข้อมูลทำให้ผู้วิจัยได้เห็นถึงจุดเด่นที่เป็นลักษณะเฉพาะของอาชญากรรมเศรษฐกิจ ซึ่งลักษณะเฉพาะที่ผ่านการศึกษาวิเคราะห์จากนักวิชาการได้มีการจำแนกออกเป็นหลากหลายประการ ตามแต่ลักษณะของการกระทำผิดที่แตกต่างกันออกไป โดยในส่วนนี้ผู้วิจัยได้รวบรวมลักษณะเฉพาะอาชญากรรมเศรษฐกิจมาสรุปไว้ดังต่อไปนี้

ลักษณะที่ 1 มีการปกปิดการกระทำความผิดและพยายามทำลายหลักฐาน เพื่อไม่ให้มีหลักฐานผูกมัดตน ทั้งนี้อาชญากรรมเศรษฐกิจจะมีความสลับซับซ้อนและมีการกระทำแบบค่อยเป็นค่อยไปต้องใช้ระยะเวลาพอสมควรจึงจะรู้ถึงความเสียหาย ทำให้การค้นหาหลักฐานเป็นไปด้วยความยากลำบากไม่ทันต่อเหตุการณ์ อันเป็นการเปิดโอกาสให้อาชญากรรมประเภทนี้ สามารถปกปิดทำลายซ่อนเร้นหลักฐานได้เป็นอย่างดี ด้วยอำนาจเงินที่ได้มาจากการกระทำความผิดทางเศรษฐกิจก่อให้เกิดอิทธิพลมืดในการปิดปากพยาน ติดสินบนเจ้าพนักงานตำรวจและเจ้าพนักงานของรัฐ รวมทั้งการจ้างผู้อื่นให้รับสารภาพแทน จึงยากที่จะทำลายได้ถึงแหล่งต้นตอที่แท้จริง[17]

ลักษณะที่ 2 เนื่องจากพฤติกรรมการกระทำที่มีลักษณะซ่อนเร้น แอบแฝง สังเกตเห็นหรือพบความผิดได้ยาก บางครั้งผู้ถูกกระทำไม่ได้รู้สึกตัวว่าตัวเองกำลังถูกกระทำหรือตกเป็นเหยื่อ ซึ่งกว่าจะรู้ตัวก็ต่อเมื่อเกิดผลขึ้นแล้ว ประกอบกับไม่มีภาพพจน์ที่เขย่าขวัญประชาชน ไม่มีลักษณะสร้างความหวาดกลัว คุกคามหรือข่มขวัญในส่วนที่เกี่ยวข้องกับชีวิตผู้ถูกกระทำโดยตรง ทำให้ผู้เสียหายไม่รู้สึกตัวว่าตนได้ตกเป็นเหยื่อของอาชญากรรมแล้ว แต่กลับคิดว่าเป็นการเสียเปรียบทางในเรื่องธุรกิจการค้าปกติเท่านั้น ทัศนคติ ค่านิยมของผู้ถูกกระทำจึงมีความรู้สึกต่อต้านไม่รุนแรงเทียบเท่าอาชญากรรมธรรมดาและไม่สร้างความโกรธแค้นให้กับผู้พบเห็น[18]

ลักษณะที่ 3 มีความรู้ความชำนาญ มีการใช้เทคโนโลยีที่ทันสมัย ไม่ว่าจะเป็นในด้านการจัดการหรือการจัดฉาก มีการใช้เครื่องมือเข้าช่วย เช่น คอมพิวเตอร์ เอกสารทางการค้า ประกอบกับมีการตระเตรียมวางแผนอย่างดี การกระทำผิดจะดำเนินการกันอย่างเป็นระบบ มีการศึกษาหาข้อมูลวางแผนและจัดการเรื่องอื่นไว้พร้อมสรรพ จึงยากต่อการสืบสวนสอบสวน จับกุม ผู้กระทำความผิด[19]

ลักษณะที่ 4 การกระทำผิดส่วนใหญ่มักจะดำเนินการเป็นกลุ่ม รวมทั้งมีประชาชน เข้าร่วมทั้งโดยรู้ตัวและไม่รู้ตัวจนเชื่อมโยงเป็นขบวนการในระดับท้องถิ่นและระดับชาติ อีกทั้งยังมีแนวโน้มจะ

[17] เรื่องเดียวกัน, หน้า 12.

[18] เรื่องเดียวกัน, หน้า 12.

[19] เรื่องเดียวกัน, หน้า 12.

รวมกันเป็นองค์กรอาชญากรรม (Organization Crime) และขยายตัวออกเป็นอาชญากรรมข้ามชาติ (Transnational Crime)[20]

ลักษณะที่ 5 มีลักษณะเป็นอันตรายต่อความผาสุกและสวัสดิภาพของประชาชน อีกทั้งยังก่อให้เกิดความเสียหายที่มีมูลค่ามากกว่าอาชญากรรมพื้นฐาน จำนวนผู้เสียหายในแต่ละครั้งมีเป็นจำนวนมาก ซึ่งนอกจากมีลักษณะของการทำร้ายประชาชนทั่วไปแล้ว อาจกล่าวได้ว่ารัฐก็นับว่าเป็นผู้เสียหายด้วยเช่นกัน เพราะอาชญากรรมเศรษฐกิจทำลายการลงทุน ขัดขวางการพัฒนาเติบโตทางสังคมและในแง่ของความมั่นคงซึ่งบางลักษณะมีผลส่งไปถึงการทำลายศีลธรรม ประเพณี และวัฒนธรรมของสังคมชาติด้วย[21]

เมื่อได้ศึกษาถึงภาพรวมลักษณะของอาชญากรรมเศรษฐกิจจะพบว่า ลักษณะเด่นนั้นมีความคล้ายคลึงกับอาชญากรรมไซเบอร์เป็นอย่างมาก ซึ่งเป็นเรื่องยากที่จะชี้ชัดให้เห็นถึงความแตกต่างระหว่างอาชญากรรมเศรษฐกิจและอาชญากรรมไซเบอร์ ในบางกรณีที่เหล่าอาชญากรมีการนำเอาเครื่องมือทางคอมพิวเตอร์ หรือ ใช้ช่องทางระบบคอมพิวเตอร์มากระทำความผิด จะทำให้เราไม่สามารถแยกอาชญากรรมทั้งสองประเภทนั้นออกมาจากกันได้ เนื่องจากอาชญากรรมทั้งสองประเภทมีความสัมพันธ์ต่อกัน ซึ่งอาชญากรรมเศรษฐกิจในยุคสมัยใหม่ล้วนแต่นำเอาเทคโนโลยีคอมพิวเตอร์มาเป็นเครื่องมือในการกระทำความผิด[22]

2.2 แนวคิดการป้องกันอาชญากรรมไซเบอร์และมาตรการความมั่นคงปลอดภัยทางไซเบอร์

2.2.1 แนวคิดการป้องกันอาชญากรรมไซเบอร์

การป้องกันอาชญากรรมไซเบอร์ (Cybercrime Prevention) เป็นสิ่งสำคัญที่สังคมต้องตระหนักถึงและให้ความสำคัญ โดยเฉพาะอย่างยิ่งในสถานการณ์ปัจจุบันการเติบโตอย่างรวดเร็วของอาชญากรรมไซเบอร์ที่แพร่ขยายตัวจนกลายเป็นปัญหาสำคัญในระดับโลก ได้ส่งผลร้ายจนทำให้สังคมทั่วโลกเริ่มหันมามองหาแนวการป้องกันอาชญากรรมที่สามารถต่อกรกับอาชญากรไซเบอร์ได้อย่างทันท่วงทีและมีประสิทธิภาพ โดยภาพในมุมมองของสังคมทั่วไปการเข้ามาจัดการปัญหาอาชญากรรมไซเบอร์ ถูกมองว่าเป็นหน้าที่ของภาครัฐที่จะต้องใช้อำนาจในฐานะตัวแทนสังคม เพื่อเข้าควบคุม

---

[20] เรื่องเดียวกัน, หน้า 12.

[21] เรื่องเดียวกัน, หน้า 12.

[22] Russell G. Smith, Peter Grabosky and Gregor Urbas, Cyber Criminals on Trial. (Cambridge: Cambridge University Press, 2004), p.9.

สถานการณ์และแก้ไขปัญหาที่เกิดขึ้น โดยเริ่มจากการวิเคราะห์ถึงสภาพปัญหาที่เกิดขึ้นจริงร่วมกับศึกษาถึงระเบียบข้อกฎหมายที่รัฐได้ออกมาบังคับใช้อยู่เดิม เพื่อวิเคราะห์ถึงปัญหาการบังคับใช้กฎหมายว่ามีช่องโหว่ทางกฎหมายให้เหล่าอาชญากรไซเบอร์ใช้เป็นช่องทางหลบเลี่ยงอยู่หรือไม่ หากมีจะต้องออกกฎหมายใหม่อย่างไรถึงจะนำมาบังคับใช้ได้อย่างเหมาะสม รวมไปถึงการศึกษาถึงรูปแบบมาตรการหรือแผนงานของหน่วยงานกำกับดูแลหรือภาครัฐ ที่จะต้องกำหนดออกเป็นนโยบายสาธารณะมาใช้ในสังคม

ในมิติของการกำหนดนโยบายสาธารณะ สำหรับในประเทศไทยการวางมาตรการหรือวางนโยบายเพื่อเข้าควบคุมสถานการณ์ภัยคุกคามทางไซเบอร์ ได้มีการหารือในระดับประเทศถึงความเป็นไปได้ในการปฏิบัติ ซึ่งภาครัฐได้พยายามผลักดันและกำหนดเป็นยุทธศาสตร์ที่สำคัญของประเทศ โดยรัฐบาลได้เตรียมแต่งตั้งกรรมการระดับชาติด้านความมั่นคงทางไซเบอร์[23] เพื่อผลักดันกฎหมายและยุทธศาสตร์ป้องกันภัยระดับชาติ รวมไปถึงการมีส่วนร่วมในการสร้างเครือข่ายป้องกันภัยไซเบอร์ระดับภูมิภาค และยกระดับขีดความสามารถรับมือกับภัยคุกคามทางไซเบอร์ที่มีความซับซ้อน และปรับเปลี่ยนรูปแบบอยู่ตลอดเวลา การป้องกันภัยไซเบอร์จะต้องวางมาตรการป้องกันที่ครอบคลุมในทุกภาคส่วนของสังคม อีกทั้งยังต้องมีการพัฒนากฎหมาย ที่จะมาเป็นเครื่องมือใช้ในการรองรับการป้องกันภัยไซเบอร์ รวมถึงการประสานความร่วมมือจากภาครัฐและเอกชน เพื่อทำให้เกิดความเชื่อมั่นและการป้องกันภัยคุกคามที่มีประสิทธิภาพ

โดย พล.อ.อ.ประจิน จั่นตอง รองนายกรัฐมนตรีในขณะนั้น ได้กล่าวปาฐกถาเรื่องยุทธศาสตร์ความปลอดภัยไซเบอร์ ในยุคไทยแลนด์ 4.0 เนื่องในโอกาสวันสื่อสารแห่งชาติ 2560 ไว้ว่า

> “ประเทศไทยมีความเสี่ยงในการถูกบุกรุกทางไซเบอร์ สิ่งที่น่าห่วงที่สุด คือ ภัยที่มากระทบกับความมั่นคง จึงต้องบริหารความเสี่ยงด้วยการมีหน่วยงานด้านความปลอดภัยไซเบอร์ เพื่อดูแลปัญหาและประสานงานร่วมกับต่างประเทศ การปกป้องระบบสำคัญของประเทศต้องมีเครื่องมือ มียุทธศาสตร์และกฎหมายที่มีขีดความสามารถรับมือกับภัยคุกคามได้ โดยให้มีหน่วยงานกลางเป็นคณะกรรมการระดับชาติมีนายกรัฐมนตรีเป็นประธาน การทำยุทธศาสตร์จะเน้นเป้าหมายที่ชัดเจน โดยมุ่งการป้องกันภัยคุกคามเป็นหลัก โดยจะมีแผนระยะสั้น ระยะกลาง และระยะยาว นอกจากนี้ ต้องมีโครงสร้างพื้นฐานที่ดี เพื่อมารองรับทั้งด้านพลังงานสำรอง การพัฒนาบุคคลากร การมีงบประมาณที่เพียงพอ ส่วนการป้องกันภัยระดับภูมิภาค อาเซียนจะมีการประชุมเพื่อร่างแผนยุทธศาสตร์ความมั่นคงไซเบอร์ร่วมกัน”

---

[23] “รัฐตั้งทีมป้องกันไซเบอร์ระดับชาติ,” กรุงเทพธุรกิจ (5 สิงหาคม 2560): 3.

คำกล่าวที่ยกมาข้างต้นสอดคล้องกับแนวทางการกำหนดยุทธศาสตร์ชาติ ในมิติด้านความมั่นคง โดยสำนักงานสภาความมั่นคงแห่งชาติได้กำหนดเป็นนโยบายอยู่ภายใต้แผนยุทธศาสตร์ “นโยบายความมั่นคงแห่งชาติ พ.ศ.2558 – 2564”[24] ซึ่งถูกวางไว้ในนโยบายที่ 10 หัวข้อนโยบายเสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศและไซเบอร์ รายละเอียดภายในกรอบนโยบายมีการวางนโยบายที่สอดคล้องไปในทิศทางเดียวกัน โดยมุ่งเป้าไปที่การสร้างเครือข่ายบูรณาการระหว่างหน่วยงานภาครัฐกับภาคเอกชน การพัฒนาบังคับใช้กฎหมาย และการพัฒนาศักยภาพด้านเทคโนโลยี อีกทั้งยังมีความสอดคล้องกับ “ร่างแผนยุทธศาสตร์ด้านความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ” (National Cybersecurity) ของ กสทช.[25] ที่ได้เสนอกรอบยุทธศาสตร์ เพื่อที่จะเป็นเข็มทิศในการวางแนวทางพัฒนาความมั่นคงปลอดภัยทางไซเบอร์ภายในประเทศ จากที่ยกมากล่าวในข้างต้น จะเห็นว่าการกำหนดนโยบายสาธารณะในระดับประเทศนั้น ได้เริ่มก่อตัวเป็นรูปเป็นร่างมากขึ้น จากการที่หน่วยงานภาครัฐที่ส่วนในการออกนโยบายได้ตระหนักถึงความสำคัญของการป้องกันภัยทางไซเบอร์จนร่วมกันผลักดันนโยบายออกมาสู่สังคมดังที่กล่าว

ในมิติของการปรับปรุงกฎหมาย ผู้วิจัยได้ศึกษาด้านข้อกฎหมายที่เกี่ยวข้อง พบว่า ประเทศไทยได้มีการพัฒนาข้อกฎหมาย เพื่อเตรียมการรับมือกับภัยคุกคามทางไซเบอร์ โดยจะดำเนินงานภายใต้กรอบนโยบายเศรษฐกิจดิจิทัลเพื่อเศรษฐกิจและสังคม (Digital Economy) ซึ่งภารกิจส่วนหนึ่งภายใต้กรอบนโยบายดังกล่าว คือ การจัดทำชุดร่างกฎหมายเพื่อการส่งเสริมเศรษฐกิจและสังคม หรือเรียกสั้น ๆ ว่า “ชุดกฎหมายเศรษฐกิจดิจิทัล” เพื่อรองรับการพัฒนาเศรษฐกิจดิจิทัล จำนวน 8 ฉบับ โดยมีสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. เป็นหน่วยงานหลักในการผลักดันกฎหมาย ซึ่งกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้เสนอคณะรัฐมนตรีและคณะรัฐมนตรีได้พิจารณาอนุมัติเห็นชอบในหลักการร่างกฎหมายเมื่อวันที่ 16 ธันวาคม 2557 และวันที่ 6 มกราคม 2558 ตามลำดับ[26]

---

[24] สำนักงานสภาความมั่นคงแห่งชาติ, **นโยบายความมั่นคงแห่งชาติ พ.ศ. 2558-2564** [ออนไลน์], 25 ธันวาคม 2560. แหล่งที่มา http://www.nsc.go.th/Download1/policy58.pdf

[25] สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ, **National Cybersecurity Strategy ยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ** [ออนไลน์], 6 ตุลาคม 2560. แหล่งที่มา https://www.nbtc.go.th/News/Information/National-Cybersecurity-Strategy-.aspx

[26] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), **ร่างกฎหมายเศรษฐกิจดิจิทัล** [ออนไลน์], 25 ธันวาคม 2560. แหล่งที่มา https://ictlawcenter.etda.or.th/de_laws

ในส่วนของกฎหมายที่น่าสนใจของกฎหมายชุดนี้อยู่ในส่วนของ “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560”[27] โดยมีการปรับปรุงบทบัญญัติจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่มีประเด็นปัญหาในการบังคับใช้กฎหมายให้มีความเหมาะสมต่อการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในปัจจุบันที่มีรูปแบบซับซ้อนมากขึ้นตามพัฒนาการทางเทคโนโลยีคอมพิวเตอร์ที่เปลี่ยนแปลงอย่างรวดเร็ว มีการกำหนดฐานความผิดขึ้นใหม่และแก้ไขเพิ่มเติมฐานความผิดเดิม รวมทั้งบทกำหนดโทษของความผิด อาทิ การกำหนดให้บุคคลใดก็ตามที่กระทำการอย่างหนึ่งอย่างใดกับระบบคอมพิวเตอร์ไม่ว่าจะเป็นการส่งคำสั่งเข้าไปฝังตัวเพื่อลักลอบนำข้อมูล หรือขัดขวางการทำงาน หรือสั่งทำลายระบบคอมพิวเตอร์ของผู้อื่น เป็นการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ความร้ายแรงของการกระทำผิดในลักษณะนี้จะทวีความรุนแรงมากขึ้น เมื่อกระทำต่อองค์กรหรือหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญของประเทศ เช่น ระบบของธนาคาร ระบบสาธารณูปโภค ระบบพลังงาน ระบบควบคุมการบิน ระบบของโรงพยาบาล เป็นต้น การปรับปรุงพระราชบัญญัติยังรวมไปถึงการปรับหลักกฎหมายให้เอื้อต่อการประสานความร่วมมือระหว่างประเทศ มีการปรับปรุงกระบวนการและหลักเกณฑ์ในการระงับ การเผยแพร่หรือลบข้อมูลคอมพิวเตอร์ ตลอดจนกำหนดให้มีการแก้ไขเพิ่มเติมอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ให้เหมาะสมยิ่งขึ้น

กฎหมายที่มีความน่าสนใจในอีกประเด็นเป็น “พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล”[28] ซึ่งเป็นการให้ความคุ้มครองสิทธิความเป็นส่วนตัว ในสังคมปัจจุบันมีแนวโน้มเกิดการละเมิดสิทธิในข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัวเพิ่มมากขึ้น โดยเฉพาะการนำข้อมูลส่วนบุคคลไปแสวงหาผลประโยชน์หรือนำไปเปิดเผยโดยมิชอบ หรือโดยไม่ได้รับความยินยอมจากทางเจ้าของข้อมูลเพื่อประโยชน์ในทางการค้า หรือเพื่อประโยชน์ในการนำข้อมูลส่วนบุคคลไปใช้ในการกระทำความผิด อาทิ การหลอกลวง การฉ้อโกง การหมิ่นประมาท เป็นต้น ซึ่งปัญหาเหล่านี้เมื่อได้กระทำความผิดบนโลกไซเบอร์ก็ถือได้ว่าเป็นปัญหาอาชญากรรมไซเบอร์เช่นเดียวกัน โดยปัญหานั้นย่อมส่งผลกระทบต่อความเชื่อมั่นในการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมตามนโยบายของรัฐบาล ดังนั้นจึงมีความจำเป็นที่ประเทศไทยจะต้องตราบัญญัติกฎหมายว่า ด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศเพื่อสร้างกลไกการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นมาตรฐานเดียวกันและสอดคล้องกับมาตรฐานที่เป็นสากล โดยต้องไม่สร้างภาระหน้าที่แก่ผู้เกี่ยวข้องจนกลายเป็นข้อจำกัด หรืออุปสรรค

---

[27] **พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พุทธศักราช 2560**.

[28] **พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562.**

ในการประกอบธุรกิจการค้าหรือการให้บริการของภาคส่วนต่าง ๆ จนเกินสมควร เพื่อแก้ไขปัญหาการละเมิดข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพ

ในมิติของการจัดตั้งหน่วยงานที่จะเข้ามากำกับดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์ พบว่า ขณะนี้ประเทศไทยได้มีการจัดตั้งหน่วยงานที่เข้ามามีส่วนรับผิดชอบดูแลปัญหาภัยคุกคามทางไซเบอร์โดยตรง เป็นหน่วยงานที่มีชื่อว่า “คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” หรือเรียกโดยย่อในภาษาไทยว่า “กมช.” และใช้ชื่อเรียกในภาษาอังกฤษว่า “National Cybersecurity Committee” เรียกโดยย่อว่า “NCSC” ขึ้นเป็นหน่วยงานของรัฐที่มีฐานะเป็นนิติบุคคล แต่ไม่เป็นส่วนราชการและรัฐวิสาหกิจ โดยมีนายกรัฐมนตรีเป็นประธานกรรมการ ในส่วนของบทบาทหน้าที่ได้กำหนดไว้ให้เข้ามาเป็นหน่วยงานหลักของภาครัฐ ในการกำหนดแนวทางและมาตรการตอบสนองและรับมือกับภัยคุกคามไซเบอร์ จัดทำแผนปฏิบัติการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติจัดทำรายงานสรุปผลการดำเนินงานที่มีผลกระทบอย่างมีนัยสำคัญ พร้อมทั้งรายงานสถานการณ์ให้สภาความมั่นคงแห่งชาติและคณะรัฐมนตรีรับทราบ ทั้งนี้การจัดตั้งหน่วยงานดังกล่าวมีการบัญญัติเอาไว้ใน “พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์” ซึ่งพระราชบัญญัติดังกล่าวได้ประกาศในราชกิจจานุเบกษา เมื่อวันที่ 27 พฤษภาคม 2562[29]

2.2.2 มาตรการความมั่นคงปลอดภัยทางไซเบอร์

คำนิยามของมาตรการความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) ได้มีการให้คำนิยามเอาไว้อย่างกว้าง ๆ ว่า หมายถึง ชุดเครื่องมือใด ๆ ก็ตามที่ถูกนำออกมาใช้ในการป้องกันสภาพแวดล้อมบนโลกไซเบอร์ โดยเครื่องมือเหล่านั้นจะอยู่ในรูปแบบที่หลากหลาย ไม่ว่าจะอยู่ในรูปของนโยบาย แนวทางการปฏิบัติ แนวคิดด้านการรักษาความปลอดภัย การบริหารจัดการความเสี่ยง ระเบียบหลักเกณฑ์ ข้อบังคับ กฎหมาย การฝึกอบรม การประกันภัย และการจัดการระบบเทคโนโลยีสารสนเทศ[30] โดยมาตรการความมั่นคงปลอดภัยทางไซเบอร์ที่ถูกนำมาใช้งานส่วนใหญ่ จะมีการปรับปรุงหรือประยุกต์มาจากกรอบการดำเนินงาน (Framework) หรือรูปแบบมาตรการต่าง ๆ ที่ถูกนำมาใช้กันในระดับสากล อาทิ กรอบการดำเนินงานของ NIST Cybersecurity Framework และกรอบการดำเนินงาน COBIT 5 ของ ISACA

โดยการศึกษาทบทวนวรรณกรรมครั้งนี้ ผู้วิจัยได้ทำการศึกษาทำความเข้าใจถึงเนื้อหาสำคัญของกรอบการดำเนินงาน NIST Cybersecurity Framework และกรอบการดำเนินงาน COBIT 5 พร้อมทั้งสรุปเนื้อหาสำคัญมาไว้ดังนี้

กรอบการดำเนินงาน NIST Cybersecurity Framework

---

[29] **พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562.**

[30] William Stallings, Effective Cybersecurity. (Addison-Wesley Professional, 2019), p.3.

กรอบการดำเนินงาน NIST Cybersecurity Framework เป็นกรอบแนวคิดที่ถูกสร้างและพัฒนา โดย สถาบันมาตรฐานและเทคโนโลยีแห่งชาติสหรัฐฯ (NIST) รายละเอียดที่สำคัญของกรอบการดำเนินงาน NIST Cybersecurity จะถูกแบ่งออกเป็น 5 ฟังก์ชัน โดยในแต่ละฟังก์ชันก็จะมีหลักความสำคัญที่แตกต่างกันออกไป รายละเอียดตามตารางประกอบ

NIST Cybersecurity Framework	
ฟังก์ชัน	**ความหมาย**
Identify การจำแนก หรือการระบุความเสี่ยง	พัฒนาองค์กรให้มีความเข้าใจในการบริหารจัดการความเสี่ยงด้านไซเบอร์ รวมไปถึงการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ
Protect การป้องกัน	พัฒนาและวางระบบรักษาความปลอดภัยที่เหมาะสม เพื่อให้มั่นใจว่าโครงสร้างของระบบจะได้รับผลกระทบจากการโจมตีทางไซเบอร์
Detect การตรวจจับ	พัฒนาและติดตั้งระบบตรวจจับสถาณการณ์ผิดปกติที่เกิดขึ้นบนระบบเทคโนโลยีสารสนเทศ
Respond การตอบสนอง	พัฒนาแนวทางการตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์
Recovery การฟื้นฟูระบบ	พัฒนากระบวนการฟื้นฟูระบบให้สามารถดำเนินกิจกรรมได้อย่างต่อเนื่องและสามารถกู้ระบบกลับคืนสู่สภาวะปกติได้อย่างทันท่วงที

ตารางที่ 2 ฟังก์ชันการทำงาน NIST Cybersecurity Framework

กรอบการดำเนินงาน COBIT 5

กรอบการดำเนินงาน COBIT ย่อมาจากคำว่า Control Objectives for Information and Related Technology มีการจัดทำขึ้น โดยสมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ (Information Systems Audit and Control Association) หรือที่เรียกกันอย่างย่อว่า ISACA ตัวกรอบดำเนินงาน COBIT ได้มีเริ่มจัดทำขึ้นมาเป็นครั้งแรก ในปี 2539 ภายใต้ชื่อเรียกว่า First edition of COBIT framework หลังจากนั้นก็ได้มีการพัฒนารูปแบบมาอย่างต่อเนื่อง จนกระทั่ง ในปี 2555 ได้มีการปล่อยตัวรูปแบบที่มีชื่อว่า COBIT 5 ออกมาใช้งานจนได้รับความนิยมอย่างแพร่หลายในระดับสากล 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 ครอบคลุมทั่วทั้งองค์กรอย่างครบวงจร

กรอบการดำเนินงาน COBIT 5 จะเข้ามาบูรณาการการกำกับดูแลระบบเทคโนโลยีสารสนเทศภายในองค์กร โดยจะเข้ามาช่วยกำกับดูแลครอบคลุมทุกกระบวนการภายในองค์กร COBIT 5 มีหลักคิดที่ว่าระบบเทคโนโลยีสารสนเทศเป็นสินทรัพย์ที่ทุกคนในองค์กรจำเป็นต้องดูแลเช่นเดียวกับสินทรัพย์อื่น ๆ โดยพิจารณาการกำกับดูแลและบริหารจัดการปัจจัยเอื้อที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศทั้งหมด เพื่อให้ครอบคลุมทั่วทั้งองค์กรอย่างครบวงจร

หลักการที่ 3 ประยุกต์ใช้กรอบการดำเนินงานที่บูรณาการเป็นหนึ่งเดียว

ในปัจจุบันมีหลากหลายองค์กรได้ออกมาตรฐานและแนวปฏิบัติที่ดีที่เกี่ยวข้องกับการกำกับดูแลระบบเทคโนโลยีสารสนเทศอยู่จำนวนมาก ซึ่งแต่ละอย่างก็มีจุดเด่นที่แตกต่างกันในด้านใดด้านหนึ่ง COBIT 5 ได้นำเอามาตรฐานและกรอบการดำเนินงานที่หลากหลากเหล่านั้น มาปรับปรุงจัดเรียงให้สอดคล้องกันในภาพรวม จนสามารถใช้เป็นกรอบการดำเนินงานที่ครอบอยู่เหนือกรอบการดำเนินงานอื่น ๆ สำหรับการกำกับดูแลและการบริหารจัดการระบบเทคโนโลยีสารสนเทศ

หลักการที่ 4 เอื้อให้วิธีปฏิบัติแบบองค์รวมสัมฤทธิ์ผล

การกำกับดูแลและการบริหารจัดการระบบเทคโนโลยีสารสนเทศให้มีประสิทธิภาพและประสิทธิผล 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 แบ่งแยกการกำกับดูแลออกจากการบริหารจัดการ

กรอบการดำเนินงานของ COBIT 5 ระบุความแตกต่างอย่างชัดเจนระหว่างการกำกับดูแลและการบริหารจัดการ หลักสองประการนี้ครอบคลุมถึงกิจกรรมที่แตกต่างกันจึงต้องการโครงสร้างการจัดองค์กรที่แตกต่างกัน และใช้เพื่อจุดประสงค์ที่แตกต่างกัน ในมุมมองของ COBIT 5 ได้มีการเปรียบเทียบให้เห็นความแตกต่างหลัก ๆ ที่เห็นเด่นชัดระหว่างการกำกับดูแลและการบริหารจัดการรายละเอียดตามตารางแนบ

การเปรียบเทียบความแตกต่างระหว่างการกำกับดูแลและการบริหารจัดการ	
การกำกับดูแล (Governance)	**การบริหารจัดการ (Management)**
การกำกับดูแลที่ดีจะทำให้มั่นใจได้ว่า ความต้องการ เงื่อนไข และทางเลือกของผู้มีส่วนได้เสียได้รับการประเมิน เพื่อกำหนดวัตถุประสงค์ที่องค์กรต้องการให้บรรลุซึ่งมีความสมดุลและเห็นชอบร่วมกัน การกำหนดทิศทางผ่านการจัดลำดับความสำคัญและการตัดสินใจและการเฝ้าติดตามผลการดำเนินงานและการปฏิบัติตามเทียบกับทิศทางและวัตถุประสงค์ที่ได้ตกลงร่วมกัน	การบริหารจัดการผู้บริหารจะมีการวางแผน การดำเนินงาน และเฝ้าติดตามกิจกรรมต่าง ๆ ให้สอดคล้องกับทิศทางที่กำหนดโดยหน่วยงานกำกับดูแล (Governance body) เพื่อให้บรรลุวัตถุประสงค์ขององค์กร
ข้อสังเกต ในองค์กรส่วนใหญ่ คณะกรรมการบริหารเป็นผู้รับผิดชอบการกำกับดูแลโดยรวมภายใต้การชี้นำของประธานกรรมการ ในองค์กรขนาดใหญ่และมีความซับซ้อน หน้าที่บางประการสำหรับการกำกับดูแลอาจมอบหมายให้กับหน่วยงานที่จัดตั้งขึ้นเป็นพิเศษในระดับที่เหมาะสม	**ข้อสังเกต** ในองค์กรส่วนใหญ่ การบริหารจัดการรับผิดชอบโดยผู้บริหารระดับสูงภายใต้การชี้นำของประธานเจ้าหน้าที่บริหาร (CEO)

ตารางที่ 3 การเปรียบเทียบความแตกต่างระหว่างการกำกับดูแลและการบริหารจัดการ

เมื่อนำหลักการทั้ง 5 ประการนี้มารวมกันจะทำให้องค์กรสามารถสร้างกรอบการดำเนินงานสำหรับการกำกับดูแลและการบริหารจัดการที่มีประสิทธิผล ซึ่งส่งผลให้การใช้สารสนเทศและการลงทุนด้านเทคโนโลยีเกิดประโยชน์สูงสุด เพื่อยังประโยชน์ให้กับผู้มีส่วนได้เสีย

2.3 แนวคิดเกี่ยวกับมาตรการของสถาบันการเงินต่อการป้องกันอาชญากรรมไซเบอร์

จากปัญหาภัยคุกคามทางไซเบอร์ที่เกิดขึ้น กลุ่มสถาบันการเงินได้เริ่มตระหนักถึงปัญหาและได้มีการประชุมหารือถึงแนวทางป้องกันอาชญากรรมไซเบอร์ที่เหมาะสมกับสภาพแวดล้อมขององค์กร

โดยแนวทางที่ได้นั้นจะได้มาจากการปรับแบบรูปแบบจากองค์กรอื่น ๆ ที่มีลักษณะสภาพแวดล้อมคล้ายคลึงกันร่วมกับรูปแบบมาตรฐานสากลที่ถูกนำมาใช้ในกันอย่างแพร่หลาย อย่างรูปแบบของ NIST Cybersecurity Framework ที่ถูกจัดทำขึ้นโดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติสหรัฐฯ (NIST)[31] หน่วยงานที่ถูกจัดตั้งมาเพื่อกำกับดูแลปัญหาภัยคุกคามทางไซเบอร์โดยเฉพาะ ซึ่งในรูปแบบดังกล่าวมักจะถูกนำมาปรับใช้ในการวางมาตรการป้องกันภัยคุกคามทางไซเบอร์ภายในองค์กรทั่วโลกและรูปแบบ PCI DSS (Payment Card Industry Data Security Standard) ซึ่งเป็นมาตรฐานความปลอดภัยสารสนเทศที่ถูกกำหนดขึ้น โดยอาศัยความร่วมมือจากผู้ให้บริการทางการเงิน 5 ค่ายยักษ์ใหญ่ ประกอบด้วย Visa, MasterCard, American Express, Discover และ JCB โดยมีจุดประสงค์เพื่อช่วยองค์กร บริษัท และร้านค้าต่าง ๆ ที่มีการรับชำระเงินด้วยบัตรเครดิตสามารถป้องกันการฉ้อโกงซึ่งเกิดขึ้นจากการทำธุรกรรมผ่านบัตรเครดิตโดยควบคุมมาตรฐานในการเก็บรักษา ประมวลผล และรับส่งข้อมูลบัตร[32]

ธนาคารแห่งประเทศไทย หน่วยงานผู้ซึ่งเป็นองค์กรที่ดำรงอยู่ในสถานะธนาคารกลางของประเทศไทย ได้มีการเตรียมความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ ด้วยการสร้างความร่วมมือกับกลุ่มสถาบันการเงิน โดยผลงานที่เห็นได้ชัดเจนในปีที่ผ่านมาได้มีการผลักดันให้มีการจัดตั้ง “ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคธนาคาร” (TB-CERT) เพื่อสร้างเครือข่ายเฝ้าระวังติดตามสถานการณ์ภัยคุกคามทางไซเบอร์ โดยจะมีการดำเนินงานครอบคลุมในทุกมิติ ทั้งการเป็นศูนย์กลางในการแลกเปลี่ยนข้อมูลภัยด้านคุกคามทางไซเบอร์และแก้ไขตามแนวทางสากล และการสร้างมาตรฐานกลางด้านความปลอดภัย เช่น Cloud Computing หรือ Biometric อีกทั้งยังมีการสร้างกรอบหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Cyber Resilience) เพื่อกำกับดูแลและบริหารจัดการความเสี่ยงในด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) โดยเน้นการจัดทำแผนเผชิญเหตุในการรับมือเหตุการณ์ผิดปกติทางไซเบอร์ ซึ่งจะจัดให้มีการซักซ้อมรับมือร่วมกันอย่างสม่ำเสมอ พร้อมทั้งพัฒนาบุคลากรที่มีอยู่ด้วยการเพิ่มพูนองค์ความรู้ในด้านความมั่นคงปลอดภัยทางไซเบอร์ให้มีศักยภาพเทียบเท่าในระดับสากล จากแผนการดำเนินงานที่ได้กล่าวมาทั้งหมดนั้นเพื่อเป้าหมายเดียวกัน คือ การสร้างระบบให้สังคมไร้เงินสดบนโลกไซเบอร์ให้มีความมั่นคงและปลอดภัย[33]

---

[31] NIST, **Cybersecurity Framework** [Online], 10 April 2018. Source https://www.nist.gov/cyberframework

[32] “Omise first in Thailand to get milestone card security compliance certification,” The Nation (22 November 2016):5B.

[33] “เก็บเบี้ยใต้ถุนร้าน: ผุดศูนย์ป้องกันไซเบอร์กันแบงก์เสียหาย สร้างความมั่นใจลูกค้า,” วารสารดอกเบี้ย 37, 436 (ตุลาคม 2560): 70-71.

นอกจากการดำเนินงานในข้างต้น ธนาคารแห่งประเทศไทยยังได้มีการลงนามร่วมมือ (MOU) ระหว่าง 4 หน่วยงาน ได้แก่ สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) สมาคมธนาคารไทย (TBA) และสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) โดยมีเป้าหมายเพื่อส่งเสริมและสนับสนุนความร่วมมือระหว่างกันในด้านการรับมือภัยคุกคามไซเบอร์ ด้วยการยกระดับความพร้อมในการรับมือภัยคุกคามไซเบอร์ (CERT Readiness) ให้แก่ภาคธุรกิจการเงิน การลงทุน และการประกันภัย โดยการร่วมกันกำหนดมาตรฐานและกรอบการบริหารจัดการภัยคุกคามไซเบอร์ และมีการแลกเปลี่ยนข้อมูลของการรักษาความมั่นคงปลอดภัยไซเบอร์ร่วมกัน ซึ่งรวมถึงแผนบริหารจัดการสื่อสารมวลชน อีกทั้งยังร่วมกันจัดทำแผนทดสอบและซ้อมรับมือภัยคุกคามไซเบอร์ เพื่อให้เกิดความพร้อมในการรับมือได้อย่างทันการณ์ พร้อมกับการส่งเสริมให้เกิดการพัฒนาและยกระดับความพร้อมของบุคลากรในภาคการเงินให้มีความรู้และความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ ท้ายสุด เป็นการร่วมกันสร้างความตระหนัก ส่งเสริมความรู้ ความเข้าใจถึงความเสี่ยงและวิธีป้องกันขั้นพื้นฐานจากภัยคุกคามไซเบอร์อย่างมั่นคงปลอดภัย เหมาะสมให้แก่ประชาชนผู้ใช้บริการทางการเงิน ซึ่งความร่วมมือทั้งหมดนี้มีผลบังคับใช้ตลอดไป และจะสิ้นสุดลง ก็ต่อเมื่อทุกหน่วยงานตกลงกันเป็นหนังสือเพื่อยกเลิกความร่วมมือดังกล่าว[34]

นอกจากลงนามร่วมมือกับภาคการเงินฯ แล้วนั้น ธปท. ยังได้ลงนามร่วมมืออีกฉบับกับ 17 หน่วยงาน ได้แก่ สำนักงานคณะกรรมการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) สำนักงานคณะกรรมการกำกับกิจการพลังงาน (กกพ.) สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) สมาคมผู้ให้บริการอินเทอร์เน็ตไทย (TISPA) สภาหอการค้าประเทศไทย สภาอุตสาหกรรมแห่งประเทศไทย (ส.อ.ท.) สมาคมธนาคารไทย (TBA) สมาคมโทรคมนาคมแห่งประเทศไทยในพระบรมราชูปถัมภ์ (สทค.) สมาคมประกันชีวิตไทย (TLAA) สมาคมประกันวินาศภัยไทย (TGIA) ตลาดหลักทรัพย์แห่งประเทศไทย (ตลท.) บริษัท การบินไทย จำกัด (มหาชน) (บกท.) บริษัท ปตท. จำกัด (มหาชน) (ปตท.) การไฟฟ้านครหลวง (กฟน.) การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) การไฟฟ้าส่วนภูมิภาค (กฟภ.) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.)

โดยมีเป้าหมายที่จะส่งเสริมและสนับสนุนความร่วมมือระหว่างกันในด้านการรับมือ ภัยคุกคามไซเบอร์ โดยการยกระดับความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ (CERT Readiness) ให้แก่ภาคธุรกิจ การค้า อุตสาหกรรม และโครงสร้างพื้นฐานสำคัญของประเทศ โดยร่วมกันสร้างความตระหนักด้านการรับมือภัยคุกคามไซเบอร์ภายในองค์กรและภายในหน่วยงาน ที่เกี่ยวข้อง ร่วมกันส่งเสริมการใช้มาตรฐานที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ในองค์กรและในหน่วยงานที่เกี่ยวข้อง ร่วมกันผลักดันให้เกิดความร่วมมือในการแก้ไขปัญหาภัยคุกคามไซเบอร์ที่อาจ

[34] “บันทึกข้อตกลงความร่วมมือด้านการยกระดับความพร้อมรับมือภัยคุกคามไซเบอร์ (CERT Readiness) ต่อภาคธุรกิจการเงิน การลงทุน และการประกันภัย,” 22 กันยายน 2559.

กระทบต่อความมั่นคงและเสถียรภาพของประเทศ พร้อมกับส่งเสริมให้มีการจัดตั้งหน่วย Sector-based CERT เพื่อร่วมกันประสานงานแก้ไขปัญหาภัยคุกคามตามขั้นตอนการแจ้งหรือรับมือเหตุภัยคุกคามไซเบอร์ และร่วมกันแลกเปลี่ยนข้อมูลภัยคุกคามไซเบอร์ที่เกิดขึ้นในองค์กรและ ในหน่วยงานที่เกี่ยวข้อง ร่วมกันบริหารจัดการสื่อในด้านการเผยแพร่ข้อมูลสู่สาธารณะ ร่วมกันพัฒนาบุคลากรที่มีความเชี่ยวชาญทางไซเบอร์ เพื่อส่งเสริมให้เกิดการพัฒนาและยกระดับความพร้อมของบุคลากรของประเทศไทยให้เพิ่มมากขึ้น ซึ่งความร่วมมือทั้งหมดนี้มีผลบังคับใช้ตลอดไป[35] เช่นเดียวกับบันทึกความร่วมมือกับในภาคการเงินดังที่กล่าวมาในข้างต้น

อีกทั้งยังได้ลงนามร่วมมือกับสถาบันพัฒนาเทคโนโลยีและวิทยาศาสตร์ประยุกต์ฮ่องกง (Hong Kong Applied Science and Technology Research Institute: ASTRI) เมื่อวันที่ 1 ธ.ค. 2559 เพื่อแลกเปลี่ยนความรู้ ประสบการณ์ ข้อมูล และพัฒนาบุคลากรในเรื่อง Cyber Security และ FinTech ร่วมกันเป็นเวลา 3 ปี ซึ่ง ASTRI ถือเป็นองค์กรที่น่าเชื่อถือและมีความเชี่ยวชาญด้านเทคโนโลยี เนื่องจากมีสถานะเป็นองค์กรของรัฐ ที่ก่อตั้งโดยรัฐบาลเขตการปกครองพิเศษฮ่องกง ตั้งแต่ พ.ศ. 2543 เพื่อเป็นศูนย์กลางด้านการวิจัยและพัฒนาทางเทคโนโลยี (R&D) มีบุคลากรและนักวิจัยที่มีความเชี่ยวชาญด้านมาตรการความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) และเทคโนโลยีทางด้านการเงิน (Financial Technology) รวมถึงมีระบบและศูนย์วิจัย (Lab) ที่รองรับในเรื่องดังกล่าว อีกทั้ง ASTRI ยังทำงานร่วมกับ Hong Kong Monetary Authority (HKMA) ซึ่งเป็นผู้กำกับดูแลสถาบันการเงินในฮ่องกง ในการร่วมสนับสนุนการกำกับดูแลด้านเทคโนโลยี[36]

นอกจากนี้ ธปท. ยังได้ประกาศหลักเกณฑ์กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน ซึ่งบังคับใช้ตั้งแต่ 1 เมษายน 2561 โดยกำหนดให้สถาบันการเงินมีธรรมาภิบาลด้านเทคโนโลยีสารสนเทศที่ดี มีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และมีการบริหารความเสี่ยงดังกล่าวอย่างเหมาะสมโดยเน้นที่องค์ประกอบและบทบาทหน้าที่ของคณะกรรมการของสถาบันการเงิน โครงสร้างองค์กร และการบริหารจัดการบุคลากร โดยคณะกรรมการและผู้บริหารระดับสูงของสถาบันการเงินต้องมีความรู้ความเข้าใจอย่างเพียงพอในการกำหนดทิศทางการใช้เทคโนโลยีให้สอดรับกับกลยุทธ์ในการดำเนินธุรกิจของสถาบันการเงิน มีความเท่าทันความเสี่ยงที่มีมากขึ้น อันเนื่องมาจากการนำเทคโนโลยีมาใช้อย่างแพร่หลาย ให้ความสำคัญกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยถือเป็นส่วนหนึ่งของการบริหารความเสี่ยงในภาพรวมของสถาบันการเงิน (Enterprise Risk Management : ERM) และมีการกำหนดและสื่อสารนโยบายที่เกี่ยวข้องไปยังบุคลากรทุกระดับในองค์กรเพื่อให้เกิดความ

---

[35] “บันทึกข้อตกลงความร่วมมือด้านการยกระดับความพร้อมรับมือภัยคุกคามไซเบอร์ (CERT Readiness) ต่อภาคธุรกิจ การค้า อุตสาหกรรม และโครงสร้างพื้นฐานสำคัญของประเทศ,” 22 กันยายน 2559.

[36] กรุงเทพธุรกิจ, **แบงก์ชาติผนึกสถาบันพัฒนาเทคโนโลยีฮ่องกง รักษาความมั่นคงปลอดภัย“ไซเบอร์-เทคโนโลยีการเงิน” 3 ปี** [ออนไลน์], 8 เมษายน 2560. แหล่งที่มา https://www.bangkokbiznews.com/news/detail/730153

ตระหนักและความเข้าใจ ตลอดจนมีการนำนโยบายไปปฏิบัติด้วยกระบวนการที่เหมาะสม รวมถึงต้องดูแลให้มีการวางแผนและบริหารจัดการด้านบุคลากรโดยเฉพาะที่ทำหน้าที่เกี่ยวข้องกับงานด้านเทคโนโลยีสารสนเทศให้มีคุณสมบัติและความรู้ที่เหมาะสมกับหน้าที่ที่ได้รับมอบหมาย และมีปริมาณที่เพียงพอที่จะรองรับการดำเนินธุรกิจของสถาบันการเงินทั้งในปัจจุบันและในอนาคต

รวมทั้งยังเน้นการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ การตรวจสอบด้านเทคโนโลยีสารสนเทศ และการบริหารจัดการโครงสร้างด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพและรัดกุม โดยอยู่ภายใต้กรอบที่สำคัญ 3 ประการ คือ

1.การรักษาความลับของระบบและข้อมูล (Confidentiality)

2.ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (Integrity)

3.ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (Availability)

รวมไปถึงการให้บริการบนพื้นฐานของการคุ้มครองข้อมูลและรักษาผลประโยชน์ของลูกค้า ทั้งนี้ ในกรณีที่สถาบันการเงินเกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญในการใช้เทคโนโลยีสารสนเทศ ซึ่งส่งผลกระทบต่อการให้บริการ ระบบ หรือชื่อเสียงของสถาบันการเงิน รวมถึงกรณีที่เทคโนโลยีสารสนเทศที่สำคัญของสถาบันการเงินถูกโจมตี หรือถูกขู่โจมตีจากภัยคุกคามทางไซเบอร์ และเป็นปัญหาหรือเหตุการณ์ที่สถาบันการเงินต้องรายงานให้ผู้บริหารในตำแหน่งสูงสุดของสถาบันการเงินทราบ ให้สถาบันการเงินต้องรายงานมายังธนาคารแห่งประเทศไทยทันทีเมื่อเกิดหรือรับรู้เหตุการณ์นั้นและเมื่อสถาบันการเงินมีการนำเทคโนโลยีทางด้านการเงินที่ถูกมาใช้เป็นครั้งแรก หรือมีการเปลี่ยนแปลงการใช้เทคโนโลยีทางด้านการเงินที่มีผลกระทบหรือมีความเสี่ยงอย่างมีนัยสำคัญต่อการดำเนินธุรกิจ[37] สถาบันการเงินจะต้องเข้ามาหารือเพื่อทดสอบการใช้งาน เพื่อศึกษาถึงช่องโหว่ ผลเสียผลกระทบ จากการนำไปใช้งานจริง ตามแนวทางการเข้าร่วมทดสอบและพัฒนานวัตกรรมเทคโนโลยีใหม่ที่จะนำมาสนับสนุนการให้บริการทางการเงิน (Regulatory Sandbox)[38] และเมื่อทดสอบจนระบบพร้อมใช้งาน จึงจะได้รับอนุญาตจากธนาคารแห่งประเทศไทยให้สามารถนำไปใช้กับกลุ่มผู้ใช้บริการต่อไป

---

[37] ธนาคารแห่งประเทศไทย, **ประกาศธนาคารแห่งประเทศไทย ที่ สนส. 19/2560 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน**, 2560. แหล่งที่มา https://www.bot.or.th/Thai/FIPCS/Documents/FPG/2561/ThaiPDF/25610021.pdf

[38] ธนาคารแห่งประเทศไทย, **ประกาศธนาคารแห่งประเทศไทย ที่ ธปท.ฝทง.ว. 311/2562 เรื่อง แนวทางการเข้าร่วมทดสอบและพัฒนานวัตกรรมที่นำเทคโนโลยีใหม่มาสนับสนุนการให้บริการทางการเงิน (Regulatory Sandbox)**, 2562. แหล่งที่มา https://www.bot.or.th/Thai/FIPCS/Documents/FOG/2562/ThaiPDF/25620036.pdf

2.4 งานวิจัยที่เกี่ยวข้อง

ผู้วิจัยได้ทำการศึกษาค้นคว้างานวิจัยที่มีความเกี่ยวข้องทั้งจากในประเทศและต่างประเทศ พร้อมสรุปใจความสำคัญและเนื้อหาที่มีส่วนเกี่ยวข้องกับงานวิจัย โดยแบ่งออกเป็นส่วนต่าง ๆ ดังนี้

2.4.1 งานวิจัยที่เกี่ยวข้องกับมาตรการความมั่นคงปลอดภัยทางไซเบอร์

การศึกษาเรื่องการพัฒนาระบบสารสนเทศสำหรับการประเมินระดับความเสี่ยงและความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร ของ วิภารัตน์ ปทักขินัง และประสงค์ ประณีตพลกรัง (2557)[39]

ผลการศึกษาพบว่า ความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กรภายในประเทศที่เป็นกลุ่มตัวอย่างในการศึกษา อาทิ วิทยาลัยเทคโนโลยีสยาม โดยรวมถือเป็นองค์กรที่มีความพร้อมมาก เนื่องจากมีนโยบายด้านการป้องกันข้อมูลสารสนเทศอย่างเข้มแข็ง มีระบบการจัดเก็บสารสนเทศอย่างรัดกุม มีบุคลากรคอยตรวจจับและตอบโต้การคุกคาม มีการประกาศให้บุคลากรทราบถึงยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์ รวมทั้งมีผู้ดูแลรับผิดชอบ มีการจัดตั้งศูนย์ประสานงานหรือการตอบสนองต่อการแจ้งเหตุภัยคุกคามทางไซเบอร์ มีการประสานงานเพื่อแลกเปลี่ยนข้อมูลสารสนเทศและซอฟต์แวร์ระหว่างหน่วยงาน รวมทั้งมีการส่งเสริม พัฒนาบุคลากรโดยการส่งไปฝึกอบรมหรือดูงานด้านความมั่นคงปลอดภัยไซเบอร์นอกสถานที่

การศึกษาเรื่อง ความรู้ความเข้าใจด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ กรณีศึกษา: ข้าราชการ กองบัญชาการกองทัพไทย ของ ศรวัสย์ สนธิ (2557)[40]

ผลการศึกษาพบว่า การสร้างความตระหนักรู้ ความรู้ ความเข้าใจเป็นสิ่งสำคัญ โดยการส่งบุคลากรในองค์กรฝึกอบรมเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ เห็นได้จากข้าราชการในกองบัญชาการกองทัพไทยผู้ที่เคยผ่านการฝึกอบรมหลักสูตรการรักษาความมั่นคงปลอดภัยสารสนเทศของกองบัญชาการกองทัพไทย มีความรู้ที่มากกว่าและมีพฤติกรรมที่จะก่อให้เกิดความเสี่ยงที่น้อยกว่าข้าราชการที่ไม่ได้รับการฝึกอบรม แต่อย่างไรก็ตามยังมีผู้ที่ยังไม่ได้ผ่านการฝึกอบรมอีกเป็นจำนวนมาก เนื่องจากข้อจำกัดด้านงบประมาณ ซึ่งจัดเพียงปีละครั้ง และจำกัดอัตราการเข้ารับการฝึกอบรม จึงทำให้ผู้เข้ารับการฝึกอบรมส่วนใหญ่เป็นข้าราชการสัญญาบัตร และเจ้าหน้าที่ที่เกี่ยวข้องเป็นผู้แทนของหน่วยงาน ข้าราชการที่เป็นเพียงผู้ใช้งานคอมพิวเตอร์จึงยังคงขาดความรู้เรื่อง

---

[39] วิภารัตน์ ปทักขินัง และประสงค์ ประณีตพลกรัง, “การพัฒนาระบบสารสนเทศสำหรับการประเมินระดับความเสี่ยงและความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร,” (สารนิพนธ์ปริญญามหาบัณฑิต สาขาวิชาระบบสารสนเทศคอมพิวเตอร์ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม,2557).

[40] ศรวัสย์ สนธิ, “ความรู้ ความเข้าใจด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ กรณีศึกษา: ข้าราชการ กองบัญชาการกองทัพไทย,” (สารนิพนธ์ปริญญาปริญญามหาบัญฑิต สาขาวิชาเทคโนโลยีคอมพิวเตอร์และการสื่อสาร คณะวิศวกรรมศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิตย์,2557).

การดูแลรักษาคอมพิวเตอร์และตระหนักในเรื่อขาดการเอาใจใส่ต่อภัยคุกคาม นอกเสียจากข้าราชการที่มีความรู้ความสนใจด้านคอมพิวเตอร์ โดยการค้นคว้าหาความรู้เพิ่มเติม

การศึกษาเรื่อง การใช้งานสื่อสังคมออนไลน์สาธารณะมีผลกระทบต่อความมั่นคงปลอดภัยของกองทัพไทย ของ วีรวดี ขุขันธิน (2560)[41]

ผลการศึกษาพบว่า การที่สื่อสังคมออนไลน์สาธารณะอาจทำให้เกิดช่องทางให้ผู้ประสงค์ร้ายสามารถเข้าสู่ระบบการรักษาความปลอดภัยของกองทัพได้ และอาจรอคอยโจมตีในเวลาที่เหมาะสม ทำให้เกิดภัยอันตรายต่อองค์กร ไม่ว่าจะการขโมยข้อมูลส่วนตัว ข้อมูลสำคัญต่าง ๆ ขององค์กร การปลอมตัวเป็นบุคคลอื่นในโลกสังคมออนไลน์ และการทำสงครามไซเบอร์ (Cyber Warfare) แนวทางป้องกันและแก้ไขปัญหาทำได้โดยการควบคุมการใช้งาน การให้ความรู้แก่ผู้ใช้งานทุกระดับ รวมถึงต้องปลูกฝังจิตสำนึก และค่านิยมในการใช้งานสื่อออนไลน์ที่ถูกต้องควบคู่ไปกับการบังคับใช้กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ การวางมาตรการป้องกัน กำหนดนโยบายการปฏิบัติอย่างจริงจัง โดยให้ผู้มีอำนาจลงมากำกับดูแลอย่างใกล้ชิด และการประสานความร่วมมือและเสริมสร้างเครือข่ายกับภาคเอกชน ภาควิชาการ การเสริมสร้างความร่วมมือระหว่างประเทศ

การศึกษาเรื่องความท้าทายด้านความมั่นคงปลอดภัยไซเบอร์ และแนวโน้มที่อาจเกิดขึ้นจากเทคโนโลยีใหม่ ๆ (Cyber Security challenges and its emerging trends on latest technologies) ของ G.NIKHITA REDDY, G.J.UGANDER REDDY (2557)[42]

ผลการศึกษาพบว่า ปัญหาที่เกี่ยวกับอาชญากรรมไซเบอร์ที่เกิดขึ้นในประเทศมาเลเซียระหว่างเดือนมกราคมปี 2555 ถึงเดือนมิถุนายน ปี 2556 มีแนวโน้มเพิ่มสูงขึ้นอย่างมีนัยสำคัญ และเมื่อปัญหาอาชญากรรมไซเบอร์เพิ่มมากขึ้น จึงต้องมีการปรับมาตรการด้านความมั่นคงปลอดภัยทางไซเบอร์เพิ่มขึ้นตาม แนวทางการใช้คอมพิวเตอร์ในรูปแบบต่าง ๆ มีผลกระทบต่อความปลอดภัยด้านไซเบอร์โดยรูปแบบที่ส่งผลกระทบอย่างมาก ได้แก่ Web servers, Cloud computing, Advanced Persistent Threat (APT), Mobile Networks, IPv6, Encryption of the code รวมไปถึงในปัจจุบันที่ผู้คนใช้สื่อสังคมออนไลน์เพิ่มมากขึ้นทุกวัน ทำให้สิ่งเหล่านี้กลายเป็นรูปแบบ (Platform) หลักที่อาชญากรจะใช้ในการโจมตีขโมยข้อมูลส่วนตัวหรือข้อมูลที่สำคัญ ซึ่งผู้ใช้บริการสื่อสังคมออนไลน์มักจะส่งมอบข้อมูลส่วนตัวให้บริษัทผู้ดูแลระบบง่ายมากขึ้น ดังนั้นเพื่อป้องกันการเกิด

---

[41] วีรวดี ขุขันธิน, “การใช้งานสื่อสังคมออนไลน์สาธารณะมีผลกระทบต่อความมั่นคงปลอดภัยของกองทัพไทย,” (เอกสารวิจัยส่วนบุคคล วิทยาลัยการทัพบก, 2560).

[42] G.NIKHITA REDDY and G.J.UGANDER REDDY, “Cyber Security challenges and its emerging trends on latest technologies,” (Personal research papers, 2014).

อาชญากรรมไซเบอร์ บริษัทเหล่านี้ต้องมีวิธีที่จะทราบถึงการคุกคามได้อย่างรวดเร็ว เพื่อที่จะแก้ไขหรือตอบสนองได้ทันท่วงทีก่อนที่จะเกิดความเสียหายจริง

การศึกษาเรื่องโลกของความมั่นคงปลอดภัยไซเบอร์ และอาชญากรรมไซเบอร์ (World of Cyber Security and Cybercrime) ของ Rachna Buch, Dhatri Ganda, Pooja Kalola, Nirala Borad (2561)[43]

ผลการศึกษาพบว่า ปัญหาอาชญากรรมไซเบอร์ เป็นหนึ่งในปัญหาอาชญากรรมหลักที่กระทำโดยผู้เชี่ยวชาญด้านคอมพิวเตอร์ โดยการสร้างความก่อกวนในเครือข่าย (network) พร้อมทั้งจารกรรมข้อมูลสำคัญและข้อมูลส่วนบุคคล โดยมักจะเป็นข้อมูลบัญชีธนาคาร เพื่อโอนเงินจากบัญชีของเหยื่อไปยังบัญชีตนเอง ซึ่งอุปกรณ์อัจฉริยะใด ๆ ที่สามารถส่งผ่านข้อมูลไปยังอุปกรณ์อื่นได้ ไม่ว่าจะผ่านเครือข่ายหรือไม่ก็ตามนั้นรวมอยู่ในขอบเขตของความปลอดภัยทางไซเบอร์ ในปัจจุบัน ทุกคนควรต้องตระหนักถึงความปลอดภัยในโลกไซเบอร์เช่นเดียวกับอาชญากรรมไซเบอร์ รวมทั้งทราบถึงสาเหตุการเกิด โดยความปลอดภัยที่เกี่ยวกับกิจกรรมผ่านทางสังคมออนไลน์อาจมีความเสี่ยงเพิ่มสูงขึ้นทุกวัน เนื่องจากอาจเกิดเหตุข้อมูลสูญหาย การแก้ไขข้อมูล การลบข้อมูลที่เป็นประโยชน์ เช่น รายละเอียดส่วนบุคคล รหัสเข้าบัญชีอีเมล บัญชีสังคมออนไลน์ หรือบัญชีธนาคาร อย่างไรก็ตามคนบางคนอาจจะทราบกฎหมายที่จะต่อสู้กับอาชญากรรมไซเบอร์ หรือกฎหมายไซเบอร์และการกระทำที่จะต้องดำเนินการเพื่อต่อสู้กับอาชญากรรม

2.4.2 งานวิจัยที่เกี่ยวข้องกับการบริหารความเสี่ยงทางไซเบอร์

การศึกษาเรื่องความเสี่ยงด้านไซเบอร์สำหรับกลุ่มการเงิน: กรอบการประเมินเชิงปริมาณ (Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment) ของ Antoine Bouveret (2561)[44]

ผลการศึกษาพบว่า ความเสี่ยงด้านไซเบอร์เป็นภัยคุกคามที่สำคัญต่อความมั่นคงทางการเงินและเกิดขึ้นกับสถาบันการเงินทุกประเภท ทั้งธนาคารกลางและธุรกิจเทคโนโลยีการเงิน อย่างไรก็ตามข้อมูลเกี่ยวกับเหตุการณ์ไซเบอร์นั้นหายากและไม่ค่อยมีการวิเคราะห์ความเสี่ยงไซเบอร์เชิงปริมาณ ซึ่งการที่ข้อมูลหายาก เนื่องจากไม่มีการกำหนดมาตรฐานในการจัดเก็บข้อมูล และบริษัทไม่ได้รับ

---

[43] Rachna Buch, Dhatri Ganda, Pooja Kalola and Nirala Borad, “World of Cyber Security and Cybercrime,” STM Journals 4,2 (August 2018): 18-23.

[44] Antoine Bouveret, “Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment,” (IMP Working Papers describe research in progress, 2018)

แรงจูงใจให้รายงานเหตุการณ์เหล่านี้ ยิ่งไปกว่านั้น การแบ่งปันข้อมูลระหว่างประเทศที่รายงานต่อหน่วยงานกำกับดูแลท้องถิ่นนั้น นอกจากต้องคำนึงถึงความเป็นส่วนตัวและข้อจำกัดอื่น ๆ แล้วนั้น จะต้องคำนึงถึงความมั่นคงของชาติในการแบ่งปันและรายงานข้อมูล

ภาคการเงินมีความเสี่ยงสูงจากการโจมตีทางไซเบอร์ในทุกประเทศ 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 ผลการสูญเสียเฉลี่ยจากการโจมตีทางไซเบอร์สำหรับประเทศในกลุ่มตัวอย่างมีมูลค่า 97 พันล้านเหรียญสหรัฐหรือร้อยละ 9 ของกำไรสุทธิของธนาคาร การสูญเสียบางครั้งนั้นมีขนาดใหญ่เกินกว่าการประกันจะครอบคลุมได้ ซึ่งเบี้ยประกันเติบโตสูงถึง 3 พันล้านเหรียญสหรัฐ และคาดว่าจะสูงถึง 12-20 พันล้านเหรียญสหรัฐในอีก 10 ปีข้างหน้า อย่างไรก็ตามสถาบันการเงินส่วนใหญ่ไม่มีการทำประกันทางไซเบอร์

2.4.3 งานวิจัยที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์

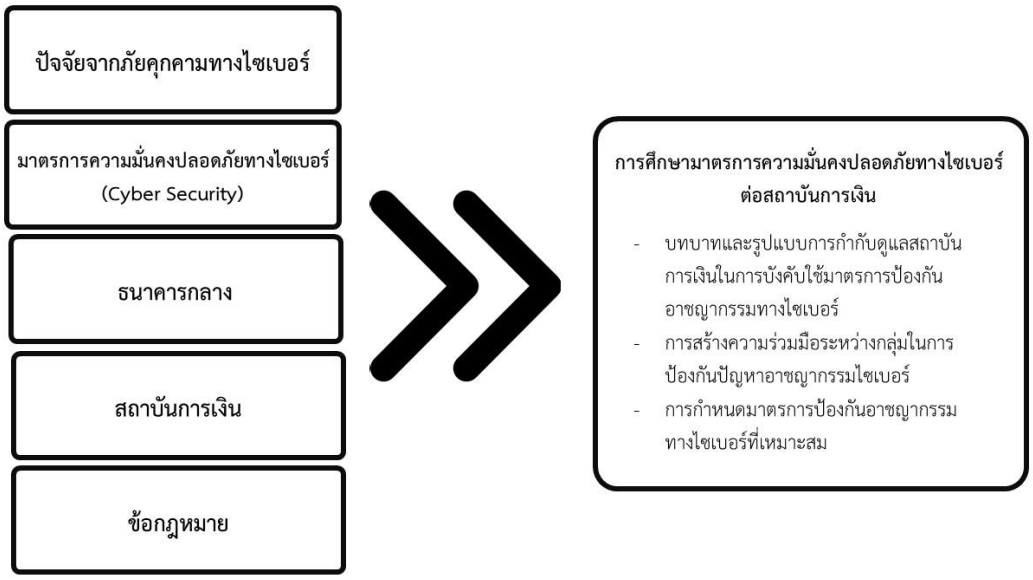
การศึกษาเรื่องอาชญากรรมไซเบอร์ และการกำกับดูแลเครือข่าย (Cybercrimes and Network Governance) ของ Anna Lucia Valvo (2559)[45]

ผลการศึกษาพบว่า ปัญหาอาชญากรรมไซเบอร์จะรุนแรงมากขึ้นหากไม่มีความร่วมมือระหว่างภาครัฐและเอกชนในพื้นที่ รวมถึงการขาดความสามารถของสถาบันในการควบคุม ซึ่งคณะกรรมาธิการยุโรปได้ยอมรับความล้มเหลวของประเทศสมาชิกในการผลิตกฎหมายที่ตอบสนองต่อกิจกรรมทางอาญาใหม่ ๆ ซึ่งปัจจุบันยังไม่มีหมวดหมู่ทางกฎหมายที่ชัดเจนที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ยกเว้นอนุสัญญาบูดาเปสต์ ฉบับที่ 185/2001 โดยเครื่องมือระหว่างประเทศที่สำคัญในสาขานี้คืออนุสัญญาของสภายุโรปเกี่ยวกับอาชญากรรมไซเบอร์ซึ่งมีผลบังคับใช้ในปี 2547 ประกอบด้วยคำนิยามทั่วไปของอาชญากรรมไซเบอร์ชนิดต่าง ๆ และการวางรากฐานความร่วมมือด้านการพิจารณาคดีระหว่างรัฐที่เข้าร่วม ลงนามโดยรัฐสมาชิกสหภาพยุโรปทั้งหมดและประเทศอื่น ๆ ที่ไม่ใช่ยุโรป เช่นสหรัฐอเมริกา แคนาดา ญี่ปุ่น และแอฟริกา อย่างไรก็ตาม อนุสัญญาบูดาเปสต์เมื่อวันที่ 23 พฤศจิกายน 2544 ยังคงไม่ได้รับการยอมรับจากทุกรัฐ แม้รัฐเหล่านี้จะให้สัตยาบันต่ออนุสัญญาแล้วก็ตาม แต่ก็ยังไม่ได้ให้สัตยาบันต่อระเบียบที่เพิ่มเติมเกี่ยวกับการเหยียดสีผิวหรือการทำให้หวาดกลัวโดยใช้ระบบคอมพิวเตอร์ อนุสัญญาดังกล่าวได้รับการพิจารณาโดยคำนึงถึงความสมดุล

[45]Anna Lucia Valvo, “Cybercrimes and Network Governance,” (Research Papers, Faculty of Economic and Legal Science, Kore University of Enna, Italy, 2016)

ระหว่างความต้องการต่อต้านอาชญากรรมไซเบอร์และการเคารพในสิทธิขั้นพื้นฐานและเสรีภาพ ทั้งนี้ ผู้บัญญัติกฎหมายต้องเผชิญกับความท้าทายมากมายจากความก้าวหน้าทางเทคโนโลยี อย่างไรก็ตาม ถ้าเราต้องการทำให้อินเทอร์เน็ตใช้งานได้อย่างอิสระและปลอดภัย แต่ละประเทศจะต้องมีความรับผิดชอบและจัดระเบียบกฎพื้นฐานทั่วไปในการกำกับดูแลของอินเทอร์เน็ตและผลกระทบที่เกี่ยวข้องที่เกิดจากการใช้งานที่เพิ่มมากขึ้น

2.5 กรอบแนวคิดในการวิจัย



รูปภาพที่ 1 กรอบแนวคิดในการวิจัย

บทที่ 3
บทบาทธนาคารกลางของไทยในการกำกับดูแลสถาบันการเงิน ต่อการบังคับใช้มาตรการความมั่นคงปลอดภัยทางไซเบอร์

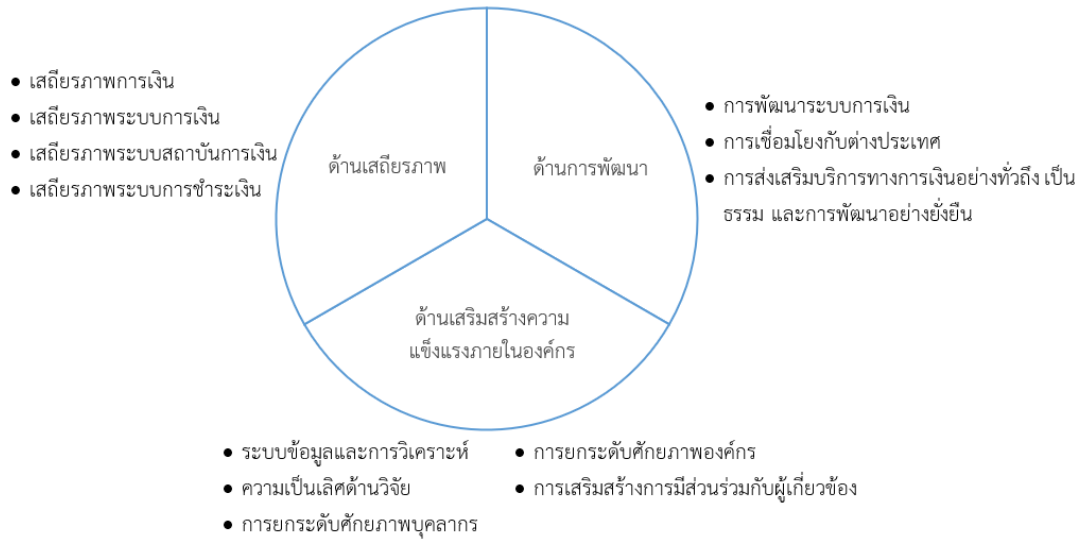
ธนาคารกลางของไทยหรือที่รู้จักกันในชื่ออย่างเป็นทางการว่า “ธนาคารแห่งประเทศไทย” ซึ่งในงานวิจัยครั้งนี้ผู้วิจัยจะขอใช้คำย่อว่า ธปท. ทดแทนการเขียนคำเต็ม โดย ธปท. นั้นมีสถานะเป็นองค์กรของรัฐที่มีความสำคัญต่อระบบการเงินของประเทศ มีบทบาทหน้าที่หลักในการดูแลกำกับสถาบันการเงิน โดยอาศัยเครื่องมือควบคุมจากการออกนโยบาย กฎเกณฑ์ ระเบียบ ข้อบังคับต่าง ๆ มากำกับดูแลสถาบันการเงิน เพื่อให้สถาบันการเงินเหล่านี้ มีระบบการให้บริการที่ดีและมีมาตรฐานด้านความปลอดภัยที่สูงเป็นไปตามเกณฑ์มาตรฐานสากล ซึ่งจากปัญหาวิจัยที่ผู้วิจัยต้องการจะศึกษาถึงบทบาทของธนาคารกลางของไทยในการกำกับดูแลสถาบันการเงิน ผู้วิจัยได้เลือกใช้เทคนิคการวิจัยเชิงคุณภาพ (Qualitative Methodology) เป็นแนวทางหลักในการศึกษาวิเคราะห์ปัญหาวิจัย โดยในส่วนการศึกษาเนื้อหา บทที่ 3 ผู้วิจัยได้เลือกใช้เครื่องมือการสัมภาษณ์เชิงลึก (In-depth Interview) มาทำการศึกษาจากกลุ่มผู้ให้ข้อมูลสำคัญ (Key Informants) ด้วยเทคนิคการสุ่มกลุ่มตัวอย่างแบบเจาะจง (Purposive Sampling) ร่วมกับการผสมผสานใช้เทคนิคการสุ่มกลุ่มตัวอย่างแบบสโนว์บอล (Snowball Sampling) ซึ่งจะใช้วิธีการแนะนำจากผู้ให้ข้อมูลแบบเจาะจงในชุดแรก ทั้งนี้เพื่อให้เกิดกระบวนการส่งต่อข้อมูลแบบต่อเนื่องจากกลุ่มเครือข่ายข้อมูลที่มีอยู่และเมื่อได้ข้อมูลครบถ้วนตามกรอบคำวิจัยที่ตั้งไว้ ผู้วิจัยจะนำข้อมูลมาสังเคราะห์ข้อมูลเชื่อมโยงให้ได้เห็นถึงบทบาทในการกำกับดูแลสถาบันการเงิน พร้อมนำเสนอในรูปแบบการพรรณนา ดังนี้

3.1 บทบาทหน้าที่ของธนาคารกลางของไทยในการกำกับดูแลสถาบันการเงิน

ธนาคารกลางของไทย มีบทบาทหน้าที่ครอบคลุมในหลากหลายมิติโดยเฉพาะในด้านการควบคุมเสถียรภาพทางการเงินของประเทศ โดยสามารถแบ่งย่อยออกเป็น 4 ด้าน 1.ด้านเสถียรภาพทางการเงิน 2.ด้านเสถียรภาพระบบการเงิน 3.ด้านเสถียรภาพระบบสถาบันการเงิน 4.ด้านเสถียรภาพระบบการชำระเงิน ซึ่งจากปัญหาวิจัยได้สะท้อนให้เห็นถึงปัญหาภัยคุกคามทางไซเบอร์ที่กำลังเข้ามาสร้างปัญหาให้กับระบบการเงิน ธนาคารกลางในฐานะที่เป็นองค์กรที่กำกับดูแลสถาบันการเงิน จึงจำเป็นที่จะต้องสร้างระบบป้องกันให้แก่ระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันไม่ให้สถาบันการเงินที่อยู่ภายใต้การกำกับดูแลสร้างช่องโหว่ให้แก่ระบบภายในองค์กร จนส่งผลกระทบไปยังองค์กรอื่น ๆ เนื่องจากระบบการเงินมีความเชื่อมโยงถึงกันทั้งหมด โดยในปัจจุบันธนาคารกลางของไทย ได้เริ่มมีการออกมาตรการเข้ามากำกับดูแลสถาบันการเงินให้เป็นไปในทิศทางเดียวกัน ซึ่งสามารถจำแนกออกเป็นรายละเอียดขั้นตอนในการดำเนินการได้ดังต่อไปนี้

3.1.1 บทบาทจากการวางกรอบและแนวทางในรับมือกับภัยคุกคามทางไซเบอร์

ธนาคารกลางของไทย หรือ ธปท. จะมีการกำหนดแผนงาน เป้าหมาย ภารกิจที่จะดำเนินการล่วงหน้าในแต่ละปี เพื่อเป็นกรอบในการดำเนินงานให้กับองค์กรได้มีเป้าหมายไปในทิศทางเดียวกัน แผนงานเหล่านี้เรียกโดยรวมว่า “ยุทธศาสตร์ธนาคารแห่งประเทศไทย” ซึ่ง ธปท. จะมีการกำหนดแผนล่วงหน้าไว้ที่วงรอบละ 3 ปี เพื่อให้เป็นการดำเนินการที่ต่อเนื่อง สามารถเห็นผลลัพธ์ที่เกิดการเปลี่ยนแปลงได้ในระยะยาว ซึ่งยุทธศาสตร์ ธปท. ที่ได้สิ้นสุดวงรอบระยะเวลาไป คือ แผนยุทธศาสตร์ประจำปี พ.ศ. 2560 – 2562[1] โดยในยุทธศาสตร์ฉบับดังกล่าว ธปท. ได้เล็งเห็นถึงความสำคัญของภัยคุกคามทางไซเบอร์ จึงได้กำหนดภารกิจและเป้าหมายที่จะดำเนินการด้านดังกล่าว ให้อยู่ในแผนงานด้านเสถียรภาพ (Stability) โดยมีการจำแนกลงไปอีกระดับชั้นอยู่ในหัวข้อย่อยเรื่องระบบสถาบันการเงินและระบบการชำระเงิน



รูปภาพที่ 2 แผนยุทธศาสตร์ธนาคารแห่งประเทศไทยประจำปี พ.ศ. 2560 - 2562

การศึกษาด้านเสถียรภาพระบบสถาบันการเงิน ผู้วิจัยพบว่า ธปท. มีเป้าหมายที่จะมุ่งเน้นผลักดันให้สถาบันการเงินและผู้ให้บริการในระบบ ปฏิบัติตามกรอบแนวปฏิบัติด้านระบบเทคโนโลยีสารสนเทศและมาตรการความมั่นคงทางไซเบอร์ที่เป็นไปตามมาตรฐานสากล ตามที่ ธปท. กำหนดขึ้น และผลักดันให้ได้รับใบรับรอง (Certify) ในระดับสากล เพื่อให้สถาบันการเงินภายใต้การกำกับดูแล มี

---

[1] ธนาคารแห่งประเทศไทย, **แผนยุทธศาสตร์ 3 ปี ธปท. พ.ศ. 2560 - 2562** [ออนไลน์], 2560. แหล่งที่มา https://www.bot.or.th/Thai/AboutBOT/RolesAndHistory/PublishingImages/StrategicPlan/write-up.pdf

ความสามารถในการป้องกัน ตรวจจับ เตรียมพร้อมตอบสนองต่อความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ ซึ่ง ธปท. จะเข้าไปประเมินความเสี่ยงทางด้านไซเบอร์และการเตรียมความพร้อมรับมือของธนาคารพาณิชย์ในทุกแห่ง รวมไปถึงบริษัทที่มีความเกี่ยวข้องกับระบบ อาทิ บริษัท เนชั่นแนล ไอทีเอ็มเอ็กซ์ จำกัด (NITMX) , บริษัท ศูนย์ประมวลผล จำกัด (PCC) ,Thai Payment Network (TPN) โดยทยอยตรวจสอบในช่วง 3 ปี ตามแผนยุทธศาสตร์ฯ และร่วมกันศึกษาหาแนวทางปิดช่องโหว่ที่เกิดขึ้น

การศึกษาด้านเสถียรภาพระบบการชำระเงิน ผู้วิจัยพบว่า มีเนื้อหาในบางส่วนที่มีความเกี่ยวข้องกับความปลอดภัยทางไซเบอร์ ดังปรากฏให้เห็นจากการที่ ธปท. ได้ตั้งเป้าหมายมุ่งเน้นที่จะยกระดับมาตรฐานความมั่นคงปลอดภัยของโครงสร้างพื้นฐานของระบบการชำระเงินที่ ธปท. ให้บริการ ให้มีความมั่นคงปลอดภัยและมีประสิทธิภาพมากยิ่งขึ้น เพื่อให้สอดคล้องกับพัฒนาการทางเทคโนโลยี และพัฒนาการด้านระบบชำระเงินที่มีการเปลี่ยนแปลงไปอย่างไม่หยุดนิ่ง ซึ่ง ธปท. เองก็ได้เล็งเห็นถึงความสำคัญในจุดนี้ จึงได้พยายามพัฒนารูปแบบของระบบการชำระเงินที่มีการใช้งานมาอย่างยาวนาน อาทิ ระบบบาทเนต (BAHTNET - Bank of Thailand Automated High-value Transfer Network) และระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็ค (Imaged Cheque Clearing and Archive System – ICAS) ซึ่งอาจมีความเสี่ยงทางด้านไซเบอร์เพิ่มขึ้นจากเทคโนโลยีที่ใช้อยู่นั้นเริ่มล้าสมัยเมื่อเปรียบเทียบกับเทคโนโลยีสมัยใหม่ โดยทำการเริ่มปรับปรุงระบบให้มีความเสถียรและมีความมั่นคงปลอดภัยยิ่งขึ้น นอกจากการปรับระบบการชำระเงินภายในที่ดีแล้ว ระบบที่ให้บริการอยู่ภายนอก ธปท. ก็ต้องมีการปรับปรุงให้ดีขึ้นไปพร้อมกัน ธปท. จึงผลักดันให้ผู้ให้บริการชำระเงินแต่ละราย ปรับปรุงระบบให้ได้ตามมาตรฐานที่ ธปท. ตั้งไว้ จากแนวทางการตรวจที่ได้ส่งไปให้ตรวจสอบหรือได้รับการรับรองที่ได้มาตรฐานสากลจากองค์กรที่เชื่อถือได้ นอกจากนี้ภายในเนื้อหายุทธศาสตร์ ธปท. ยังระบุไว้ถึงการวางแผนยกระดับการกำกับดูแลความเสี่ยงให้เท่าทันต่อนวัตกรรมและความเสี่ยงจากการเชื่อมโยงนวัตกรรมที่มาจากหลากหลายภาคส่วน (interconnectedness) โดยการสร้างหรือเข้าไปมีมีส่วนร่วมในกลไกการติดตามนวัตกรรมและความเสี่ยงจากการใช้เทคโนโลยีและบริการชำระเงินสมัยใหม่ อาทิ การจัดตั้งหรือมีส่วนร่วมในการประชุมรับฟังข้อเสนอแนะ แลกเปลี่ยนความคิดเห็น (Public Hearing) ในขั้นตอนการกำหนดนโยบายร่วมกับผู้มีส่วนเกี่ยวข้องและผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย เพื่อวางกรอบนโยบายในการกำกับดูแลความเสี่ยงจากเทคโนโลยีและบริการสมัยใหม่ โดยจัดลำดับความเข้มข้นของการบังคับใช้เกณฑ์ให้สอดคล้องกับความเสี่ยงที่เกิดขึ้น รวมไปถึงการประสานงานร่วมกับหน่วยงานที่มีส่วนเกี่ยวข้องกับระบบการชำระเงิน เพื่อสนับสนุนให้มีการออกมาตรการความมั่นคงปลอดภัยทางไซเบอร์

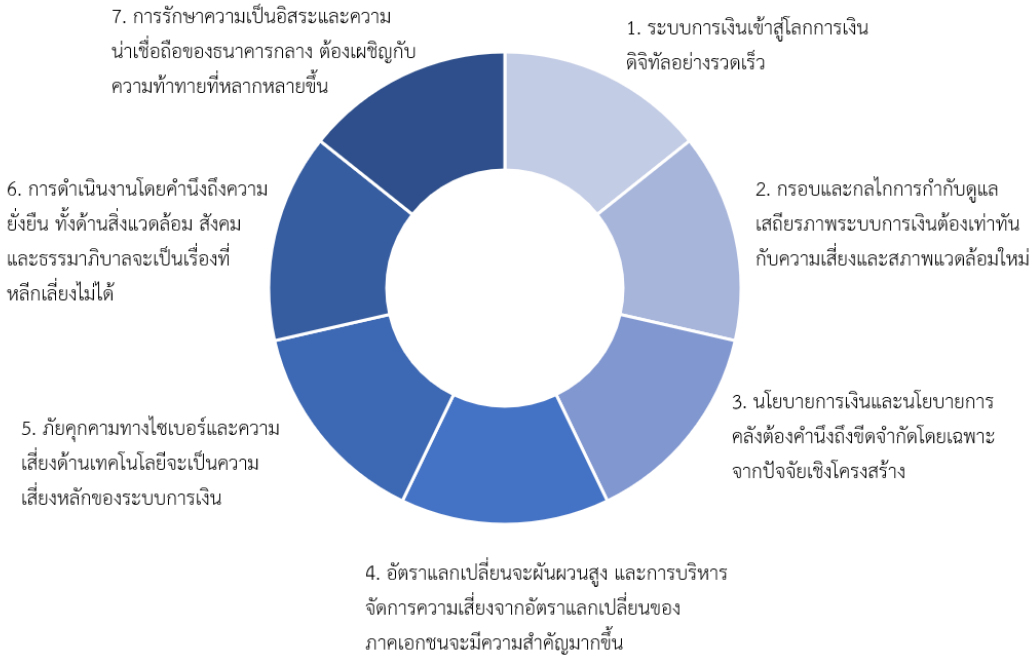
ทั้งนี้การยกระดับการกำกับดูแลระบบการชำระเงินจะมีบทบาทมากขึ้นเรื่อย ๆ ในอนาคต โดยเฉพาะอย่างยิ่งเมื่อสังคมโลกกำลังก้าวเข้าสู่สังคมไร้เงินสด (Cashless Society) จากการเข้ามาของเทคโนโลยีระบบการชำระเงินใหม่ ๆ ที่เห็นได้ชัดอย่างระบบพร้อมเพย์ (PromptPay) หรือ ในกลุ่มกระเป๋าเงินอิเล็กทรอนิกส์ (E-Wallet) ซึ่งผู้วิจัยคาดว่าในอนาคตข้างหน้าเราจะได้พบกับ

เทคโนโลยีระบบการชำระเงินแบบใหม่ ๆ ที่เปลี่ยนแปลงไปจากเดิมอีกมาก ที่จะเข้ามาอำนวยความสะดวก เพื่อให้ประชาชนได้รับความสะดวกสบายมากยิ่งขึ้น ซึ่งเมื่อเทคโนโลยีเข้ามาแล้วระบบจึงต้องมีการพัฒนาด้านความปลอดภัยควบคู่กันไปด้วย โดยจะต้องมีการพัฒนาระบบให้อยู่ในมาตรฐานระดับสากลจนสามารถสร้างความเชื่อมั่นให้กับผู้ใช้บริการและหันมาทำธุรกรรมผ่านระบบการชำระเงินออนไลน์มากขึ้น

ทั้งนี้จากแผนยุทธศาสตร์ที่ ธปท. วางไว้ล่วงหน้า 3 ปี ผู้วิจัยได้สัมภาษณ์เจ้าหน้าที่ฝ่ายวางแผนองค์กร ของ ธปท. ซึ่งทำหน้าที่ติดตามความคืบหน้าผลการดำเนินการตามแผนยุทธศาสตร์ พบว่าผลจากการปฏิบัติงานที่เกิดขึ้นจริงตลอดช่วงระยะเวลา 3 ปีที่ผ่านมา ผลงานที่เห็นได้ชัด คือ ธปท. ได้ออกแนวปฏิบัติต่าง ๆ สำเร็จมากมาย อาทิ แนวปฏิบัติ Cyber Security แนวปฏิบัติ Third Party Risk Management แนวปฏิบัติการทดสอบเจาะระบบแบบ Red Teaming และแนวปฏิบัติ Mobile Banking Security ทั้งยังสนับสนุนให้สมาคนธนาคารไทยจัดตั้ง Thailand Banking Sector Computer Emergency Response Team (TB-CERT) สำเร็จและเข้าร่วมเป็นสมาชิกกลุ่ม Central Banks, Regulators and Supervisory Entities Forum (CERES forum)

นอกจากนี้ ธปท. ยังได้จัดทำบันทึกข้อตกลงความร่วมมือ (MOU) การแลกเปลี่ยนข้อมูลกับผู้กำกับดูแล ได้แก่ Hong Kong Monetary Authority (HKMA) และ Monetary Authority of Singapore (MAS) เพื่อแลกเปลี่ยนข้อมูลภัยคุกคามไซเบอร์และ Best Practice ในการบริหารจัดการความเสี่ยงด้าน IT และภัยคุกคามไซเบอร์ ส่วนด้านทรัพยากรบุคคล พบว่า ธปท. ได้ร่วมมือกับสมาคมส่งเสริมสถาบันกรรมการบริษัทไทย (Institute of Directors: IOD) พัฒนาหลักสูตรส่งเสริมความรู้ให้กับผู้บริหารระดับสูงและพนังงานของสถาบันกรเงิน ส่วนการพัฒนาด้านระบบการชำระเงิน ธปท. ได้ผลักดันสมาชิกของระบบ BATHNET และ ICAS จนได้รับการรับรองมาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001 จนครบทุกองค์กรแล้ว และเนื่องจากแผนยุทธศาสตร์ที่ผู้วิจัยได้กล่าวมาข้างต้นได้สิ้นสุดลงในปี 2562 ผู้วิจัยได้พบว่า ธปท. ได้จัดทำแผนยุทธศาสตร์ฉบับใหม่สำหรับรอบระยะเวลา 3 ปี ระหว่าง พ.ศ. 2563 – 2565[2] ขึ้นมาแล้ว ซึ่งได้เปลี่ยนแปลงแนวทางการจัดทำเดิมมาในรูปแบบของความท้าทายที่ต้องเผชิญในอนาคต โดย ธปท. ยังคงให้ความสำคัญกับภัยคุกคามทางไซเบอร์อย่างต่อเนื่องและกำหนดให้เป็น 1 ใน 7 ความท้าทายสำคัญที่ ธปท. ต้องเข้าไปกำกับดูแล

[2] ธนาคารแห่งประเทศไทย, **แผนยุทธศาสตร์ ธปท. พ.ศ. 2563 - 2565** [ออนไลน์], 2563. แหล่งที่มา https://www.bot.or.th/Thai/AboutBOT/RolesAndHistory/DocLib_StrategicPlan/BOT-StrategicPlan2020to2022.pdf



รูปภาพที่ 3 แผนยุทธศาสตร์ธนาคารแห่งประเทศไทยประจำปี พ.ศ. 2563 – 2565

ธปท. ได้เล็งเห็นว่าประเด็นภัยคุกคามทางไซเบอร์และความเสี่ยงด้านเทคโนโลยีสารสนเทศจะเข้ามาเป็นความเสี่ยงหลักของระบบการเงินไทย เนื่องจากภัยคุกคามทางไซเบอร์มีการพัฒนารูปแบบที่หลากหลาย สามารถคาดเดาได้ยาก จึงมีการกำหนดทิศทางการดำเนินงานไว้เพื่อเตรียมความพร้อมรับมือกับปัญหาดังกล่าว ดังนี้

ประการแรก ยกระดับความทนทาน (Resilience) ต่อความเสี่ยงด้านเทคโนโลยีและ ภัยคุกคามทางไซเบอร์ของระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ของภาคการเงินให้ได้มาตรฐานสากล ซึ่ง ธปท. จะยกระดับการกำกับดูแลให้เป็นแบบ proactive แบบต่อเนื่องมากขึ้น โดยจัดทำ Self-Assessment Platform ตาม Cyber Resilience Assessment Framework (CRAF) เพื่อให้สถาบันการเงิน CII อาทิ NITMX, NCB, BATHNET, ICAS ผู้ให้บริการ e-payment และ non-bank ใช้ประเมินตนเอง พร้อมทั้งเชื่อมโยงข้อมูลจาก Platform นี้กับข้อมูลการประเมิน Cybersecurity จากภายนอก รวมทั้งกำกับดูแลให้มีการปิดช่องโหว่ที่สำคัญ ทั้งยังผลักดันให้องค์กรที่มีผลการประเมิน Cyber Inherent Risk ระดับที่สูงทำการทดสอบเจาะระบบของตนเอง

ประการสอง จัดทำแนวปฏิบัติเพื่อกำกับเทคโนโลยีใหม่ที่จะเกิดขึ้น และสภาพแวดล้อมที่เปลี่ยนแปลงไป เช่น AI, Blockchain และ Biometrics และจัดทำเกณฑ์กำกับดูแลความเสี่ยงจากการใช้เทคโนโลยีหรือโครงสร้างพื้นฐานร่วมกัน และความเสี่ยงจากการกระจุกตัว (Concentration Risk) ของการใช้บริการจากผู้ให้บริการเพียงบางราย เช่น Cloud Computing

ประการสาม ยกระดับการกำกับดูแลข้อมูลส่วนบุคคลและธรรมาภิบาลการใช้ข้อมูลของผู้ให้บริการทางการเงิน เพื่อรองรับความเสี่ยงจากการใช้ข้อมูลรายธุรกรรมที่เพิ่มขึ้น โดย ธปท. จะจัดทำแนวปฏิบัติ Data governance เพื่อให้ใช้เป็นแนวทางในการกำกับดูแลข้อมูล และปีต่อ ๆ ไปจะมีการให้ สง. CII และผู้ให้บริการ e-payment ประเมิน Data governance ด้วยตนเอง โดยใช้ Self-Assessment Platform เช่นเดียวกับการประเมิน Cyber resilience

ประการสี่ สร้างกลไกความร่วมมือและการแลกเปลี่ยนข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ กับหน่วยงานกำกับดูแล และผู้ที่เกี่ยวข้องในภาคการเงินให้เข้มแข็งขึ้น และขยายไปยังภาคธุรกิจอื่น ภายในประเทศ อาทิ ภาคโทรคมนาคม ภาคพลังงานและสาธารณูปโภค สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (NCSA) และขยายความร่วมมือและแลกเปลี่ยนข้อมูลกับต่างประเทศเพิ่มเติม อาทิ มาเลเซีย สิงคโปร์ ออสเตรเลีย สหรัฐอเมริกา รัสเซีย และกลุ่มประเทศยุโรป รวมถึงกลุ่มหรือองค์กรในต่างประเทศ ได้แก่ Cybersecurity Resilience and Information Sharing Platform (CRISP) Operational Security Situational Awareness Teleconference (OSSAT) และ BIS

ประการห้า สร้างกลไกรองรับการพัฒนาบุคลากรในภาคการเงิน ที่เชื่อมโยงไปยังระดับประเทศและภูมิภาค เพื่อให้มีบุคลากรที่พร้อมรับมือความเสี่ยงด้านเทคโนโลยี และภัยคุกคามไซเบอร์ อาทิ จัดให้มี e-learning platform สำหรับเรื่อง IT risk และ cybersecurity ในภาคการเงิน จัดให้มี cyber range facility สำหรับพัฒนาทักษะการรับมือภัยคุกคามไซเบอร์สำหรับภาคการเงินทั้งในประเทศและภูมิภาค รวมทั้งมีโครงการร่วมกับภาคการศึกษาระดับอาชีวะและระดับมหาวิทยาลัย และหรือผู้เชี่ยวชาญจากภาคเอกชน เพื่อสร้างบุคลากร cybersecurity เข้าสู่ภาคการเงิน

ผู้วิจัยเห็นว่าจากแผนยุทธศาสตร์ฯ ล่าสุด ธปท. ยังคงให้ความสำคัญกับประเด็นทางไซเบอร์คล้าย ๆ แผนยุทธศาสตร์ครั้งก่อน อาทิ การยกระดับความมั่นคงของระบบ การสร้างความร่วมมือและการพัฒนาบุคลากร แต่มีการขยายขอบเขตให้ใหญ่มากขึ้น มองไปยังองค์กรอื่นนอกเหนือจากเฉพาะภาคการเงินภายในประเทศ ปรับตัวรองรับความท้าทายใหม่ ๆ ที่จะเข้ามาในอนาคตมากขึ้น

3.1.2 บทบาทจากการกำหนดมาตรการและนโยบายต่าง ๆ

จากการสัมภาษณ์เชิงลึกกลุ่มเจ้าหน้าที่ฝ่ายกำกับและตรวจสอบความเสี่ยงเทคโนโลยีสารสนเทศ ของ ธปท. พบว่า ธปท. ได้มีการกำหนดกรอบการปฏิบัติให้สถาบันการเงินทุกแห่งต้องปฏิบัติตาม เพื่อเป็นการเตรียมความพร้อมในการรับมือภัยคุกคามไซเบอร์ ซึ่งกรอบการปฏิบัติดังกล่าวคือ กรอบการประเมินความพร้อมในการรับมือภัยคุกคามไซเบอร์ (Cyber Resilience Assessment

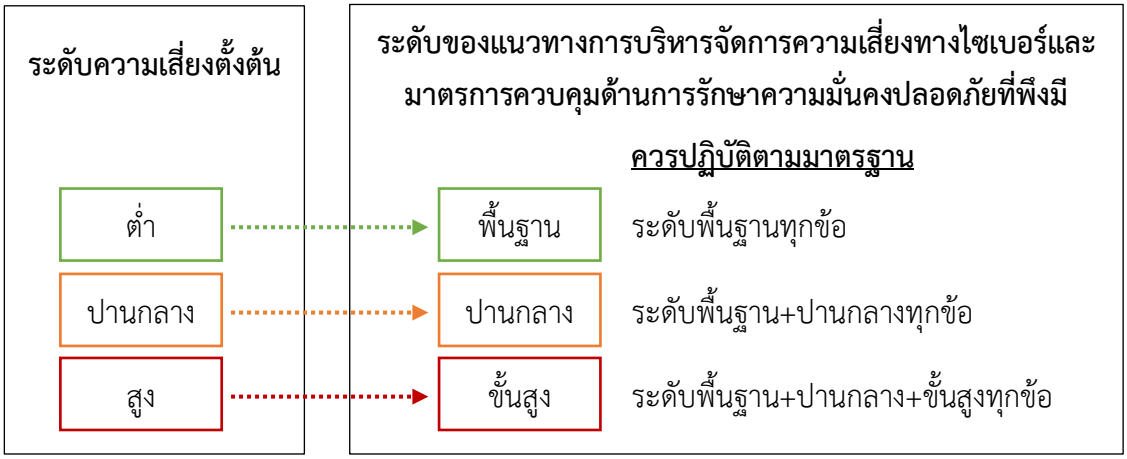
Framework)[3] โดยประกาศใช้เมื่อวันที่ 15 สิงหาคม 2562 เพื่อให้สถาบันการเงินใช้เป็นแนวทางในการประเมินตนเองใน 2 ด้าน ซึ่ง ธปท. กำหนดให้ประเมินและรายงานอย่างน้อยปีละ 1 ครั้งและทุกครั้งที่มีการเปลี่ยนแปลงเชิงโครงสร้างที่สำคัญ

จากการศึกษาผู้วิจัยพบว่าการประเมินระดับความเสี่ยงตั้งต้นทางไซเบอร์เป็นการประเมินโอกาสเกิดและผลกระทบจากภัยคุกคามไซเบอร์ แบ่งออกเป็น 5 ข้อ ได้แก่ 1. ประเภท ขอบเขต และปริมาณการใช้เทคโนโลยีสารสนเทศ การติดต่อสื่อสารรวมถึงการเชื่อมต่อของระบบเทคโนโลยีสารสนเทศ 2. ความหลากหลายของการให้บริการทางช่องทางอิเล็กทรอนิกส์ 3. รูปแบบ ปริมาณ และความซับซ้อนของผลิตภัณฑ์หรือบริการ จำนวนลูกค้า 4. ขนาดและลักษณะเฉพาะขององค์กร 5. ประวัติการถูกคุกคามไซเบอร์ โดยผลการประเมินจะแบ่งออกเป็น 3 ระดับ คือ ต่ำ ปานกลาง และสูง เมื่อประเมินครบทั้ง 5 ข้อจึงจะมาดูว่าผลประเมินระดับไหนมีจำนวนข้อมากที่สุด ก็จะสรุปว่าสถาบันการเงินนั้นมีความเสี่ยงรวมทั้งหมดเป็นระดับนั้น และเมื่อประเมินแล้วจะได้นำมาเป็นข้อมูลในการกำหนดแนวทางการบริหารจัดการความเสี่ยงให้สอดคล้อง ส่วนอีกด้านคือการประเมินระดับของแนวทางการบริหารจัดการความเสี่ยงทางไซเบอร์และมาตรการควบคุมด้านการรักษาความมั่นคงปลอดภัยที่พึงมี เพื่อดูว่าสอดคล้องกับระดับความเสี่ยงที่มีหรือไม่ ซึ่งควรสอดคล้องกับระดับความเสี่ยงที่ได้ประเมินไว้ในด้านแรก หรือมีช่องว่างในเรื่องใดบ้าง แบ่งออกเป็น 6 ข้อ ได้แก่ 1. กรอบการกำกับดูแล (Governance) 2. การระบุความเสี่ยง (Risk Identification) 3. การป้องกัน (Protection) 4. การเฝ้าระวังและตรวจจับ (Detection) 5. การตอบสนองต่อเหตุการณ์และการกู้คืน (Response and Recovery) 6. การบริหารความเสี่ยงด้านภัยคุกคามไซเบอร์ที่เกิดจากหน่วยงานภายนอก (Third party risk management) โดยแบ่งระดับความพร้อมออกเป็น 3 ระดับ คือ พื้นฐาน (Baseline) ปานกลาง (Intermediate) และขั้นสูง (Advanced) โดยมีการกำหนดเกณฑ์การประเมินแต่ละระดับของแต่ละข้อเอาไว้อย่างชัดเจนค่อนข้างมาก

ทั้งนี้ เจ้าหน้าที่ฝ่ายกำกับและตรวจสอบความเสี่ยงเทคโนโลยีสารสนเทศ กล่าวว่าในปัจจุบัน ธปท. ได้มีการจัดทำเป็น Template ในรูปแบบ Excel ให้สถาบันการเงินดาวน์โหลดและกำหนดให้หน่วยงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management) หน่วยงานกำกับการปฏิบัติตามหลักเกณฑ์ (Compliance) และหน่วยงานตรวจสอบภายใน (Internal Audit) ของสถาบันการเงินแต่ละแห่งเป็นผู้รับผิดชอบในการประเมิน

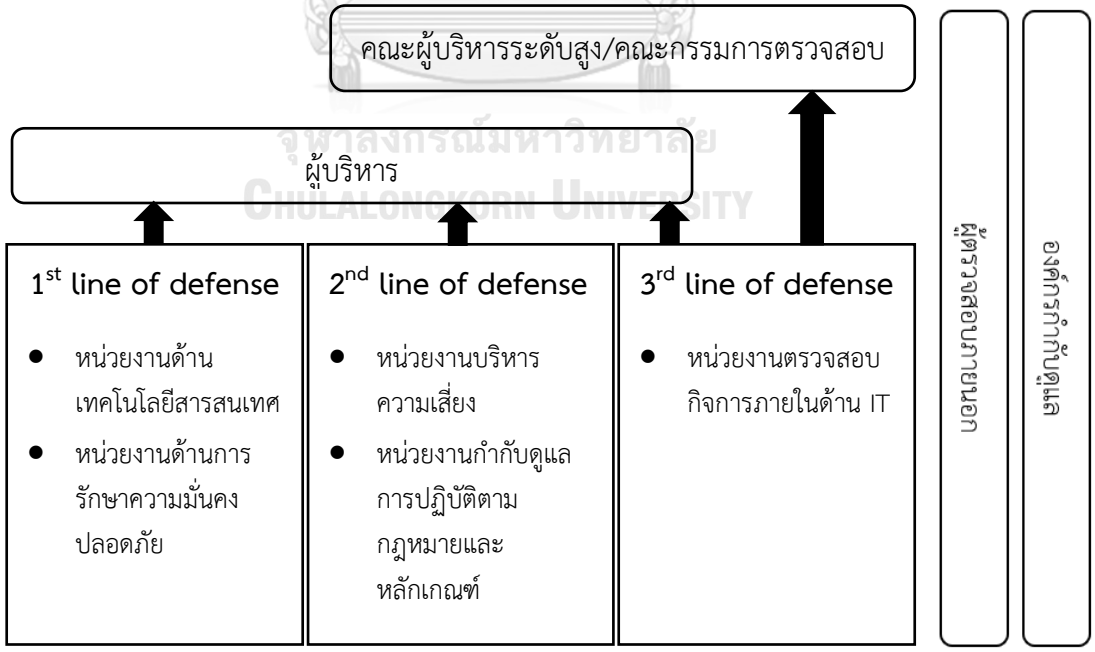
---

[3] ธนาคารแห่งประเทศไทย, **กรอบการประเมินความพร้อมในการรับมือภัยคุกคามไซเบอร์** [ออนไลน์], 2562. แหล่งที่มา https://www.bot.or.th/Thai/FinancialInstitutions/PruReg_HB/FSINotifications/Cyber%20resilience%20framework%202019.pdf



รูปภาพที่ 4 ระดับความเสี่ยงและระดับของแนวทางการบริหารจัดการความเสี่ยง

โครงสร้างในการกำกับดูแลการดำเนินงานที่เหมาะสมที่ ธปท. กำหนดคือควรเป็นไปตามหลักกลไกการป้องกันความเสี่ยง 3 ระดับ (Three lines of defense) ซึ่งผู้วิจัยเห็นด้วยอย่างมากเนื่องจากเป็นหลักการแบ่งแยกหน้าที่ที่ดีเพื่อบริหารความเสี่ยงตามหลักสากลอยู่แล้วที่ทุกองค์กรควรจะเป็น หลักการนี้หมายถึงการมีการถ่วงดุลอำนาจอย่างอิสระโดยมีการแบ่งแยกหน้าที่อย่างชัดเจน ถ้ามองในมุมสถาบันการเงินที่เกี่ยวข้องกับภัยคุกคามไซเบอร์ สามารถแบ่งแยกได้ออกเป็น



รูปภาพที่ 5 หน่วยงานที่รับผิดชอบตาม Three lines of defense

- 1st line of defense คือ หน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและผู้ใช้งานระบบเทคโนโลยีสารสนเทศ อาทิ หน่วยงานด้านเทคโนโลยีสารสนเทศ หน่วยงานด้านการรักษาความมั่นคงปลอดภัย
- 2nd line of defense คือ หน่วยงานที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ อาทิ หน่วยงานบริหารความเสี่ยง หน่วยงานกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์
- 3rd line of defense คือ หน่วยงานที่ทำหน้าที่ตรวจสอบการปฏิบัติงานและการบริหารความเสี่ยงของ 1st line และ 2nd line ได้แก่ หน่วยงานตรวจสอบกิจการภายในด้าน IT

ประกาศและแนวปฏิบัติที่ ธปท. จัดทำและขอความร่วมมือจากสถาบันการเงินให้ปฏิบัติตาม นอกเหนือจากกรอบการประเมินความพร้อมในการรับมือภัยคุกคามไซเบอร์ยังมีอีกหลายฉบับ โดยจากการศึกษาผู้วิจัยจะกล่าวถึงเฉพาะประกาศหรือแนวปฏิบัติที่สำคัญที่เกี่ยวข้องกับภัยคุกคามไซเบอร์โดยตรงเท่านั้น

> “ในปี 2560 – 2561 เป็นปีที่ ธปท. สร้างพื้นฐานด้านไอทีทั้งหมดในกับสถาบันการเงิน อดีตเราไม่เคยมี เกณฑ์เรามีน้อยมาก แต่ปัจจุบันสถาบันการเงินใช้ไอทีเยอะมาก ทุกอย่างใช้ไอทีหมด แต่ ธปท. ไม่ได้ดูเรื่องความเสี่ยงพวกนี้เลย เพราะฉะนั้น 2 ปีนั้น เป็นการสร้างพื้นฐานจึงออกเกณฑ์เรื่องการบริหารจัดการความเสี่ยงด้านไอที เกณฑ์เรื่อง Cyber และเกณฑ์ที่จำเป็น”
>
> (ผู้บริหารระดับสูงฝ่ายกำกับและตรวจสอบความเสี่ยงเทคโนโลยีสารสนเทศ)

ประกาศ สนส. 21/2562 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน[4] ประกาศ ณ วันที่ 1 ต.ค. 2562 มีผลบังคับใช้ 15 พ.ย. 2562 ซึ่งเป็นการปรับปรุงจากประกาศฉบับเก่าที่ออกเมื่อปี 2560 เพื่อปรับปรุงหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศเพื่อให้รองรับรูปแบบทางธุรกิจและสอดคล้องกับนวัตกรรมทางเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว โดยมีสาระสำคัญ คือ ธนาคารพาณิชย์ที่มีนัยต่อความเสี่ยงเชิงระบบในประเทศ (Domestic Systemically Important Banks: D-SIBs) และสถาบันการเงินที่มีความเสี่ยงตั้งต้นทางไซเบอร์ระดับสูง ต้องจัดให้มีผู้บริหารระดับสูงที่รับผิดชอบเรื่องบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศของสถาบันการเงิน (Chief Information Security Officer: CISO) รวมทั้งต้องมีการรายงานโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญประจำปีให้ ธปท. ทราบ ซึ่งได้ยกเลิกการต้องขออนุญาตล่วงหน้า ยกเว้นบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ยังคงต้องขออนุญาตก่อน ทั้งนี้สถาบันการเงินที่มีบริษัทในกลุ่มธุรกิจหรือ

---

[4] ธนาคารแห่งประเทศไทย, **ประกาศธนาคารแห่งประเทศไทย ที่ สนส. 21/2562 เรื่องหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน** [ออนไลน์], 2562. แหล่งที่มา https://www.bot.or.th/Thai/FIPCS/Documents/FOG/2562/ThaiPDF/25620272.pdf

บริษัทที่มีความเกี่ยวข้องกันและต้องการมีโครงสร้างการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศแบบรวมศูนย์ ไม่ว่าจะรวมอยู่ในต่างประเทศหรือต่างประเทศ ธปท. กำหนดให้สถาบันการเงินจะต้องขออนุญาตก่อนใช้โครงสร้างดังกล่าว

อย่างไรก็ตามจากหลักเกณฑ์ต่าง ๆ ที่กำหนดในประกาศ หากสถาบันการเงินเห็นว่าไม่สามารถปฏิบัติตามได้ ธปท. ก็อนุโลมให้สามารถยื่นขอผ่อนผันเป็นรายกรณี ผ่านระบบ e-Application ในเว็ปไซต์ ธปท. โดยระบุเหตุผล ความจำเป็นและแผนที่จะดำเนินการให้สามารถปฏิบัติได้ตามประกาศต่อไป

ประกาศ สนช. 11/2561 เรื่องนโนบายและมาตรการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ[5] ประกาศ ณ วันที่ 16 เมษายน 2561 และมีผลบังคับใช้ทันที ธปท. ประกาศออกมาเพื่อต้องการให้มีมาตรฐานในการกำหนดนโยบายและมาตรการความมั่นคงปลอดภัยทางระบบสารสนเทศและใช้เป็นแนวทางกำหนดวิธีปฏิบัติในการตรวจสอบและรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่เกี่ยวข้องกับระบบการชำระเงินที่มีความสำคัญ โดยประกาศได้กำหนดกรอบการออกนโยบายของสถาบันการเงินและแนวปฏิบัติเพื่อให้ใช้เป็นแนวทาง คือ อย่างน้อยในนโยบายต้องมีการพูดถึงการควบคุมการเข้าถึงและการพิสูจน์ตัวตนผู้ใช้ การรักษาความลับข้อมูลและความถูกต้องเชื่อถือได้ของระบบสารสนเทศ การรักษาสภาพความพร้อมใช้งานของการให้บริการ และการตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศ ธปท. กำหนดให้มีการตรวจสอบอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่านโยบายและมาตรการที่มีเป็นไปอย่างมีประสิทธิภาพจริง พร้อมทั้งส่งสำเนาผลการตรวจให้ ธปท. ด้วย

แนวปฏิบัติ ธปท. เรื่อง แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลัก (IT Best Practices Phase 1 and 2) เน้นธุรกรรมที่มีผลกระทบต่อประชาชนในวงกว้าง โดย Phase 1[6] เป็นการพูดถึงการทำธุรกรรมหลักของสถาบันการเงิน คือ ฝาก ถอน และโอนเงิน ซึ่งออกใช้เมื่อเดือนพฤศจิกายน 2556 เป็นการกำหนดแนวทางให้แต่ละสถาบันการเงินที่มีการออกแบบการควบคุมภายในที่แตกต่างหลากหลายให้มีมาตรฐานแนวปฏิบัติการควบคุม

---

[5] ธนาคารแห่งประเทศไทย, **ประกาศธนาคารแห่งประเทศไทย ที่ สนช. 11/2561 นโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ** [ออนไลน์], 2561. แหล่งที่มา https://www.bot.or.th/Thai/FIPCS/Documents/FPG/2561/ThaiPDF/25610093.pdf

[6] ธนาคารแห่งประเทศไทย, **แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลัก (IT Best Practices) Phase 1: ธุรกรรมฝาก ถอน และโอนเงิน** [ออนไลน์], 18 กุมภาพันธ์ 2563. แหล่งที่มา https://www.bot.or.th/Thai/FinancialInstitutions/PruReg_HB/RiskMgt_Manual/download/%E0%B9%81%E0%B8%99%E0%B8%A7%E0%B8%9B%E0%B8%8F%E0%B8%B4%E0%B8%9A%E0%B8%B1%E0%B8%95%E0%B8%B4%20IT%20Best%20Practices%20-%20Phase%20l.pdf

ภายในที่สอดคล้องกับมาตรฐานสากล เพื่อควบคุมความเสี่ยงรองรับธุรกรรมด้านเงินฝาก ถอน และโอนเงิน ผ่านช่องทางสาขา ATM และ Internet Banking ซึ่งการจัดทำแนวปฏิบัติฉบับนี้ได้มีการจ้างที่ปรึกษาภายนอก และรับฟังความเห็นจากธนาคารพาณิชย์ทุกแห่ง เพื่อให้แนวปฏิบัตินี้ยืดหยุ่นเหมาะสมกับบริบทของสถาบันการเงินไทยแต่ยังสอดคล้องกับมาตรฐานสากล อาทิ กรอบแนวทางการตรวจสอบเทคโนโลยี Global Technology Audit Guide (GTAG) ขององค์กรวิชาชีพการตรวจสอบภายใน (Institute of Internal Auditors: IIA) กรอบการควบคุมด้านความปลอดภัยเทคโนโลยีสารสนเทศ (ISO27001) ขององค์กรมาตรฐานสากล (International Organization for Standardization: ISO) และกรอบการบริหารจัดการด้านเทคโนโลยีสารสนเทศของหน่วยงาน The Information Systems Audit and Control Association (ISACA) และสามารถนำไปปฏิบัติใช้ได้จริง โดยแนวปฏิบัติสามารถแบ่งออกได้เป็น 2 หัวข้อหลัก คือ 1. แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของกระบวนการฝาก ถอน และโอนเงิน ไม่ว่าจะเป็นการควบคุมด้วยระบบ IT หรือการควบคุมด้วยระเบียบวิธีการปฏิบัติงาน เช่น การพิสูจน์ตัวตนลูกค้าจากบัตรประชาชนอิเล็กทรอนิกส์ การกำหนดสิทธิ์ให้พนักงานตามบทบาทหน้าที่ที่ได้รับเท่านั้น การพิสูจน์ตัวตนของผู้อนุมัติรายการด้วยวิธีการที่ปลอดภัย 2. แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบ IT ที่ใช้รองรับ โดยครอบคลุมโครงสร้างระบบ IT ที่สำคัญ เช่น Data Center ระบบเครือข่ายสื่อสาร ระบบช่องทางการให้บริการต่าง ๆ ซึ่งการควบคุมประกอบด้วย 1) การควบคุมการเข้าถึงระบบ (Access Control) ไม่ให้เข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต 2) การบริหารจัดการระบบ IT ให้มีความปลอดภัย (Security Management) เพื่อให้ระบบและข้อมูลมีความถูกต้อง 3) การบริหารจัดการระบบ IT ให้มีความพร้อม (Availability Management) ในการรองรับการทำธุรกรรมอย่างต่อเนื่อง

> “ตอนร่างแนวปฏิบัติ มีปัญหาจากการนำมาตรฐานของต่างประเทศมาประยุกต์ เนื่องจาก scale ของต่างประเทศและของไทยไม่เหมือนกัน เช่น ในสหรัฐอเมริกา จำนวนลูกค้า 1 แสนคนถือว่าต่ำ แต่ในไทยอาจจะถือว่าสูงแล้ว เพราะจำนวนประชากรไม่เท่ากัน เราจึงต้องนำมาปรับให้เหมาะสมด้วย”
>
> (เจ้าหน้าที่ฝ่ายกำกับและตรวจสอบความเสี่ยงเทคโนโลยีสารสนเทศ)

ทั้งนี้แนวปฏิบัติ Phase 2[7] ที่ออกมาตามหลังในเดือนธันวาคม 2557 พูดถึงธุรกรรมการเงินผ่านช่องทางอิเล็กทรอนิกส์ การให้บริการการเงินและการชำระเงินทางอิเล็กทรอนิกส์ (E-Banking

[7] ธนาคารแห่งประเทศไทย, **แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลัก (IT Best Practices) Phase 2: ธุรกรรมการเงินผ่านชองทางอิเล็กทรอนิกส การใหบริการการเงินและการชำระเงินทางอิเล็กทรอนิกส (E-Banking และ E-Payment)** [ออนไลน์], 18 กุมภาพันธ์ 2563. แหล่งที่มา https://www.bot.or.th/Thai/FinancialInstitutions/PruReg_HB/RiskMgt_Manual/download/%E0%B9%81%E0%B8%99%E0%B8%A7%E0%B8%9B%E0%B8%8F%E0%B8%B4%E0%B8%9A%E0%B8%B1%E0%B8%95%E0%B8%B4%20IT%20Best%20Practices%20-%20Phase%20II.pdf

และ E-Payment) เนื่องจาก ธปท. เห็นถึงอัตราการขยายตัวของธุรกรรมประเภทนี้ที่จะมีมากขึ้นในอนาคต ซึ่งความมั่นคงปลอดภัยนั้นเป็นจุดสำคัญที่จะสร้างความเชื่อมั่นให้กับผู้ใช้บริการ โดยแนวทางการจัดทำแนวปฏิบัติยังคงคล้ายคลึงกับ Phase 1 ยังคงอิงมาตรฐานสากลเช่นเดิม ซึ่งแนวปฏิบัติสามารถแบ่งออกได้เป็น 2 หัวข้อหลัก คือ 1. แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของกระบวนการทำธุรกรรมการเงินผ่านช่องทางอิเล็กทรอนิกส์ ครอบคลุมทั้งการให้บริการ E-Banking คือ Internet Banking หรือ Mobile Banking และการให้บริการชำระเงินทางอิเล็กทรอนิกส์ (E-Payment) เช่น บริการเงินอิเล็กทรอนิกส์ บริการชำระเงินระหว่างธนาคาร ตั้งแต่การสมัครใช้บริการ การทำรายการ จนถึงการชำระเงิน 2. แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบ IT ที่รองรับธุรกรรมทางอิเล็กทรอนิกส์ เนื่องจากธุรกรรมประเภทนี้มีการเชื่องโยงข้อมูลสู่ภายนอกองค์กรค่อนข้างมาก ความเสี่ยงด้านภัยคุกคามไซเบอร์จึงสูงขึ้นตาม ธปท. จึงได้จัดทำกรอบแนวปฏิบัติที่ดีสำหรับการบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์ ซึ่งการควบคุมแบ่งเป็น 3 ระดับ คือ 1) การกำกับดูแลความเสี่ยง (Cybersecurity Governance) 2) การบริหารจัดการความเสี่ยง (Cybersecurity Risk Management) 3) กระบวนการปฏิบัติงาน (Cybersecurity Operation) การป้องกัน การตรวจพบ การรับมือ และการกู้คืน ซึ่ง ธปท. ก็ต้องการให้สถาบันการเงินนำ IT Best Practice ทั้ง 2 ฉบับนี้ไปใช้ในการประเมินตนเอง นำไปเป็นตัวเทียบเคียงในการปรับปรุงกระบวนการทำงานและพัฒนาระบบให้ดียิ่งขึ้น ซึ่ง ธปท. เองก็ทราบดีว่าแนวปฏิบัติอาจจะยังไม่ครอบคลุมผลิตภัณฑ์หรือบริการบางอย่างของสถาบันการเงินเพราะมีการพัฒนาและเปลี่ยนแปลงอยู่ตลอดเวลาตามเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว ซึ่ง ธปท. ก็จะมีการทบทวนแนวปฏิบัติอย่างต่อเนื่องให้เท่าทัน

แนวปฏิบัติ ธปท. เรื่อง การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Implementation Guideline)[8] ธปท. ออกแนวปฏิบัติฉบับนี้เพราะเห็นว่าความเสี่ยงด้านเทคโนโลยีสารสนเทศนั้นมีความสำคัญมาก สามารถกระทบชื่อเสียงและความเชื่อมั่นที่ลูกค้ามีต่อสถาบันการเงินได้ด้วย ธปท. จึงได้กำหนดหลักให้สถาบันการเงินใช้เป็นแนวทางในการกำกับและบริหารจัดการความเสี่ยงให้เหมาะสม โดยเริ่มตั้งแต่การเตรียมความพร้อมของระบบเทคโนโลยีสารสนเทศให้พร้อมรับกับความเปลี่ยนแปลงที่อาจเกิดขึ้นในอนาคต โดยบทบาทของคณะกรรมการของสถาบันการเงินและผู้บริหารระดับสูงเกี่ยวกับเรื่องนี้ คือ ต้องร่วมสนับสนุนและผลักดันให้องค์กรมีกลยุทธ์และนโยบายที่เหมาะสมพร้อมรับมือกับภัยคุกคามทางเทคโนโลยีและทางไซเบอร์ รวมทั้งให้ทั้งองค์กรรู้จักตระหนักถึงความสำคัญในการบริหารความเสี่ยงเรื่องนี้ ให้ตระหนักว่าเป็นหน้าที่ของทุกคน

[8] ธนาคารแห่งประเทศไทย, **แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ** [ออนไลน์], 18 กุมภาพันธ์ 2563. แหล่งที่มา https://www.bot.or.th/Thai/FinancialInstitutions/PruReg_HB/RiskMgt_Manual/Documents/IT-RM_Implementation_Guideline.pdf.

ที่ต้องรับผิดชอบ ไม่ใช่ของบุคคลใดบุคคลหนึ่ง ดังนั้นสถาบันการเงินจึงควรมีการกำหนดกรอบการบริหารความเสี่ยงให้ครอบคลุมทั่วทั้งองค์กร ไม่ว่าจะเป็นเรื่องการกำหนดนโยบายที่จะต้องสอดคล้องกับระดับความเสี่ยงที่มี บทบาทความรับผิดชอบ การพัฒนาเครื่องมือและกระบวนการ รวมทั้งการพัฒนาความรู้และความเชี่ยวชาญในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ไม่ว่าจะเป็นคณะกรรมการ ผู้บริหารระดับสูง และบุคลากรทุกระดับ ต้องมีการพัฒนาอย่างต่อเนื่องเพื่อเพิ่มมุมมองความรู้ ความเชี่ยวชาญ และเท่าทันภัยคุกคามใหม่ๆ นอกจากนี้ ธปท. ยังมีการกำหนดโครงสร้างการกำกับดูแลให้สอดคล้องตามหลัก 3 lines of defense ตามที่ผู้วิจัยได้กล่าวถึงไปแล้วในข้างต้น

อย่างไรก็ตาม เจ้าหน้าที่ฝ่ายกำกับและตรวจสอบความเสี่ยงเทคโนโลยีสารสนเทศรายหนึ่ง ได้ให้ความเห็นว่า

> “นโยบายที่ ธปท. ออกเป็นเพียงแนวปฏิบัติ ไม่ทำตามไม่มีผลตามกฎหมาย เราไม่มีบทลงโทษ ของประเทศเราอ่อนกว่าประเทศอื่น หากจะผลักดันให้เป็นเกณฑ์ ต้องคุยกันอีกนาน และ Cyber มีความหลากหลาย ขนาด พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ ที่เขียนกว้างมากยังใช้เวลาตั้ง 20 ปี ดังนั้นสิ่งที่เราทำได้ตอนนี้ คือ การสร้างความตระหนัก ให้ความรู้”

3.1.3 บทบาทในการกำกับดูแลและตรวจสอบ

จากการศึกษาผู้วิจัยทราบว่าฝ่ายงานของ ธปท. ที่มีหน้าที่รับผิดชอบเกี่ยวกับภัยคุกคามไซเบอร์ของสถาบันการเงิน คือ ฝ่ายกำกับและตรวจสอบความเสี่ยงเทคโนโลยีสารสนเทศ หรือใช้ตัวย่อว่า ฝตท. ซึ่งหน้าที่ของฝ่ายงานนี้คือการกำหนดนโยบาย หลักเกณฑ์ และแนวปฏิบัติการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศและความเสี่ยงจากภัยคุกคามไซเบอร์ของสถาบันการเงิน รวมทั้งมีหน้าที่ตรวจสอบและวิเคราะห์ติดตามการดำเนินงานและบริหารความเสี่ยงด้านเทคโนโลยีของสถาบันการเงิน รวมถึงการวิเคราะห์เชิงลึกในประเด็นเทคโนโลยีที่มีความสำคัญต่อความเสี่ยงภาพรวมของระบบสถาบันการเงิน หรือระบบการชำระเงิน และไม่ว่าจะเป็นการให้ความเห็นในการพิจารณาคำขอกรณีสถาบันการเงินต้องการสร้างผลิตภัณฑ์ใหม่ๆ ที่อาจมีประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งจากการสัมภาษณ์เชิงลึกผู้บริหารระดับสูงฝ่ายกำกับและตรวจสอบความเสี่ยงเทคโนโลยีสารสนเทศ ของ ธปท. ได้อธิบายถึงแนวทางการตรวจสอบของ ฝตท. พบว่าการตรวจสอบของ ฝตท. นั้นแบ่งออกเป็นหลายส่วน

1) การตรวจสอบเจาะจงเฉพาะเรื่อง (Thematic)

เป็นการเลือกตรวจสอบเรื่องที่มีความเสี่ยงสูงหรือเรื่องใหม่ ๆ เพื่อให้ทันกับการเปลี่ยนแปลงทางเทคโนโลยี อย่างเช่นในปี 2562 จะเน้นตรวจสอบเรื่องการบริหารจัดการข้อมูลสารสนเทศ และการดูแลความเสี่ยงจากการนำเทคโนโลยีใหม่มาใช้ โดยกรอบที่ ฝตท. นำไปใช้ประเมินเรื่องการบริหารจัดการข้อมูลสารสนเทศของสถาบันการเงินนั้นได้อ้างอิงกรอบจากสมาคมบริหารจัดการข้อมูลระหว่าง

ประเทศ (The Data Management Association: DAMA) ซึ่งเป็นกรอบเดียวกับที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (Digital Government Development Agency: DGA) ใช้ โดย DGA เป็นหน่วยงานในสังกัดของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) กระทรวงวิทยาศาสตร์และเทคโนโลยี โดยกรอบนี้เน้น 2 เรื่อง คือ ธรรมภิบาลข้อมูล (Data Governance) และกระบวนการบริหารจัดการข้อมูล (Data Management Process) เนื่องจาก ธปท. เห็นว่าการโจมตีไซเบอร์ส่วนใหญ่ต้องการเจาะเพื่อเอาข้อมูลสำคัญ ไม่ว่าจะเพื่อเรียกค่าไถ่ ต้องการทำให้ระบบทำงานไม่ได้ หรือสร้างธุรกรรมปลอมเพื่อโอนเงินออก ดังนั้นยิ่งสถาบันการเงินใดที่มีข้อมูลเยอะยิ่งตกเป็นเป้า ธปท. จึงเห็นว่าการรักษาความปลอดภัยในเรื่องระบบข้อมูลนั้นสำคัญมาก โดยเฉพาะข้อมูลที่มีความอ่อนไหว

ซึ่งผู้บริหารระดับสูง ฝตท. ได้กล่าวว่า ผลจากการตรวจสอบสถาบันการเงินในปี 2562 ฝตท. ได้พบจุดบกพร่องของสถาบันการเงินหลายเรื่องโดยเฉพาะความพร้อมด้านธรรมภิบาลข้อมูลหรือการดูแลรักษาความปลอดภัยข้อมูลที่สถาบันการเงินส่วนใหญ่ยังอยู่ในระดับต่ำ ยังมีช่องโหว่บางอย่างที่ต้องพัฒนาเพิ่มเติม และกรอบการดูแลความเสี่ยงจากการนำเทคโนโลยีใหม่มาใช้ยังไม่ครบถ้วน ซึ่งจากการตรวจสอบพบว่าส่วนใหญ่เกิดจากกรอบและแนวทางการกำกับดูแลกำหนดการเข้าถึง การเชื่อมต่อและการรักษาความปลอดภัยยังไม่รัดกุมเพียงพอเทคโนโลยีใหม่ที่กล่าวถึง อาทิ เทคโนโลยีชีวมิติ (Biometrics) ระบบปัญญาประดิษฐ์ (Artificial Intelligence) การเรียนรู้ของคอมพิวเตอร์ (Machine Learning) บล็อกเชน (Blockchain) เป็นต้น

โดยในปี 2563 ฝตท. มีทิศทางการกำกับตรวจสอบแบบเจาะจงที่มุ่งเน้น 2 เรื่อง คือ 1) สถาปัตยกรรมของระบบไอที (IT Architecture) เพื่อพิจารณาว่าสามารถรองรับธุรกรรมของธุรกิจได้หรือไม่ และ 2) การพัฒนาของศูนย์ปฏิบัติการไซเบอร์ (SOC Maturity) เพื่อพิจารณาความสามารถว่าสามารถตรวจจับ ป้องกันภัยไซเบอร์ได้จริงหรือไม่ ซึ่งจะมีการออกไปลงพื้นที่จริงตรวจตามสถาบันการเงินต่าง ๆ ที่ได้มีการวางแผนจำนวน และเจาะจงสถาบันการเงินที่จะเข้าตรวจไว้ล่วงหน้าแล้ว

2) การออกเยี่ยมเยียน (Site Visit)

ฝตท. จะออกเยี่ยมเยียนสถาบันการเงินแห่งอื่นที่ไม่ได้ลงพื้นที่ตรวจเพื่อสอบทานเกี่ยวกับกลยุทธ์ทางไอทีของสถาบันการเงินนั้น ๆ การเปลี่ยนแปลงที่มีนัยสำคัญ ประเด็นการตรวจสอบที่เคยตรวจพบในอดีตในปีปัจจุบันก็จะไปติดตามความคืบหน้าในการแก้ไขปรับปรุง และประเด็นสำคัญอื่น ๆ หากมีเพิ่มเติมของแต่ละสถาบันการเงิน

3) การตรวจติดตามต่อเนื่อง (Offsite Monitoring)

เป็นการตรวจโดยไม่ต้องไปยังสถานที่ตั้งของสถาบันการเงิน สามารถปฏิบัติงานได้ที่ ธปท. โดยดูจากรายงานและข้อมูลที่สถาบันการเงินต้องนำส่งให้ ธปท. เป็นระยะตามที่ประกาศ หรือแนวปฏิบัติกำหนดไว้ โดยหากพบประเด็นจากการตรวจติดตามต่อเนื่องก็จะมีการขอข้อมูลเพิ่มเติม หรือออกไปตรวจยังสถาบันการเงิน

> “Cyber threat มาได้จากทุกทิศทุกทาง และ real time เราไม่มีทางปิดความเสี่ยงได้ 100% มันมีเทคนิคแพรวพราว มาได้ทุกรูปแบบ แล้วยิ่งในอนาคตสามารถพัฒนาไปได้อีกเรื่อย ๆ ดังนั้นผู้บริหารต้องมี vision อาจจะไม่ต้องรู้ด้านเทคนิค เพราะมันยากที่จะเข้าใจ แล้วค่อยให้ฝ่ายเทคนิคไปคิดให้ก็ได้ ถ้าเราคิดว่าปิดได้ 100% เมื่อไหร่ ก็โดนเมื่อนั้นแหละ”
>
> (เจ้าหน้าที่ฝ่ายกำกับและตรวจสอบความเสี่ยงเทคโนโลยีสารสนเทศ)

หนึ่งในรายงานที่สถาบันการเงินต้องจัดทำและนำส่งให้ ธปท. ทุกปีคือ รายงานการประเมินความเสี่ยงและความพร้อมการรับมือภัยคุกคามไซเบอร์ ตามกรอบการประเมินความพร้อมในการรับมือภัยคุกคามไซเบอร์ (Cyber Resilience Assessment Framework) ที่ผู้วิจัยเคยกล่าวไว้ในข้างต้นแล้ว ซึ่งเป็นการประเมินด้วยตนเอง (Self-assessment) ตามแบบฟอร์มที่ ธปท. กำหนด ซึ่ง ธปท. ได้นำส่งให้เป็นเอกสารอิเล็กทรอนิกส์ในรูปของ Excel และมีการกำหนดระยะเวลาการตอบกลับอย่างชัดเจน โดยในปี 2563 ธนาคารพาณิชย์ต้องส่งกลับภายในเดือนมีนาคม และสถาบันการเงินเฉพาะกิจต้องส่งกลับภายในเดือนเมษายน โดยการตรวจสอบเกี่ยวกับภัยคุกคามไซเบอร์นั้น ฝตท. ได้ลงพื้นที่ตรวจจริงในทุกสถาบันการเงินตั้งแต่ปี 2560 โดยอ้างอิงกรอบมาตรฐานสากล เช่น สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (NIST) ของสหรัฐอเมริกา ธนาคารกลางฮ่องกง (HKMA) เป็นต้น แล้วนำมาประยุกต์ให้เข้ากับบริบทการดำเนินงานของธุรกิจสถาบันการเงินในประเทศไทย โดยการตรวจสอบในครั้งนั้น ฝตท. ประเมินความเสี่ยงโดยธรรมชาติ (Inherent Risk) ก่อนลงพื้นที่ตรวจโดยการให้สถาบันการเงินประเมินตนเองเป็นข้อมูลเชิงคุณภาพ

> “เวลาธนาคารพาณิชย์ประเมินตนเองก่อนในเบื้องต้น ส่วนใหญ่พบว่า ประเมินดีเกินไป ไม่มีปัญหาอะไรเลย แต่พอไปตรวจจริง ๆ มีปัญหาเยอะมาก”
>
> (เจ้าหน้าที่ฝ่ายกำกับและตรวจสอบความเสี่ยงเทคโนโลยีสารสนเทศ)

> “ในปี 2564 มีแผนจะให้ทำ self-assessment ผ่านระบบ ทุกวันนี้ทำผ่าน excel ก็เหนื่อย เจ้าหน้าที่ต้องมานั่งดูทีละ excel ระบบสามารถดึงภาพรวม ทำวิเคราะห์ออกมาได้เลย ซึ่งต่างประเทศก็ใช้แบบนี้ โดยเพิ่งไปดูงานที่ออสเตรเลีย เมื่อปี 2562 ที่นั่นก็ทำเหมือนเรา เป็นการ confirm ว่าที่เราคิดมันถูกทาง ที่นั่นทำ self-assessment เหมือนกันโดยทำผ่านระบบ”
>
> (ผู้บริหารระดับสูงฝ่ายกำกับและตรวจสอบความเสี่ยงเทคโนโลยีสารสนเทศ)

ซึ่ง ฝตท. ก็จะขอข้อมูลเพิ่มเติมหลังจากส่งผลประเมินมาให้ เพื่อที่จะนำข้อมูลทั้งหมดมาประเมินเองอีกครั้งก่อนจะนำหารือกับสถาบันการเงิน เนื่องจากการควบคุมจะเข้มขนาดไหนขึ้นอยู่กับความเสี่ยงของแต่ละสถาบันการเงิน ปัจจัยที่มีผลต่อความเสี่ยง อาทิ ขนาดของสถาบันการเงิน สถาบันการเงินขนาดใหญ่จะเสี่ยงมากว่าสถาบันการเงินขนาดเล็ก รวมถึงจำนวนผลิตภัณฑ์ที่มี หรือช่องทางการเข้าถึงหรือติดต่อกับสถาบันการเงิน เป็นต้น ปัจจัยที่ใช้พิจารณานี้มีประมาณ 10 หัวข้อ

หากสถาบันการเงินมีความเสี่ยงมาก การตรวจก็จะยิ่งเข้มข้นขึ้นมากตามไปด้วย ซึ่งหลังจากการเข้าตรวจสอบเมื่อปี 2560 นั้นทาง ธปท. ก็ไม่ได้มีการลงพื้นที่ตรวจในเรื่องนี้อีกเลย แต่จะเป็นการให้ประเมินด้วยตนเองแล้วส่งมาที่ ธปท. แทน และติดตามคอยดูเหตุการณ์ที่อาจเกิดขึ้นอยู่ห่าง ๆ หากมีประเด็นสำคัญจึงจะเข้าไปตรวจเฉพาะเรื่องนั้นเพิ่มเติม

3.1.4 บทบาทการให้ความรู้แก่ภาคประชาชน

จากการสัมภาษณ์ผู้บริหารระดับสูง ฝตท. พบว่า ธปท. ให้ความสำคัญกับการให้ความรู้เกี่ยวกับภัยคุกคามไซเบอร์อย่างมาก เนื่องจากมองว่าความปลอดภัยทางไซเบอร์จะเกิดขึ้นได้ต่อเมื่อมีระบบนิเวศที่ส่งเสริมให้เกิดความรู้ความเข้าใจ โดยเฉพาะการป้องกันตนเองขั้นพื้นฐาน เพราะปัญหาภัยคุกคามไซเบอร์ไม่สามารถแก้ไขได้ด้วยคนใดคนหนึ่ง แต่ต้องเกิดจากความร่วมมือร่วมใจของทุกคนในระบบนิเวศนี้ ไม่ว่าจะเป็นประชาชนผู้ใช้บริการ สถาบันการเงิน และโครงสร้างพื้นฐานต่าง ๆ รวมถึงตัวผู้กำกับดูแลเช่น ธปท. เอง รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง อาทิ กสทช. หน่วยงานป้องกันและปราบปรามผู้กระทำผิด เป็นต้น

โดย ธปท. ให้ความรู้ตามความเหมาะสมของกลุ่มคนแต่ละกลุ่มซึ่งไม่เหมือนกัน

1) กลุ่มคนจากธนาคารกลางต่างประเทศ สถาบันการเงินและหน่วยงานกำกับดูแล

ในกลุ่มนี้ ธปท. จะมีทั้งการให้ความรู้โดยตรง ได้แก่ ส่งตัวแทนเป็นวิทยากรงานสัมมนาที่องค์กรอื่นจัดขึ้น เช่น งานสัมมนา Thailand Cybersecurity Week 2017 ที่จัดขึ้นโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์กรมหาชน) (สพธอ.) รวมทั้งจัดประชุมให้แก่สถาบันการเงินให้มาเข้าร่วมที่ ธปท. เช่น หากเป็นผู้บริหารสถาบันการเงินระดับสูง จะให้ความรู้ในเชิงการควบคุมดูแลการบริหารจัดการ และการรับมือในภาพรวม หากเป็นผู้ปฏิบัติงานของสถาบันการเงิน จะให้ความรู้ในเชิงเทคนิค การรับมือหากเกิดภัยคุกคามไซเบอร์ ทั้งมีการจัดการประชุมเชิงปฏิบัติการ (Workshop) ใน ธปท. โดยสมมติหากเกิดเหตุการณ์ขึ้นจริงแต่ละคนมีหน้าที่ที่จะต้องทำอะไรบ้าง เพื่อซักซ้อมกับผู้บริหารสถาบันการเงินทุกไตรมาส และร่วมกับผู้ปฏิบัติการทุกเดือน

หรืออาจเป็นในมุมของการแบ่งปัน แลกเปลี่ยนข้อมูลความรู้ระหว่างกัน เพื่อนำมุมมองและแนวปฏิบัติที่แตกต่างกันมาประยุกต์ให้องค์กรของตนมีการดำเนินการที่ดียิ่งขึ้น ไม่ว่าจะภายในประเทศหรือต่างประเทศ เช่น การประชุมระหว่างผู้ว่าการธนาคารกลางแต่ละประเทศ

2) กลุ่มประชาชน

ธปท. จะมีการให้ความรู้ที่เกี่ยวข้องกับการปฏิบัติตนในชีวิตประจำวันเพื่อสร้างความตระหนักเกี่ยวกับการป้องกันภัยคุกคามไซเบอร์ บางครั้งก็จะให้ความรู้เชิงวิชาการเพื่อเสริมสร้างความรู้ผ่านช่องทางต่าง ๆ มากมาย ได้แก่

เว็บไซต์ของศูนย์คุ้มครองผู้ใช้บริการทางการเงิน (ศคง.) www.1213.or.th หรือเฟสบุ๊ค ชื่อ “ศคง. 1213” ซึ่งหมายเลข 1213 เป็นเบอร์โทรศัพท์ที่ใช้โทรติดต่อ ศคง. เพื่อขอคำปรึกษาหรือร้องเรียนเกี่ยวกับบริการทางการเงิน ซึ่งเว็บไซต์หรือเฟสบุ๊คนี้จะมีการลงความรู้เกี่ยวกับการเงิน

รวมถึงการป้องกันตัวจากภัยคุกคามไซเบอร์ด้วยภาษาที่เข้าใจง่าย และเป็นเรื่องใกล้ตัวที่อาจพบเจอในชีวิตประจำวัน เพื่อให้ประชาชนสามารถนำไปปรับใช้ได้จริง เช่น การตั้งรหัส การตรวจสอบอีเมลปลอมจากสถาบันการเงิน เป็นต้น (ดังรูปที่ 5)

รูปภาพที่ 6 ตัวอย่างความรู้เกี่ยวกับภัยคุกคามไซเบอร์ที่ประชาสัมพันธ์ผ่านเฟสบุ๊ค

การจัดกิจกรรมหรือนิทรรศการให้ความรู้ที่ศูนย์การเรียนรู้ธนาคารแห่งประเทศไทย (Bank of Thailand Learning Center: BOTLC) ซึ่งภายในมีห้องสมุดและพิพิธภัณฑ์เงินตรา รวมทั้งมีพื้นที่สำหรับจัดกิจกรรมและนิทรรศการต่าง ๆ ซึ่งจะมีการจัดกิจกรรมและนิทรรศการให้ความรู้แก่ประชาชนทุกเดือน บุคคลที่สนใจสามารถเข้าร่วมรับฟังได้โดยไม่เสียค่าใช้จ่ายใด ๆ โดยติดตามข่าวสารและกิจกรรมได้ผ่านทางเว็บไซต์ www.botlc.or.th จะมีการอัพเดทข้อมูลเป็นระยะ ซึ่งการจัดกิจกรรมให้ความรู้นี้มีหัวข้อที่เกี่ยวข้องกับภัยคุกคามไซเบอร์ เช่น Trend ความปลอดภัยไซเบอร์และการใช้ชีวิตในยุคดิจิทัล ซึ่งเชิญวิทยากรมาจากภายนอก ธปท. (ดังรูปที่ 6-7)

รูปภาพที่ 7 ศูนย์การเรียนรู้ธนาคารแห่งประเทศไทย และพื้นที่จัดกิจกรรม

รูปภาพที่ 8 ตัวอย่างประชาสัมพันธ์กิจกรรมให้ความรู้

การจัดสัมมนาโดย ธปท. ภายในพื้นที่ ธปท. เช่น ธปท. ร่วมกับสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลากหลักทรัพย์ (ก.ล.ต) สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) สมาคมธนาคารไทย และสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) จัดงาน Financial Cybersecurity Boot Camp เป็นประจำทุกปี ปีละ 1 ครั้ง เช่น ปี 2562 จัดระหว่างวันที่ 1-3 พฤศจิกายน 2562 เป็นการจัดให้กับนิสิตนักศึกษาที่มีความสนใจด้าน Cybersecurity เพื่อให้ได้เรียนรู้ผ่านประสบการณ์จริงจากผู้เชี่ยวชาญใน

ภาคการเงิน รวมทั้งได้แสดงศักยภาพผ่านการแข่งขันป้องกันและโจมตีด้านภัยคุกคาม ไซเบอร์ระหว่างกันด้วยระบบจำลอง (ดังรูปที่ 8)

รูปภาพที่ 9 การจัดกิจกรรม Financial Cybersecurity Boot Camp 2561 – 2562

ที่มา: https://www.bot.or.th/Thai/AboutBOT/Activities/Pages/FinancialBootCamp_2019.aspx และ https://www.bot.or.th/Thai/AboutBOT/Activities/Pages/BOT_FCBC.aspx

บทที่ 4
การสร้างความร่วมมือระหว่างกลุ่มสถาบันการเงินในการกำหนดมาตรการป้องกันอาชญากรรมไซเบอร์

ในส่วนของความร่วมมือระหว่างกลุ่มสถาบันการเงิน ผู้วิจัยได้ทำการศึกษาจากการสัมภาษณ์ผู้ที่มีส่วนเกี่ยวข้องและนำข้อมูลมาเขียนเชิงพรรณนา โดยสามารถแบ่งเนื้อหาออกเป็นหัวข้อย่อย ๆ เป็น 3 ส่วน ดังนี้

4.1 การสร้างความร่วมมือและสร้างพันธมิตรกับองค์กรอื่นทั้งภายในและต่างประเทศ

ข้อมูลจากการสัมภาษณ์ผู้บริหารระดับสูง และกลุ่มเจ้าหน้าที่ ฝตท. ทำให้ผู้วิจัยสรุปได้ว่าความร่วมมือที่ ธปท. ได้ดำเนินการกับองค์กรภายนอกนั้น สามารถแบ่งออกเป็น 3 กลุ่ม ดังนี้

4.1.1 กลุ่มความร่วมมือกับสถาบันการเงิน

ธปท. ได้พยายามผลักดันให้มีศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร หรือ Thailand Banking Sector CERT (TB-CERT) เพื่อทำหน้าที่เป็นหน่วยงานกลางที่คอยดูแลรับมือภัยไซเบอร์ โดยให้สถาบันการเงินต่าง ๆ เข้ามาเป็นสมาชิก รวมทั้งคอยอบรมให้ความรู้ หรือแบ่งปันข้อมูลภัยไซเบอร์ที่สมาชิกแต่ละแห่งพบเจอให้สมาชิกรายอื่นได้รับทราบเพื่อระมัดระวังตนเอง อย่างไรก็ตาม ธปท. ไม่ได้เข้าร่วมเป็นสมาชิกกลุ่มความร่วมมือดังกล่าว เนื่องจาก ธปท. เห็นว่าตนเองนั้นเป็นผู้กำกับดูแล หากเข้าร่วมเป็นสมาชิกอาจทำให้สถาบันการเงินที่เป็นสมาชิกอื่น ๆ เกิดความไม่สบายใจ เมื่อประสบเหตุภัยไซเบอร์จะไม่กล้าเปิดเผยและแบ่งปันข้อมูลกันเพราะกลัว ธปท. จะรับทราบและถือเป็นความผิด ดังนั้น ธปท. จึงเห็นว่าควรปล่อยให้สถาบันการเงินแลกเปลี่ยนข้อมูลกันเอง

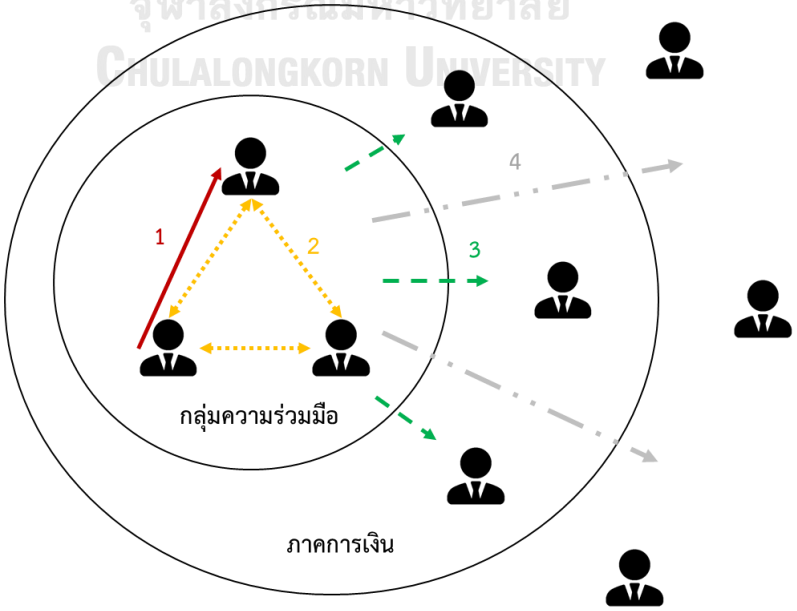
โดยจุดเริ่มต้นของการคิดจะจัดตั้ง TB-CERT เกิดจากในปี 2558 เกิดเหตุการณ์ Distributed Denial-of-Service (DDoS) ในสถาบันการเงิน 4-5 แห่ง และสถาบันการเงินเหล่านี้เริ่มมีการปรึกษาหารือและเปลี่ยนข้อมูลระหว่างกัน จึงเป็นจุดประกายความคิดให้ ธปท. เกิดแนวคิดว่าสถาบันการเงินควรสร้างความร่วมมือกัน และจากการไปดูงานที่ต่างประเทศถึงการรับมือภัยไซเบอร์ พบว่าไม่มีประเทศไหนรับมือภัยนี้เองด้วยตัวคนเดียว เพราะจะไม่สามารถบริหารจัดการได้ทันท่วงที จึงเห็นความจำเป็นที่จะต้องจัดตั้งกลุ่มความร่วมมือเพื่อรับมือเมื่อเกิดภัยไซเบอร์ ซึ่ง ธปท. เองก็เห็นว่าการมีสมาชิกที่หลากหลายนั้นทำให้มีข้อดีจากการที่สมาชิกบางแห่งที่มีเทคโนโลยีที่พัฒนาที่ก้าวไกลกว่าแห่งอื่น สมาชิกนั้นก็จะสามารถนำเทคนิคการรับมือมาเผยแพร่แบ่งปันแก่สมาชิกอื่นได้เพื่อให้ลองนำไปประยุกต์ใช้

ขั้นตอนแรกของการจัดตั้งนั้น ผู้ว่าการธนาคารแห่งประเทศไทย (ผว.) ได้เรียกประธานกรรมการบริหาร (Chief Executive Officer: CEO) ของธนาคารมาพูดคุยเพื่อหารือว่าควรเริ่มต้น

ความร่วมมือกัน ขณะเดียวกัน ฝตท. ฝ่ายงานของ ธปท. ที่รับผิดชอบดูแลการตรวจสอบด้านเทคโนโลยีก็เริ่มศึกษารูปแบบแนวทางความร่วมมือกันของต่างประเทศ เช่น สหรัฐอเมริกา เนเธอร์แลนด์ ฯลฯ เพื่อวิเคราะห์ รวบรวม สรุปผล และส่งผลการศึกษาไปยังสมาคมธนาคารไทยให้ทราบรูปแบบความร่วมมือที่เป็นไปได้ อาทิ ร่วมมือกันระหว่างสถาบันการเงิน ร่วมมือกับองค์กรอื่น เป็นต้น ซึ่งทางสมาคมธนาคารไทยได้รับไปปฏิบัติงานต่อ โดยเริ่มจากสร้างกลุ่มความร่วมมือเป็นกลุ่มเล็ก ๆ เรียกว่า Information Sharing Group สมาชิกประกอบด้วยสถาบันการเงิน 7 แห่ง ซึ่งในเวลานั้นยังไม่ได้จดทะเบียนเป็น TB-CERT ซึ่งเป็นการให้สมาชิกทั้ง 7 แห่ง ร่วมมือกันวางแผนโครงสร้างและรูปแบบความร่วมมือระหว่างกัน เนื่องจากการร่วมมือกันนั้นไม่ง่ายอย่างที่คิด ไม่ใช่อยากเข้าร่วมก็สามารถเข้าร่วมได้เลย จะต้องมีการสมัครสมาชิก มีการกำหนดข้อตกลงและระเบียบ มีการอุดหนุนเงิน มีการกำหนดแนวทางการแบ่งปันข้อมูลข่าวสาร

จากการสัมภาษณ์เจ้าหน้าที่จากศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคธนาคาร (TB-CERT) ศึกษาผู้วิจัยพบว่า แนวทางการแบ่งปันข้อมูลข่าวสารนั้นมีความสำคัญอย่างมาก เพราะข้อมูลบางอย่างมีความอ่อนไหว จึงต้องมีการออกแบบแนวทางการแบ่งปันข้อมูล (The Traffic Light Protocol: TLP) เพื่อป้องกันข้อมูลความลับรั่วไหล โดยแนวทางนี้เป็นแนวทางตามมาตรฐานสากลทั่วไป และ TB-CERT ได้ออกแบบแบ่งออกเป็น 4 ระดับ คือ

1. แดง หมายถึงข้อมูลเป็นความลับสูงสุด จะแบ่งปันกันแค่ 2 คนที่เกี่ยวข้องเท่านั้น ให้ข้อมูลตัวต่อตัว และไม่บอกคนอื่นในกลุ่มสมาชิก
2. เหลือง หมายถึง ทุกคนในกลุ่มสมาชิกสามารถรับรู้ได้
3. เขียว หมายถึง สามารถเผยแพร่ข้อมูลออกไปนอกกลุ่มสมาชิกได้ แต่ยังคงอยู่ในภาคการเงินเท่านั้น
4. ขาว หมายถึง สามารถเผยแพร่ไปให้ใครก็ได้



รูปภาพที่ 10 แนวทางการแบ่งปันข้อมูล (The Traffic Light Protocol: TLP) ของ TB-CERT

และเมื่อกลุ่มความร่วมมือได้กำหนดสิ่งต่าง ๆ ที่กล่าวข้างต้นเรียบร้อยเป็นรูปเป็นร่างแล้ว ก็จะเริ่มเรียกสมาชิกมาเข้าร่วมเพิ่มเติม เริ่มจากเหล่าธนาคารพาณิชย์ไทยทั้ง 15 แห่งที่เป็นสมาชิกสมาคมธนาคารไทย และได้จัดตั้งเป็น TB-CERT ขึ้นมาอย่างเป็นทางการ เริ่มกระตุ้นเรื่องการแบ่งปันข้อมูลกันเองภายในโดยไม่ต้องมี ธปท. คอยกระตุ้นเหมือนเช่นแรกเริ่ม ที่แรกเริ่มนั้น ธปท. จะเข้าไปมีบทบาทในการถามไถ่ทุกเดือนว่ามีการแบ่งปันข้อมูล หรือพูดคุยกันบ้างหรือไม่ ซึ่งปัจจุบัน TB-CERT มีการจัดประชุมหารือทุกเดือน และมีการจ้างคนกลางที่มีความเชี่ยวชาญด้านการรักษาความปลอดภัยไซเบอร์มาช่วยเหลือการปฏิบัติงาน เพื่อให้สมาชิกเล็งเห็นประโยชน์ของกลุ่มความร่วมมือ ซึ่งจะส่งผลให้มีการแบ่งปันข้อมูลกันมากยิ่งขึ้น หลังจากดำเนินการไปสักระยะ TB-CERT ก็ได้ขยายสมาชิกเพิ่มอาทิ ธนาคารเฉพาะกิจ (Specialized Financial Institutions: SFIs) ผู้ให้บริการทางการเงินแต่ไม่ใช่สถาบันการเงิน (Non-Bank) ซึ่งจุดสำคัญที่จะให้มีการแบ่งปันข้อมูลระหว่างกัน คือ ความเชื่อใจ ซึ่งทาง TB-CERT ก็มีการจัดกิจกรรมร่วมกันทุกปี เช่น สัมมนาต่างจังหวัด ประชุมประจำเดือน จัดแข่งขันเจาะระบบ เป็นต้น เพื่อสร้างความสนิทสนมและมีมิตรสัมพันธ์ต่อกัน ปัจจุบันช่องทางการแบ่งปันข้อมูลใน TB-CERT ก็มีหลากหลายช่องทาง เช่น e-mail, web portal ภายในที่หน่วยงานได้พัฒนาขึ้น โดยการแบ่งปันข้อมูลจะระบุหรือไม่ระบุชื่อผู้ส่งก็ได้ และระบบจะมีการแจ้งเตือนเมื่อมีข่าวสารใหม่ ๆ

ทั้งนี้ตัว TB-CERT เองก็ได้สมัครสมาชิก CERT ของต่างประเทศเพื่อที่จะได้ข้อมูลจากต่างประเทศที่เป็นประโยชน์มาแบ่งปันให้กับสมาชิก ซึ่งการเข้าร่วมเป็นสมาชิก CERT ของต่างประเทศนั้น TB-CERT เองก็ต้องมีการปฏิบัติงานที่เป็นมาตรฐานเพื่อให้ CERT ต่างประเทศยอมรับและสามารถเข้าร่วมเป็นสมาชิกได้

4.1.2 กลุ่มความร่วมมือกับหน่วยงานอื่น ๆ ภายในประเทศ

ธปท. มีการลงนามบันทึกข้อตกลงความร่วมมือ (Memorandum of understanding: MOU) ด้านการยกระดับความพร้อมรับมือภัยคุกคามไซเบอร์ (CERT Readiness) กับองค์กรภาคธุรกิจการเงิน การลงทุน และประกันภัย ในปี 2559[1] กับองค์กรอีก 4 แห่ง ได้แก่ สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (สำนักงาน คปภ.) สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงานคณะกรรมการ ก.ล.ต.) สมาคมธนาคารไทย (TBA) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์กรมหาชน) (สพธอ.) โดยมีวัตถุประสงค์เพื่อร่วมมือกันเกี่ยวกับการกำหนดมาตรฐานและกรอบการบริหารจัดการเพื่อให้หน่วยงานมีแนวปฏิบัติที่มีมาตรฐาน ร่วมสร้างกลไกและรูปแบบการแลกเปลี่ยนข้อมูล ร่วมผลักดันให้เกิดความร่วมมือในการแก้ไขปัญหาภัยคุกคามและตั้ง Financial Sector CERT ร่วมผลักดันให้แต่ละหน่วยงานมีการจัดทำ

[1] “บันทึกข้อตกลงความร่วมมือด้านการยกระดับความพร้อมรับมือภัยคุกคามไซเบอร์ (CERT Readiness) ต่อภาคธุรกิจการเงิน การลงทุน และการประกันภัย,” 22 กันยายน 2559.

แผนรับมือและแผนการบริหารจัดการสื่อมวลชน รวมทั้งร่วมทดสอบและซ้อมรับมือตามที่กำหนดในแผน ร่วมกันพัฒนาบุคลากรให้มีความเชี่ยวชาญ และร่วมสร้างความตระหนัก ความเข้าใจถึงความเสี่ยงและวิธีป้องกันให้ประชาชนได้รับทราบ โดยข้อตกลงความร่วมมือนี้ไม่มีกำหนดสิ้นสุด จนกว่าจะมีหน่วยงานใดขอยกเลิก

ซึ่ง ธปท. มองว่าประเด็นเรื่องการสร้างบุคลากรที่เชี่ยวชาญทางไซเบอร์เป็นหัวใจสำคัญที่สุด เป็นเรื่องที่ทำได้ยากที่สุด เรื่องเทคนิคต่าง ๆ นั้นไม่ยากเท่ากรณีมีเทคนิคใหม่ ๆ หากมีงบประมาณ ก็สามารถจัดซื้อได้ เรื่องกระบวนการ หากไม่มีก็สามารถกำหนดขึ้นมาได้ แต่เรื่องคนมีปัญหาค่อนข้างมาก มีทั้งปัญหาขาดแคลนทรัพยากรบุคคล คนไม่มีความสามารถเพียงพอ คนไม่มีความรู้ อย่างไรก็ตามปัญหาเหล่านี้ก็ได้มีการกำหนดแนวทางในการแก้ไขแล้ว ได้แก่

<u>การแก้ไขปัญหาขาดแคลนทรัพยากรบุคคล</u>

จัดกิจกรรม Boot camp ทุกปี ปีละ 1 ครั้ง เริ่มตั้งแต่ปี 2560 โดยคัดเลือกนิสิต นักศึกษามหาวิทยาลัยปีการศึกษาที่ 3 และ 4 ที่มีความสามารถ ผ่านการสอบคัดเลือก มาทำกิจกรรมร่วมกันและสังเกตการณ์ขณะทำกิจกรรมว่าเด็กคนไหนมีความโดดเด่น มีความสามารถก็จะสนับสนุนและผลักดันให้มาทำงานต่อในภาคการเงิน

<u>การแก้ไขปัญหาคนไม่มีความสามารถ</u>

จัดอบรมให้ความรู้ โดยมี TB-CERT เป็นหน่วยงานหลักในการดำเนินงานการอบรมเชิงเทคนิค และจัดแข่งขัน Cyber Game

<u>การแก้ไขปัญหาคนไม่มีความรู้</u>

ร่วมกันสร้างความตระหนัก (Awareness) โดยเกณฑ์ของ ธปท. มีการกำหนดให้สถาบันการเงินทุกแห่งมีหน้าที่สร้างความตระหนักให้กับพนักงานในองค์กรและประชาชน

ธปท. มองว่ากลุ่มคนที่มีความสำคัญและส่งผลกระทบมากที่สุดหากไม่มีความรู้ คือ คณะผู้บริหารระดับสูง (Board of Director) ของสถาบันการเงิน เนื่องจากการดำเนินงานเพื่อให้สัมฤทธิ์ผลอย่างรวดเร็วโดยทั่วไปมักต้องเกิดจากผู้บริหารเห็นความสำคัญ และผลักดันให้เกิดเป็นนโยบายรูปธรรม หรือปลูกฝังเป็นวัฒนธรรมขององค์กร หรือเรียกว่า Tone from the top หากผู้บริหารไม่เห็นความสำคัญของมาตรการความมั่นคงปลอดภัยทางไซเบอร์ การจัดสรรงบประมาณ บุคลากร เครื่องมืออาจจะไม่เหมาะสม รวมถึงว่าแม้ ธปท. จะออกเกณฑ์ที่ครอบคลุมและมีประสิทธิภาพขนาดไหน หากผู้บริหารระดับสูงของสถาบันการเงิน ไม่ตื่นตัว ก็จะทำให้เกิดผลในทางปฏิบัติได้ยาก ธปท. จึงพยายามที่จะสร้าง Tone from the top ให้กับสถาบันการเงิน โดยการให้ความรู้แก่ผู้บริหารระดับสูง ให้รู้สึกว่าเป็นเรื่องใกล้ตัวที่ต้องระมัดระวัง เพราะนอกจากจะต้องสูญเสียชื่อเสียงแล้ว ก็อาจจะต้องเสียเงินมูลค่าหลายร้อยหรือพันล้านบาท ซึ่งในห้วงระยะเวลา 3 - 4 ปี ที่ผ่านมา ธปท. ได้มีการดำเนินงานจัดโครงการให้ความรู้ผู้บริหารระดับสูงมาโดยตลอด

ในปีที่ 1 ได้มีการเชิญผู้บริหารระดับสูงให้เข้าร่วมสัมมนาที่ ธปท.

ในปีที่ 2 ได้มีการบรรจุหลักสูตร Cyber Security สำหรับผู้บริหารไว้ในหลักสูตรของสมาคมส่งเสริมสถาบันกรรมการบริษัทไทย (IOD)

ในปีที่ 3 เชิญผู้บริหารระดับสูงของสถาบันการเงินเข้าอบรมหลักสูตรที่ ธปท. จัดอบรมทั้งหมด 6 หลักสูตร ซึ่งแต่ละหลักสูตรจะแบ่งเป็นกิจกรรมให้ความรู้ทางวิชาการ ในช่วงครึ่งวันเช้าและอีกในช่วงครึ่งวันบ่ายจะเป็นการเล่นเกมสมมติเหตุการณ์ (Simulation) เมื่อมีการโจมตีทางไซเบอร์เกิดขึ้น ผู้บริหารจะต้องมีการตอบสนองอย่างไรบ้าง เพื่อให้เกิดความเข้าใจในการบริหารเหตุการณ์ รู้ในหลักขั้นตอนการรับมือ และท้ายสุด ธปท. ได้มอบคู่มือสำหรับการปฏิบัติงานสำหรับผู้บริหารระดับสูง ไว้ใช้เป็นแนวทางในการรับมือและตอบสนองเมื่อเกิดเหตุ

ความรู้ที่จัดอบรมให้เพื่อสร้างความตระหนักนั้น อาจเป็นการนำแฮกเกอร์ (Hacker) มาบรรยายวิธีการทำงานให้ฟังเพื่อให้รู้สึกตื่นกลัว หลังจากนั้นจึงนำผู้รับมือภัยไซเบอร์ที่มีความรู้ความเชี่ยวชาญมาบรรยายให้ความรู้ต่อเนื่อง เพื่อให้เข้าใจว่าสิ่งที่น่ากลัวนั้นสามารถบริหารจัดการได้ หากคุณมีการเตรียมความพร้อมที่ดีพอ

นอกเหนือจากการสร้าง Tone from the top แล้วสถาบันการเงิน ก็ต้องสร้างความตระหนักรู้ให้กับพนักงานในส่วนระดับปฏิบัติการไปควบคู่กัน

นอกจาก ธปท. จะสร้างความร่วมมือกับภาคการเงินในประเทศแล้ว ธปท. ก็ยังสร้างความร่วมมือกับภาคธุรกิจอื่น ได้แก่

สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) เป็นการร่วมมือกันอย่างเป็นทางการ ลงนามร่วมกันระหว่างผู้ว่าการธนาคารแห่งประเทศไทย กับเลขาธิการ กสทช. โดยจะมีการประชุมร่วมกันอยู่เป็นประจำเกี่ยวกับ Mobile Banking ซึ่งกำลังร่วมมือกันกำหนดกระบวนการรับมือภัยไซเบอร์ร่วมกันระหว่าง ธปท. และ กสทช.

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ซึ่งเป็นหน่วยงานที่รับผิดชอบดูแลภัยไซเบอร์ของประเทศ

เจ้าของเทคโนโลยีต่าง ๆ เป็นการร่วมมืออย่างไม่เป็นทางการ บางแห่งจะมีการนัดอัพเดทเทคโนโลยีใหม่ ๆ ร่วมกันทุกเดือน บางแห่งเป็นบริษัทที่ให้บริการแก่สถาบันการเงิน ทำให้ ธปท. ได้รู้เท่าทันเทคโนโลยีของสถาบันการเงิน หรือบางครั้งจะขอความอนุเคราะห์ผู้เชี่ยวชาญมาช่วยพิจารณาการออกเกณฑ์กำกับดูแลใหม่ ๆ เพื่อให้ได้มุมมองจากคนที่หลากหลาย

อย่างไรก็ตาม ธปท. มีการลงนามบันทึกข้อตกลงความร่วมมือ (Memorandum of understanding: MOU) ด้านการยกระดับความพร้อมรับมือภัยคุกคามไซเบอร์ (CERT Readiness) กับองค์กรภาคธุรกิจการค้า อุตสาหกรรม และโครงสร้างพื้นฐานสำคัญของประเทศ ในปี 2559[2] กับ

[2] “บันทึกข้อตกลงความร่วมมือด้านการยกระดับความพร้อมรับมือภัยคุกคามไซเบอร์ (CERT Readiness) ต่อภาคธุรกิจ การค้า อุตสาหกรรม และโครงสร้างพื้นฐานสำคัญของประเทศ,” 22 กันยายน 2559.

องค์กรอีกทั้งหมด 17 แห่ง ได้แก่ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (สำนักงาน กสทช.) สำนักงานคณะกรรมการกำกับกิจการพลังงาน (สำนักงาน กกพ.) สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงานคณะกรรมการ ก.ล.ต.) สมาคมผู้ให้บริการอินเทอร์เน็ตไทย (TISPA) สภาหอการค้าแห่งประเทศไทย (BoT) สภาอุตสาหกรรมแห่งประเทศไทย (ส.อ.ท.) สมาคมธนาคารไทย (TBA) สมาคมโทรคมนาคมแห่งประเทศไทยในบรมราชูปถัมภ์ (สทค.) สมาคมประกันชีวิตไทย (TLAA) สมาคมประกันวินาศภัยไทย (TGIA) ตลาดหลักทรัพย์แห่งประเทศไทย (ตลท.) บริษัท การบินไทย จำกัด (มหาชน) (บกท.) บริษัท ปตท. จำกัด (มหาชน) (ปตท.) การไฟฟ้านครหลวง (กฟน.) การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) การไฟฟ้าส่วนภูมิภาค (กฟภ.) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) โดยมีวัตถุประสงค์เพื่อร่วมสร้างความตระหนักโดยการให้ความรู้และสร้างวัฒนธรรมองค์กรเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ร่วมส่งเสริมการใช้มาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ในองค์กร ร่วมผลักดันให้เกิดความร่วมมือในการแก้ไขปัญหาภัยคุกคามและตั้ง Sector-based CERT ร่วมประสานงานแก้ไขปัญหาภัยคุกคามไซเบอร์ทั้งการแจ้งเหตุและการรับมือเหตุ ร่วมบริหารจัดการสื่อในการเผยแพร่ข้อมูลสู่สาธารณะ ร่วมพัฒนาบุคลากรให้มีความเชี่ยวชาญ ซึ่งข้อตกลงความร่วมมือที่ได้จัดทำนี้ไม่มีกำหนดสิ้นสุด

4.1.3 กลุ่มความร่วมมือกับหน่วยงานต่างประเทศ

นอกจากหาพันธมิตรภายในประเทศแล้ว ธปท. มีการสร้างความร่วมมือกับธนาคารกลางหรือหน่วยงานที่รับผิดชอบดูแลด้าน Cyber Security ของต่างประเทศ ได้แก่ ฮ่องกง อิสราเอล สิงคโปร์ สวิตเซอร์แลนด์ และประเทศล่าสุด คือ รัสเซีย โดยมีทั้งแบบเป็นทางการและไม่เป็นทางการ โดยไม่มีการลงนามความร่วมมือกันไว้ แต่ตกลงจะทำภารกิจบางอย่างร่วมกัน อาทิ สวิตเซอร์แลนด์มีการตกลงมาช่วยทำระบบงานจำลองการฝึกด้านไซเบอร์ (Cyber Range) ตั้งแต่ปี 2562 และในปี 2563 จะมาช่วยในการกำหนดแนวทางการติดตั้ง Cyber Range เพื่อให้คนในกลุ่มอาเซียนเข้ามาใช้ในการฝึกรับมือภัยไซเบอร์

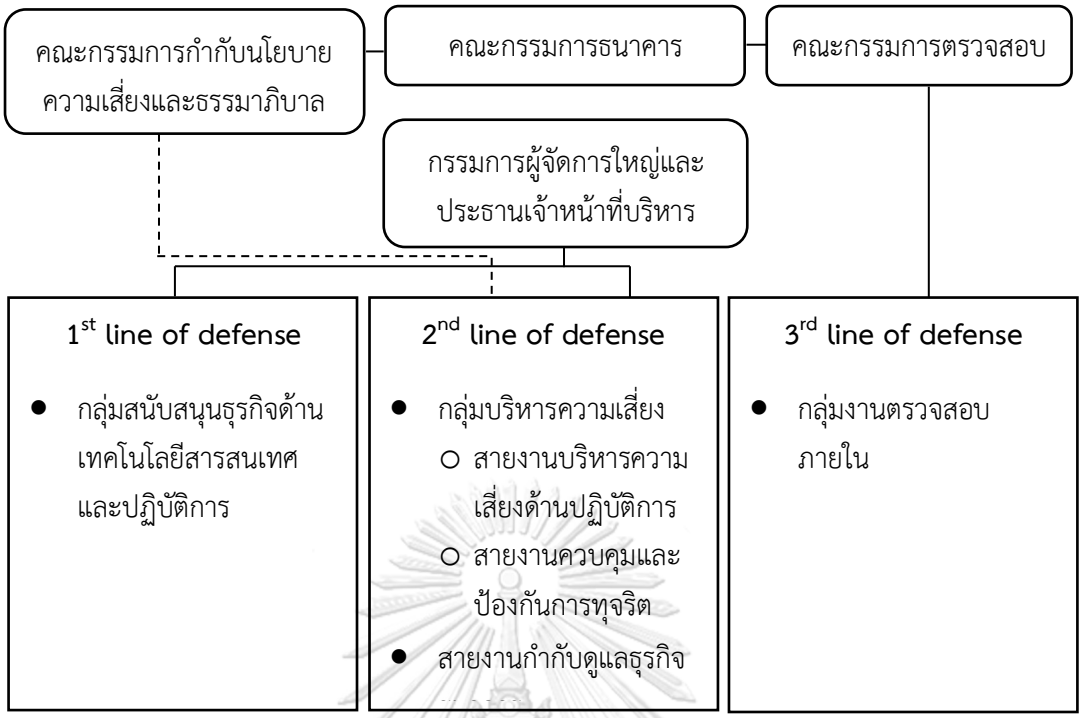
สำหรับประเทศที่มีการตกลงความร่วมมือกันอย่างเป็นทางการ มีการลงนามข้อตกลง MOU ร่วมกันกับ ธปท. ได้แก่ สิงคโปร์ ฮ่องกง และรัสเซีย ซึ่งมีการระบุว่าจะมีการช่วยเหลือด้านความมั่นคงปลอดภัยทางไซเบอร์แก่กัน มีการแลกเปลี่ยนข้อมูลข่าวสารระหว่างกัน รวมทั้งมีการแลกเปลี่ยนพนักงานเพื่อไปฝึกงานแลกเปลี่ยนประสบการณ์และความรู้ นอกจากนี้ ธปท. ยังเข้าร่วมเป็นสมาชิกกลุ่มความร่วมมือเพื่อการแลกเปลี่ยนข้อมูลระหว่างธนาคารกลางและหน่วยงานกำกับดูแลที่เกี่ยวข้อง (Central Banks, Regulators and Supervisory Entities Forum: CERES Forum) ซึ่งเป็นกลุ่มความร่วมมือแรกที่มีขึ้นสำหรับหน่วยงานกำกับดูแลทางการเงินในภูมิภาคที่มีการขยายไปเชื่อมต่อกับทั่วโลก มีสมาชิกประมาณ 20 ประเทศ ซึ่งมีการประชุมร่วมกันทุกเดือนผ่านการประชุมทางโทรศัพท์ (Conference Call) เพื่อแลกเปลี่ยนข้อมูลและเหตุการณ์ภัยคุกคาม รวมถึงข้อมูลเชิงนโยบาย และกรอบการกำกับดูแลภัยไซเบอร์อย่างเป็นระบบ

ธปท. ลงนามบันทึกข้อตกลงกับสถาบันพัฒนาเทคโนโลยีและวิทยาศาสตร์ประยุกต์ฮ่องกง (Hong Kong Applied Science and Technology Research Institute: ASTRI) ในปี 2559 เพื่อสร้างความร่วมมือด้านความปลอดภัยไซเบอร์และการพัฒนาเทคโนโลยีทางการเงิน (Fintech) เป็นเวลา 3 ปี โดย ASTRI เป็นองค์กรที่ก่อตั้งโดยรัฐบาลฮ่องกงที่มีทีมงานวิจัยและพัฒนาที่มีความเชี่ยวชาญด้าน Cybersecurity และ Fintech โดยมีขอบเขตความร่วมมือ ดังนี้

1. ยกระดับความปลอดภัยไซเบอร์ในระบบการเงินไทย ผ่านการสนับสนุนด้านเทคนิค และแบ่งปันความรู้และคำแนะนำเกี่ยวกับกรอบความมั่นคงปลอดภัยไซเบอร์ ข่าวกรอบ ไซเบอร์ การทดสอบไซเบอร์ หรือกิจกรรมความร่วมมืออื่น ๆ ที่เกี่ยวข้องกับความปลอดภัยไซเบอร์
2. ส่งเสริมการพัฒนาเทคโนโลยีทางการเงิน (Fintech) ทั้งในฮ่องกงและประเทศไทย ดำเนินการผ่านการเยี่ยมชม แบ่งปันประสบการณ์ ให้คำปรึกษา และทำงานในโครงการหรือภารกิจช่วยเหลือด้านเทคนิคที่เกี่ยวข้องกับ Fintech
3. ให้คำแนะนำในการพัฒนาบุคลากรด้านความปลอดภัยไซเบอร์และ Fintech ทั้งรูปแบบของการแลกเปลี่ยนพนักงานเพื่อฝึกงาน การเยี่ยมชม การแบ่งปันประสบการณ์ การให้คำปรึกษา การเข้าร่วมอบรมหรือสัมมนา

4.2 ตัวอย่างการปฏิบัติตามกฎเกณฑ์ ธปท. ของสถาบันการเงิน

จากการสัมภาษณ์ผู้บริหารสายงานบริหารความเสี่ยงด้านการปฏิบัติการของธนาคารพาณิชย์ไทยแห่งหนึ่งเกี่ยวกับการปฏิบัติตามนโยบายของ ธปท. ซึ่งสายงานดังกล่าวถือเป็น Second line ใน Three lines of defense ซึ่งเป็นรูปแบบโครงสร้างที่ ธปท. กำหนดให้มีตามที่ผู้วิจัยเคยกล่าวถึงในข้อ 3.1.2 บทบาทจากการกำหนดมาตรการและนโยบายต่าง ๆ



รูปภาพที่ 11 การจัดโครงสร้างตามหลัก Three lines of defense ของธนาคารพาณิชย์แห่งหนึ่ง

สายงานบริหารความเสี่ยงด้านปฏิบัติการของธนาคารพาณิชย์แห่งนี้ มีการกำหนดกรอบแนวทางการตรวจสอบด้านไอที (IT Compliance Framework) ของธนาคารเอง โดยอ้างอิงจากกฎเกณฑ์องค์กรกำกับดูแลต่าง ๆ ที่เกี่ยวข้อง เช่น ธปท. และกำหนดประมวลข้อกำหนดด้านไอที (IT Compliance universe) เป็น 6 ด้าน ได้แก่ ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (IT Governance) การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security) การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management) การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT compliance) การตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit) และการบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (IT project management)

โดยหลักการตรวจสอบการปฏิบัติตามข้อกำหนดด้านไอที (IT compliance audit) ของธนาคาร แบ่งรูปแบบการทำงาน 2 แบบ คือ

1. การป้องกัน (Prevent) การทำงานรูปแบบนี้มีหน้าที่หลัก ๆ ที่ต้องรับผิดชอบ ดังนี้

1.1 ให้คำแนะนำเป็นที่ปรึกษาให้กับหน่วยงานต่าง ๆ (Business Unit) ในเรื่องที่เกี่ยวกับกฎเกณฑ์ต่าง ๆ ของผู้กำกับดูแล โดยหน่วยงานจะมาปรึกษากรณีจัดทำผลิตภัณฑ์ใหม่ ๆ เพื่อพิจารณาว่าไม่เป็นการฝ่าฝืนกฎเกณฑ์ที่เกี่ยวข้อง

1.2 กรณีหน่วยงานกำกับดูแลออกกฎเกณฑ์ใหม่ หรือเปลี่ยนแปลงกฎเกณฑ์ ก็มีหน้าที่สื่อสารกฎเกณฑ์เหล่านี้ให้ผู้ที่เกี่ยวข้องรับทราบ เพื่อให้ปฏิบัติได้ถูกต้อง

1.3 ติดตามกำกับดูแล กรณีหน่วยงานภายนอกตรวจพบประเด็น จึงมีหน้าที่ติดตามความคืบหน้าของการปรับปรุงแก้ไขและจัดทำรายงานเสนอให้ผู้บริหารรับทราบ

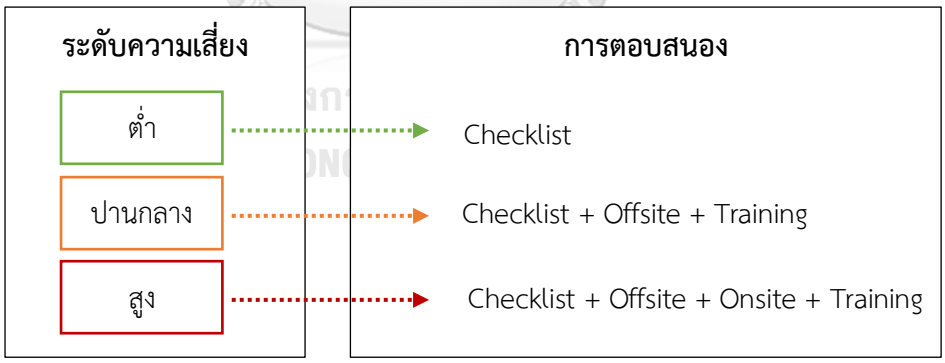
2. การติดตาม (Monitor) จะทำภายหลังมีการระบุและประเมินความเสี่ยงแล้ว เพื่อจะได้ออกแบบรูปแบบการติดตามที่เหมาะสม ได้แก่ รายการตรวจสอบ (Checklist) การตรวจสอบนอกสถานที่ทำการ (Offsite) หรือการตรวจสอบ ณ สถานที่ทำการ (Onsite) โดยธนาคารจะพิจารณาในมุมของความคุ้มค่าเทียบกับผลกระทบที่จะเกิดขึ้น ซึ่งการติดตามนั้นมีวิธีการทำงาน เริ่มจากการระบุและประเมินความเสี่ยงว่าความเสี่ยงนั้นอยู่ในระดับเขียว (ต่ำ) เหลือง (ปานกลาง) หรือแดง (สูง) เน้นพิจารณาที่ผลกระทบเพื่อบ่งบอกระดับ และจะนำไปสู่การตอบสนองที่แตกต่างกัน

2.1 รายการตรวจสอบ (Checklist) ใช้กับความเสี่ยงทุกระดับ เพื่อสอบทานความเข้าใจต่อพิธีปฏิบัติ และกฎเกณฑ์ต่าง ๆ

2.2 การตรวจสอบนอกสถานที่ทำการ (Offsite) ใช้กับความเสี่ยงระดับปานกลางและสูง เป็นการตรวจสอบโดยขอเอกสารจากหน่วยงานมาสอบทาน และเป็นหลักฐานยืนยันเพื่อให้มั่นใจว่าสิ่งที่ปฏิบัติถูกต้อง เป็นไปตามกฎเกณฑ์

2.3 การตรวจสอบ ณ สถานที่ทำการ (Onsite) ใช้กับความเสี่ยงระดับสูง เป็นการลงพื้นที่ ไปสังเกตการณ์สิ่งหน่วยงานปฏิบัติตั้งแต่กระบวนการแรกถึงกระบวนการสุดท้าย (Walk-through) และสัมภาษณ์ผู้ปฏิบัติงาน เพื่อให้มั่นใจสิ่งที่ปฏิบัตินั้นถูกต้องเป็นไปตามกฎเกณฑ์ที่เกี่ยวข้อง

2.4 การอบรมให้ความรู้ (Training)



รูปภาพที่ 12 การตอบสนองต่อความเสี่ยงแต่ละระดับ

ซึ่งผู้บริหารธนาคารพาณิชย์ได้กล่าวว่า ธนาคารมีแนวทางปฏิบัติ (Approach) ในการเข้าไปตรวจสอบ แบ่งได้เป็น 2 แบบ คือ

1. แบบทั่วไป (General) เป็นการสอบทานสิ่งที่ปฏิบัติว่าเป็นไปตามนโยบาย ระเบียบกฎเกณฑ์ที่เกี่ยวข้อง เช่น นโยบาย ธปท. กำหนดว่าอย่างน้อยต้องครอบคลุม 3 ข้อ ก็ต้องตรวจสอบให้มั่นใจว่าครอบคลุมทั้ง 3 ข้อที่ ธปท. กำหนดจริง

2. แบบเทคนิค (Technical) ต้องใช้ความรู้ทางด้านไอที แบ่งย่อยได้ 2 ระดับ ได้แก่
   2.1 ขั้นพื้นฐาน (Fundamental) สอบทานเชิงเทคนิคทั่วไป ใช้ความรู้พื้นฐานไอทีหรือประสบการณ์การสอบทานเชิงเทคนิค เช่น สอบทานการตั้งค่าตัวแปร (Parameter) ของเครือข่าย (Network) หรือสอบทานเอกสารทางเทคนิค
   2.2 ขั้นสูง (Advance) สอบทานโดยใช้ความรู้เชิงลึก โดยอาศัยผู้เชี่ยวชาญหรือความรู้เฉพาะด้าน เช่น การเจาะระบบ

จากบทสัมภาษณ์ของผู้บริหารธนาคารพาณิชย์ดังกล่าวได้ให้ความเห็นต่อบทบาทการกำกับดูแลของ ธปท. ไว้ว่า

“ไม่อยากให้ ธปท. ออกกฎเกณฑ์อะไรที่ตายตัวเกินไป เพราะจะทำให้ไม่เกิดการพัฒนาเพื่อแข่งขันกัน แต่สิ่งสำคัญที่สุดคือ Capacity Building คือเรื่อง resource จะเป็นเรื่องดีมากถ้า industry ช่วยกันผลักดันในเรื่องนี้ร่วมกัน จะได้ไม่มีปัญหาคนย้ายงานบ่อย ๆ แย่งคนกันไปมา ถ้า ธปท. ช่วยผลักดันเรื่องนี้จะดีมาก เพื่อไม่ให้มีการเหลื่อมล้ำกันในเรื่องความได้เปรียบเสียเปรียบ”

4.3 การมีส่วนร่วมด้านกฎหมายระหว่าง ธปท. และหน่วยงานอื่น ๆ

จากการศึกษาผู้วิจัยพบว่า นอกเหนือจากประกาศของ ธปท. ที่กำหนดเกี่ยวกับความปลอดภัยไซเบอร์เพื่อกำกับดูแลสถาบันการเงินแล้ว ยังมีหน่วยงานอื่น ๆ ที่มีหน้าที่กำกับดูแลสถาบันการเงินออกหลักเกณฑ์ แนวปฏิบัติเกี่ยวกับความปลอดภัยไซเบอร์เช่นเดียวกัน

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) ได้ออกแนวปฏิบัติที่เกี่ยวข้องกับความปลอดภัยไซเบอร์สำหรับผู้ประกอบธุรกิจหลักทรัพย์และสัญญาซื้อขายล่วงหน้าต้องปฏิบัติตามซึ่งสถาบันการเงินหลายแห่งมีการออกผลิตภัณฑ์เหล่านี้ จึงมีความเกี่ยวข้องกับงานวิจัยฉบับนี้เนื่องจากสถาบันการเงินเหล่านั้นต้องปฏิบัติตามมาตรการที่ออก ได้แก่

ประกาศ ก.ล.ต. ที่ สธ. 37/2559 เรื่องข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ[3] ซึ่งบังคับใช้ตั้งแต่ 1 ก.ย.60 สำหรับผู้ประกอบธุรกิจหลักทรัพย์และธุรกิจสัญญาซื้อขายล่วงหน้า เพื่อให้ระบบเทคโนโลยีมีประสิทธิภาพและเป็นไปในแนวทางเดียวกัน โดยต้องมีการกำหนดนโยบายการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศในองค์กร นโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ การบริหารจัดการทรัพย์สินสารสนเทศและควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ รวมทั้งการรักษาความมั่นคงปลอดภัยด้านการสื่อสาร

[3] สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, **ประกาศ ก.ล.ต. ที่ สธ. 37/2559 เรื่องข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ** [ออนไลน์], 2559. แหล่งที่มา https://capital.sec.or.th/webapp/nrs/data/7038s.pdf

ข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์และการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ

ต่อเนื่องจากประกาศข้างต้น ก.ล.ต. ได้ออกประกาศย่อยเพื่อขยายความและลงรายละเอียดข้อกำหนดใน ประกาศ สธ. 37/2559 ให้ชัดเจนยิ่งขึ้น เพื่อให้ทราบว่าข้อกำหนดแต่ละข้อผู้ประกอบการควรดำเนินการอย่างไรบ้าง จึงออกประกาศแนวปฏิบัติ ที่ นป. 3/2559 เรื่องแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ[4] ในวันที่ 12 ก.ย. 60 สำหรับผู้ประกอบธุรกิจหลักทรัพย์และธุรกิจสัญญาซื้อขายล่วงหน้าใช้เป็นแนวทางปฏิบัติในเรื่องการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี และการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) ได้ออกแนวปฏิบัติที่เกี่ยวข้องกับความปลอดภัยไซเบอร์สำหรับบริษัทประกันภัย ซึ่งสถาบันการเงินหลายแห่งมีการออกผลิตภัณฑ์ที่เป็นประกันภัยและประกันชีวิตด้วยเช่นกัน จึงต้องปฏิบัติตามมาตรการกำกับดูแลของ คปภ. ด้วย ได้แก่

ประกาศ คปภ. เรื่องหลักเกณฑ์ วิธีการออกกรมธรรม์ประกันภัย การเสนอขายกรมธรรม์ประกันภัยและการชดใช้เงิน หรือค่าสินไหมทดแทนตามสัญญาประกันภัย โดยใช้วิธีการทางอิเล็กทรอนิกส์ พ.ศ. 2560[5] ประกาศในราชกิจจานุเบกษาเมื่อ 27 ก.พ. 60 ซึ่งมีการกำหนดมาตรการเกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศอยู่ในหมวด 6 ของประกาศ ที่กำหนดให้บริษัทประกันภัยที่เสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ต้องมีแนวนโยบายและแนวปฏิบัติด้านการบริหารจัดการความเป็นส่วนตัวและข้อมูลส่วนบุคคล รวมทั้งต้องมีการตรวจรับรองระบบสารสนเทศโดยผู้ตรวจสอบอิสระ ทั้งยังอ้างอิงไปยัง พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ว่าต้องปฏิบัติตาม พรบ. ดังกล่าวด้วยเช่นกัน

---

[4] สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, **ประกาศ ก.ล.ต. ที่ นป. 3/2559 เรื่อง แนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ** [ออนไลน์], 2559. แหล่งที่มา http://capital.sec.or.th/webapp/nrs/data/7041s.pdf

[5] ราชกิจจานุเบกษา, **ประกาศ คปภ. เรื่องหลักเกณฑ์ วิธีการออกกรมธรรม์ประกันภัย การเสนอขายกรมธรรม์ประกันภัยและการชดใช้เงิน หรือค่าสินไหมทดแทนตามสัญญาประกันภัย โดยใช้วิธีการทางอิเล็กทรอนิกส์ พ.ศ. 2560** [ออนไลน์], 27 กุมภาพันธ์ 2560. แหล่งที่มา http://oiceservice.oic.or.th/document/Law/file/05090/05090_914ba349ca43c3969d51649e52e82c52.pdf

ประกาศ คปภ. เรื่องหลักเกณฑ์ วิธีการออกกรมธรรม์ประกันภัย การเสนอขายกรมธรรม์ประกันภัยและการชดใช้เงินตามสัญญาประกันชีวิต โดยใช้วิธีการทางอิเล็กทรอนิกส์ พ.ศ. 2560[6] ได้กำหนดมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศอยู่ในหมวด 6 ของประกาศ เช่นเดียวกับประกาศสำหรับผู้ประกอบธุรกิจประกันชีวิตข้างต้นและประกาศ ณ วันเดียวกัน ซึ่งมีเนื้อหาที่เหมือนกันแตกต่างกันแค่บังคับใช้กับผู้ประกอบธุรกิจคนละกลุ่มเท่านั้น

ต่อมา คปภ. ได้เผยแพร่แนวทางปฏิบัติสำหรับรักษาความปลอดภัยและควบคุมความเสี่ยงของระบบเทคโนโลยีสารสนเทศ (Information Technology Risk Management) และความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cybersecurity)[7] เมื่อ ธ.ค.60 เพื่อให้บริษัทประกันภัยมีแนวทางสำหรับประยุกต์ใช้ในการกำกับดูแลและบริหารจัดการของธุรกิจแต่ละแห่งที่มีความซับซ้อนแตกต่างกันได้อย่างเหมาะสม ทั้งในด้านการควบคุมความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cyber Risk) ของตนเองให้สามารถระบุความเสี่ยง (identify) ป้องกัน (protect) ตรวจพบ (detect) รับมือ (respond) กู้ระบบคืนสู่สภาวะปกติ (recover) สามารถดำเนินธุรกิจได้อย่างต่อเนื่อง และเพื่อพัฒนาโครงสร้างพื้นฐานระบบ IT เตรียมความพร้อมเพื่อการขยายธุรกิจเข้าสู่เศรษฐกิจยุคดิจิตอล ซึ่งผู้วิจัยเห็นว่าค่อนข้างมีความคล้ายคลึงกับแนวปฏิบัติที่ ธปท. ประกาศ ไม่ว่าจะเป็นเรื่อง แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลัก (IT Best Practices Phase 1 and 2) หรือ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Implementation Guideline) ต่างกันเพียงธุรกิจที่กำกับดูแล ซึ่ง ธปท. กำกับดูแลสถาบันการเงิน แต่ คปภ. กำกับดูแลธุรกิจประกันภัย

นอกเหนือจากประกาศ แนวปฏิบัติที่ผู้มีหน้าที่กำกับดูแลได้ออกมาบังคับใช้กับเหล่าสถาบันการเงินแล้ว จากการสัมภาษณ์ผู้เชี่ยวชาญด้านกฎหมายเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับสถาบันการเงิน พบว่า ยังมีพระราชบัญญัติอื่นที่อาจเข้ามาเกี่ยวข้องด้วย ได้แก่

---

[6] ราชกิจจานุเบกษา, **ประกาศ คปภ. เรื่องหลักเกณฑ์ วิธีการออกกรมธรรม์ประกันภัย การเสนอขายกรมธรรม์ประกันภัยและการชดใช้เงินตามสัญญาประกันชีวิต โดยใช้วิธีการทางอิเล็กทรอนิกส์ พ.ศ. 2560** [ออนไลน์], 27 กุมภาพันธ์ 2560. แหล่งที่มา http://oiceservice.oic.or.th/document/Law/file/05079/05079_a4896511fce69a40b015c81dd7eb02b7.pdf

[7] สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย, **แนวทางปฏิบัติสำหรับรักษาความปลอดภัยและควบคุมความเสี่ยงของระบบเทคโนโลยีสารสนเทศ (Information Technology Risk Management) และความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cybersecurity)** [ออนไลน์], 2560. แหล่งที่มา https://www.oic.or.th/sites/default/files/content/368/information-technology-risk-management-guideline-28-thanwaakhm-2560.pdf

พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562[8] ประกาศเมื่อ 27 พ.ค. 62 สิ่งที่ผู้วิจัยเห็นว่ามีความเกี่ยวข้องกับงานวิจัยฉบับนี้ พรบ. มาตรา 44 มีการระบุให้หน่วยงานควบคุมหรือกำกับดูแลต้องจัดทำแนวทางปฏิบัติและมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศโดยเร็ว ซึ่งอย่างน้อยต้องประกอบด้วยเนื้อหาเกี่ยวกับแผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละ 1 ครั้ง และมีแผนการรับมือคุมคามไซเบอร์ ทั้งนี้จากการศึกษาของผู้วิจัยเห็นว่าประกาศที่ ธปท. ออกใช้เพื่อกำกับดูแลสถาบันการเงินได้ระบุประเด็น 2 ข้อข้างต้นอย่างครบถ้วนแล้ว ซึ่ง พรบ. ฉบับนี้ให้ความสำคัญกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยหน่วยงานด้านการเงินการธนาคารถือเป็นหนึ่งในหน่วยงานโครงสร้างพื้นฐานสำคัญ ซึ่งตามมาตรา 53 ระบุให้หน่วยงานควบคุมหรือกำกับดูแลตรวจสอบมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานที่สำคัญ หากไม่ได้มาตรฐานให้แจ้งหน่วยงานดังกล่าวให้แก้ไขโดยเร็ว ผู้วิจัยเห็นว่า ธปท. ได้มีการกำหนดหน่วยงานที่ทำหน้าที่ตรวจสอบเรื่องนี้อย่างครบถ้วนดังที่เคยกล่าวไป ธปท. มีฝ่ายตรวจสอบเทคโนโลยีสารสนเทศ (ฝตท.) คอยทำหน้าที่ตรวจสอบสถาบันการเงินต่าง ๆ หรือไม่ว่าจะเป็นมาตรา 56 ที่กำหนดให้หน่วยงานโครงสร้างพื้นฐานสำคัญต้องมีกลไกหรือขั้นตอนเพื่อรับมือภัยคุกคามไซเบอร์ มาตรา 57 เมื่อมีเหตุภัยคุกคามไซเบอร์ให้รายงานต่อหน่วยงานควบคุมหรือกำกับดูแล ทั้งหมดนี้จากการศึกษาของผู้วิจัยเห็นว่า ธปท. ได้กำหนดอยู่ในประกาศค่อนข้างครบถ้วนสมบูรณ์

พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550[9] รวมทั้งฉบับประกาศเพิ่มเติม ล่าสุดประกาศเพิ่มเติมฉบับที่ 2[10] ประกาศเมื่อ 24 ม.ค. 2560 พรบ. กล่าวถึงบทลงโทษเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ อาทิ การเข้าถึงข้อมูลโดยมิชอบ การดักรับข้อมูลของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ การแก้ไข ทำลาย ดัดแปลงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบมี การขัดขวาง ชะลอ รบกวนการทำงานของระบบคอมพิวเตอร์โดยมิชอบ การส่งข้อมูลคอมพิวเตอร์แก่ผู้อื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาทำให้รบกวนการใช้คอมพิวเตอร์ของผู้อื่น การส่งข้อมูลคอมพิวเตอร์แก่ผู้อื่นอันเป็นการสร้างความเดือดร้อน รำคาญโดยผู้รับไม่สามารถปฏิเสธ ทั้งนี้ความผิดมีทั้งจำคุก ปรับเงิน หรือทั้งจำและปรับ ความรุนแรงของโทษขึ้นอยู่กับเจตนาและผลกระทบที่เกิดขึ้น การจำคุกมีตั้งแต่หลักเดือนจนถึงหลายปี เช่นเดียวกับการปรับเงินเริ่มตั้งแต่หลักหมื่นบาทจนถึงหลักแสนบาท ผู้วิจัยเห็นว่า พรบ. นี้อาจจะช่วยลดการเกิดภัยคุกคามไซเบอร์ที่เกิดจากบุคคลในประเทศไทยได้บ้างเนื่องจากมีการระบุบทลงโทษค่อนข้างชัดเจน แต่อย่างไรก็ตามมีกลุ่ม

[8] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562.

[9] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550.

[10] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560.

คนก่อเหตุบางกลุ่มที่ไม่ใช่ประชากรไทยหรือผู้ที่อาศัยอยู่ในประเทศไทยก็อาจยากที่ลงโทษหาคนเหล่านั้นหรือเรียกมารับบทลงโทษได้ ซึ่ง พรบ. นี้อาจไม่ได้ช่วยลดภัยไซเบอร์ที่เกิดจากกลุ่มคนดังกล่าว

พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544[11] รวมทั้งฉบับประกาศเพิ่มเติม โดยล่าสุดประกาศเพิ่มเติมฉบับที่ 4 ประกาศเมื่อ 22 พ.ค. 2562 พรบ. กล่าวถึงข้อควรปฏิบัติและข้อระมัดระวังในการใช้ ส่งต่อและเข้าถึงข้อมูลอิเล็กทรอนิกส์ ความน่าเชื่อถือของข้อมูล การระบุตัวตน การเก็บรักษาข้อมูลและการถือเป็นหลักฐานทางกฎหมาย เพื่อสร้างความน่าเชื่อถือให้กับธุรกรรมทางอิเล็กทรอนิกส์ให้น่าเชื่อถือและมีผลทางกฎหมายเช่นเดียวกับการทำธุรกรรมโดยวิธีการทั่วไป ซึ่งสถาบันการเงินแทบทุกแห่งมีการทำธุรกรรมทางอิเล็กทรอนิกส์ทั้งสิ้นและมีแนวโน้มจะเพิ่มขึ้นเรื่อย ๆ ในอนาคตจึงต้องมีการปฏิบัติตาม พรบ. ฉบับนี้ ซึ่ง พรบ. อาจไม่ได้กล่าวถึงภัยคุกคามไซเบอร์โดยตรง แต่สิ่งที่ พรบ. กำหนดเป็นข้อควรปฏิบัติขั้นพื้นฐานที่ควรกระทำเพื่อป้องกันการเกิดภัยคุกคามไซเบอร์ เช่น การปลอมแปลงข้อมูล การปลอมแปลงตัวตนทางอิเล็กทรอนิกส์ที่อาจทำได้โดยง่ายหากผู้ให้บริการไม่พึงระวัง

บทที่ 5
สรุปผลศึกษา อภิปรายผลการศึกษา และข้อเสนอแนะ

ผลจากการศึกษา ทำให้ผู้วิจัยมองเห็นว่าประเด็นปัญหาอาชญากรรมไซเบอร์ ไม่ได้เป็นสิ่งที่อยู่ไกลตัวอีกต่อไป แต่เป็นปัญหาอาชญากรรมที่เข้ามาอยู่ในกระแสหลักของสังคม ซึ่งเห็นได้จากการที่ทุกภาคส่วนในสังคม เริ่มมีการกล่าวถึงปัญหาอาชญากรรมไซเบอร์และเริ่มมีการรวมกลุ่มในองค์กรที่มีความเสี่ยงต่อการโจมตีระดับที่สูง หรือ องค์กรที่มีสภาพแวดล้อมเดียวกัน

[11] พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544.

โดยการศึกษาเรื่อง “มาตรการความมั่นคงปลอดภัยทางไซเบอร์ต่อสถาบันการเงิน” ในครั้งนี้ ผู้วิจัยได้ตั้งวัตถุประสงค์ในการศึกษาไว้สามประการ คือ ประการแรก เพื่อศึกษาบทบาทธนาคารกลางของไทยในการกำกับดูแลสถาบันการเงินต่อการบังคับใช้มาตรการความมั่นคงปลอดภัยทางไซเบอร์ ประการที่สอง เพื่อศึกษาวิเคราะห์แนวทางการสร้างความร่วมมือระหว่างกลุ่มสถาบันการเงินในการกำหนดมาตรการป้องกันอาชญากรรมไซเบอร์ และประการที่สาม เพื่อเสนอแนะแนวทางการกำหนดมาตรการป้องกันอาชญากรรมไซเบอร์ที่เหมาะสม

รูปแบบวิธีวิจัยที่ใช้จะเป็นการศึกษาวิจัยเชิงคุณภาพ (Qualitative Research) โดยใช้การวิจัยเอกสาร (Documentary Research) ศึกษาค้นคว้าข้อมูลที่อยู่ในรูปแบบข้อมูลทุติยภูมิ (Secondary Data) ร่วมกับการสัมภาษณ์เชิงลึก (In-depth Interview) จากกลุ่มผู้ให้ข้อมูลสำคัญ (Key Informants) โดยเริ่มจากการใช้เทคนิคการสุ่มกลุ่มตัวอย่างแบบเจาะจง (Purposive Sampling) จากผู้ปฏิบัติงานในด้านกำกับดูแลตรวจสอบเทคโนโลยีสารสนเทศของธนาคารแห่งประเทศไทย จำนวน 2 ท่าน และใช้เทคนิคการสุ่มกลุ่มตัวอย่างแบบสโนว์บอล (Snowball Sampling) จำนวน 10 ท่าน ไปจนถึงจุดอิ่มตัวของข้อมูล ผู้วิจัยจึงนำข้อมูลทั้งหมดมาวิเคราะห์ด้วยวิธีการวิเคราะห์เชิงเนื้อหา (Content Analysis) ซึ่งสามารถสรุปออกมาเป็นผลการศึกษาและข้อเสนอแนะ ได้ดังนี้

5.1 สรุปผลการศึกษา

ในส่วนของการสรุปผลการศึกษา ผู้วิจัยจะแบ่งออกเป็น 2 ส่วน คือ บทบาทธนาคารกลางของไทยในการกำกับดูแลสถาบันการเงินต่อการบังคับใช้มาตรการความมั่นคงปลอดภัยทางไซเบอร์ และแนวทางการสร้างความร่วมมือระหว่างกลุ่มสถาบันการเงินในการกำหนดมาตรการป้องกันอาชญากรรมไซเบอร์

5.1.1 บทบาทธนาคารกลางของไทยในการกำกับดูแลสถาบันการเงินต่อการบังคับใช้มาตรการความมั่นคงปลอดภัยทางไซเบอร์

จากผลการศึกษา พบว่า ธนาคารกลางของไทย หรือ ธปท. มีบทบาทที่เกี่ยวข้องกับมาตรการความมั่นคงปลอดภัยไซเบอร์ ที่สามารถแบ่งออกเป็น 4 มิติ ได้แก่

5.1.1.1 การวางกรอบและแนวทางในรับมือกับภัยคุกคามทางไซเบอร์

โดย ธปท. ได้กำหนดมาตรการความมั่นคงปลอดภัยไซเบอร์เป็นหนึ่งในหัวข้อสำคัญในแผนยุทธศาสตร์ขององค์กร เพื่อเป็นการกำหนดทิศทางในการดำเนินงานภายในองค์กร ซึ่งส่งผลต่อภารกิจและการผลักดันโครงการต่าง ๆ ที่จะส่งผลต่อองค์กรภายนอกที่ได้กำกับดูแล อาทิ ผลักดันให้สถาบันการเงินปฏิบัติตามกรอบแนวปฏิบัติด้านระบบเทคโนโลยีสารสนเทศและมาตรการความมั่นคงทางไซเบอร์ที่เป็นไปตามมาตรฐานสากล ผลักดันให้ได้รับใบรับรองเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Certify) ในระดับสากลจากองค์กรที่เชื่อถือได้ ออกแนวปฏิบัติ Cyber Security

5.1.1.2 การกำหนดมาตรการและนโยบายต่าง ๆ

ธปท. ได้มีการมอบนโยบายให้สถาบันการเงินทุกแห่งต้องปฏิบัติตาม เพื่อให้มีการเตรียมความพร้อมรับมือภัยคุกคามไซเบอร์ อาทิ การสร้างกรอบการประเมินความพร้อมในการรับมือภัยคุกคามไซเบอร์ (Cyber Resilience Assessment Framework) ให้สถาบันการเงินประเมินตนเอง เพื่อให้ทราบความเสี่ยงและบริหารจัดการความเสี่ยงได้อย่างเหมาะสม ประกาศหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน โดยกำหนดให้ต้องมีผู้บริหารระดับสูงที่รับผิดชอบเรื่องบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ และต้องมีการรายงานโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญประจำปีให้ ธปท. ทราบ ประกาศนโนบายและมาตรการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ ได้กำหนดกรอบการออกนโยบายของสถาบันการเงินและแนวปฏิบัติเพื่อให้ใช้เป็นทางเลือก เช่น อย่างน้อยในนโยบายต้องมีการพูดถึงการควบคุมการเข้าถึงและการพิสูจน์ตัวตนผู้ใช้ เป็นต้น

5.1.1.3 การกำกับและตรวจสอบ

ฝ่ายกำกับและตรวจสอบความเสี่ยงเทคโนโลยีสารสนเทศ (ฝตท.) ธนาคารแห่งประเทศไทย เป็นฝ่ายงานที่มีหน้าที่รับผิดชอบกำกับและตรวจสอบเกี่ยวกับภัยคุกคามไซเบอร์ของสถาบันการเงิน ได้แก่ การกำหนดนโยบาย หลักเกณฑ์ และแนวปฏิบัติ รวมทั้งตรวจสอบและวิเคราะห์ติดตามการดำเนินงาน ซึ่งการตรวจสอบของแบ่งออกเป็น 3 รูปแบบ

1) การตรวจสอบเจาะจงเฉพาะเรื่อง (Thematic)

2) การออกเยี่ยมเยียน (Site Visit)

3) การตรวจติดตามต่อเนื่อง (Offsite Monitoring)

5.1.1.4 การให้ความรู้แก่ภาคประชาชน

ซึ่ง ธปท. ได้ให้ความรู้กับกลุ่มคนที่หลากหลาย และจัดเนื้อหาที่แตกต่างกันเพื่อให้เหมาะสมกับแต่ละกลุ่มเป้าหมาย อาทิ กลุ่มคนจากธนาคารกลางต่างประเทศ สถาบันการเงินและหน่วยงานกำกับดูแล กลุ่มประชาชนทั่วไป ไม่ว่าจะเป็นการมอบหมายคนที่มีความเชี่ยวชาญไปเป็นวิทยากรให้กับองค์กรภายนอกต่าง ๆ การเชิญบุคคลภายนอกเข้ามาร่วมประชุมสัมมนาที่จัดขึ้นภายใน ธปท. การให้ข้อมูลผ่านทางเว็บไซต์หรือเฟสบุ๊ค และการจัดกิจกรรมหรือนิทรรศการที่ศูนย์การเรียนรู้ ธปท.

5.1.2 แนวทางการสร้างความร่วมมือระหว่างกลุ่มสถาบันการเงินในการกำหนดมาตรการป้องกันอาชญากรรมไซเบอร์

จากผลการศึกษา เห็นได้ว่า ธปท. ได้มีการสร้างความร่วมมือกับองค์กรมากมาย ไม่ว่าจะเป็นภายในประเทศ หรือต่างประเทศ ทั้งกับกลุ่มสถาบันการเงินและในกลุ่มภาคธุรกิจอื่น ๆ โดยสามารถแบ่งความร่วมมือต่าง ๆ ออกเป็นหัวข้อย่อย ได้ดังนี้

5.1.2.1 ความร่วมมือกับสถาบันการเงิน

ธปท. ได้ผลักดันให้เกิดศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร หรือ Thailand Banking Sector CERT (TB-CERT) ซึ่งทำหน้าที่เป็นหน่วยงานกลางที่คอยดูแลรับมือภัยไซเบอร์ และแบ่งปันข่าวสารที่เป็นประโยชน์ โดยให้สถาบันการเงินต่าง ๆ เข้าร่วมเป็นสมาชิก

5.1.2.2 ความร่วมมือกับหน่วยงานอื่น ๆ ภายในประเทศ

ธปท. ได้ลงนามในบันทึกข้อตกลงความร่วมมือกับองค์กรภาคธุรกิจการเงิน การลงทุน และประกันภัย ซึ่งประกอบด้วยองค์กรของรัฐ และองค์กรที่มีหน้าที่ในการกำกับดูแล เพื่อร่วมสร้างกลไกความร่วมมือในการแบ่งปันข้อมูลข่าวสาร และร่วมกันแก้ไขปัญหาภัยคุกคามไซเบอร์

นอกเหนือจากที่ ธปท. ได้ลงนามความร่วมมือกับภาคการเงินแล้ว ธปท. ยังลงนามในบันทึกข้อตกลงความร่วมมือกับองค์กรภาคธุรกิจอื่นด้วย ได้แก่ ภาคธุรกิจการค้า อุตสาหกรรม และโครงสร้างพื้นฐานสำคัญของประเทศ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เพื่อร่วมกันสร้างกลไกแก้ไขปัญหาภัยคุกคามไซเบอร์ และแบ่งปันข้อมูล รวมทั้งตกลงร่วมมือกันอย่างไม่เป็นทางการกับเจ้าของเทคโนโลยีต่าง ๆ

5.1.2.3 ความร่วมมือกับหน่วยงานต่างประเทศ

ธปท. มีการสร้างความร่วมมือทั้งแบบเป็นทางการ และไม่เป็นทางการกับธนาคารกลางหรือหน่วยงานที่รับผิดชอบดูแลด้าน Cyber Security ของต่างประเทศ ได้แก่ ฮ่องกง อิสราเอล สิงคโปร์ สวิตเซอร์แลนด์ รัสเซีย

นอกเหนือจากการที่ ธปท. ตกลงความร่วมมือกับองค์กรต่าง ๆ แล้ว แต่ละองค์กรที่มีหน้าที่กำกับดูแลก็ได้ออกประกาศ กฎเกณฑ์ หรือแนวปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ของตนเพื่อกำกับดูแลธุรกิจที่เกี่ยวข้องเช่นเดียวกัน ไม่ว่าจะเป็นสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) หรือสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) ซึ่งกลุ่มสถาบันการเงินบางแห่งก็มีความเกี่ยวข้องที่จะต้องปฏิบัติตามมาตรการที่องค์กรเหล่านี้กำหนดขึ้นเช่นเดียวกับการปฏิบัติตามมาตรการของ ธปท.

5.2 อภิปรายผลการศึกษาบทบาทธนาคารกลางของไทยในการกำกับดูแลสถาบันการเงินต่อการบังคับใช้มาตรการความมั่นคงปลอดภัยทางไซเบอร์

จากการศึกษาบทบาทธนาคารกลางของไทยในการกำกับดูแลสถาบันการเงินต่อการบังคับใช้มาตรการความมั่นคงปลอดภัยทางไซเบอร์ มีการนำทฤษฎีทางสังคมวิทยา แนวคิด และงานวิจัยที่เกี่ยวข้องมาใช้อธิบายบทบาทของธนาคารแห่งประเทศไทยในแต่ละมิติ ได้ดังนี้

มิติที่ 1 การวางกรอบและแนวทางในรับมือกับภัยคุกคามทางไซเบอร์

จากผลการศึกษา พบว่า ธปท. เห็นความสำคัญอย่างมากในเรื่องความมั่นคงปลอดภัยไซเบอร์ และได้กำหนดอยู่ในแผนยุทธศาสตร์ขององค์กร ตลอดระยะเวลา 6 ปี ตั้งแต่ปี 2560 – 2565 เพื่อเป็นแนวทางในการดำเนินงานในอนาคต วางแผนโครงการ กำหนดภารกิจ สื่อสารเป้าหมายเพื่อขับเคลื่อนองค์กรไปในทิศทางดังกล่าว ซึ่งสอดคล้องกับแนวคิดของ Chandler[1] ที่ได้ระบุไว้ในหนังสือเรื่อง Strategy and Structures ว่ายุทธศาสตร์เป็นตัวขับเคลื่อนองค์กร เป็นการตัดสินใจในเป้าหมายและวัตถุประสงค์ระยะยาว การวางแผนยุทธศาสตร์นอกเหนือจากกำหนดวัตถุประสงค์หลักแล้ว ธปท. ยังได้กำหนดกลยุทธ์ย่อย ๆ เพื่อให้การดำเนินการสำเร็จได้ตามวัตถุประสงค์หลัก และยังแตกย่อยลงมาถึงโครงการที่จะจัดทำในระหว่างรอบระยะเวลายุทธศาสตร์ฉบับนั้น ๆ มีการกำหนดและยกตัวอย่างไว้ในรายละเอียดของยุทธศาสตร์อย่างชัดเจน รวมทั้งมีการติดตามผลการดำเนินโครงการทุกปี เพื่อทราบความคืบหน้า อุปสรรคที่เกิดที่อาจทำให้แผนการตามยุทธศาสตร์ไม่บรรลุวัตถุประสงค์ หรือความล่าช้าของโครงการที่ต้องเร่งปรับปรุง

มิติที่ 2 การกำหนดมาตรการและนโยบายต่าง ๆ

เนื่องจาก ธปท. มองเห็นปัญหาที่อาจเกิดขึ้นในอนาคตเกี่ยวความมั่นคงปลอดภัยไซเบอร์เนื่องจากเทคโนโลยีเข้ามามีบทบาทในยุคปัจจุบันมาขึ้นเรื่อย ๆ ธปท. จึงได้ออกประกาศ กรอบ และแนวปฏิบัติให้สถาบันการเงินภายใต้การกำกับดูแลต้องปฏิบัติตามมากมาย ซึ่งการออกประกาศแต่ละครั้ง ธปท. มีการจัดทำร่างเพื่อให้สถาบันการเงินที่ต้องปฏิบัติตามสามารถเสนอความคิดเห็นในประกาศดังกล่าวก่อนประกาศใช้จริง ซึ่งสอดคล้องกับหลักการวิเคราะห์ผลกระทบในการออกกฎหมาย (Regulatory impact assessment: RIA) ที่องค์การเพื่อความร่วมมือและการพัฒนาทางเศรษฐกิจ (Organization for Economic Co-operation and Development: OECD) [2] ได้ระบุไว้ว่าประกอบด้วยขึ้นตอนที่สำคัญ 6 ขั้นตอน สรุปได้ดังนี้

1. การระบุปัญหา ซึ่งปัญหาของ ธปท. ในด้านไซเบอร์คือ ระบบและเครือข่ายของสถาบันการเงินที่สำคัญมีช่องโหว่หรือจุดอ่อนให้อาชญากรไซเบอร์สามารถก่ออาชญากรรมได้ รวมทั้งไม่สามารถป้องกัน ตรวจจับ และรับมือได้อย่างมีประสิทธิภาพ
2. กำหนดทางเลือกต่าง ๆ ในการแก้ปัญหา ธปท. มีหลากหลายทางเลือกในการแก้ปัญหาทั้งเช่น การออกมาตรการ การให้ความรู้ การตรวจสอบระบบและเครือข่ายสถาบันการเงิน
3. เก็บรวบรวมข้อมูล เป็นการหาข้อมูลจากผู้ที่เกี่ยวข้องหรือได้รับผลกระทบจากทางเลือกต่าง ๆ ที่ ธปท. จะเลือกใช้ เช่น ความเห็นของสถาบันการเงิน

---

[1] Alfred D. Chandler, Jr., **Strategy and Structure: Chapters in the History of the Industrial Enterprise** (Cambridge: The MIT Press, 1962). p. 13.

[2] OECD, **Introductory Handbook for Undertaking Regulatory Impact Analysis (RIA)** [Online], 2008. Source https://www.oecd.org/gov/regulatory-policy/44789472.pdf

4. การวิเคราะห์ทางเลือกต่าง ๆ เปรียบเทียบระหว่างต้นทุน ผลประโยชน์ของแต่ละทางเลือก พิจารณาถึงต้นทุนที่สถาบันการเงินอาจต้องแบกรับเพิ่มเติม

5. การเลือกทางเลือกที่ดีที่สุด

6. สื่อสารผลลัพธ์ที่ได้จากการทำ RIA เมื่อ ธปท. เลือกทางเลือกว่าจะออกนโยบายใหม่ ธปท. จะมีการสื่อสารร่างนโยบายให้สถาบันการเงินที่เกี่ยวข้องทราบ และให้เวลาในการเสนอความเห็นต่อร่างนโยบายนั้นเพื่อแก้ไขปรับปรุงให้เหมาะสมยิ่งขึ้น ก่อนประกาศใช้จริง

ซึ่งการที่ ธปท. ทำตามหลักการข้างต้น ทำให้มาตรการและนโยบายต่าง ๆ ได้รับการตอบสนองอย่างมีประสิทธิภาพ สถาบันการเงินมีความเต็มใจในการปฏิบัติตาม

มิติที่ 3 การกำกับและตรวจสอบ

จากการศึกษา พบว่า ธปท. มีหน่วยงานที่คอยกำกับและตรวจสอบความเสี่ยงเทคโนโลยีสารสนเทศของสถาบันการเงินต่าง ๆ โดยการตรวจสอบแต่ละส่วนทั้งการตรวจสอบเจาะจงเฉพาะเรื่อง ที่มุ่งเน้นเรื่องที่มีความเสี่ยงสูง การออกเยี่ยมเยียนเพื่อติดตามความคืบหน้าข้อแนะนำในอดีตที่เสนอให้สถาบันการเงินได้ปรับปรุงแก้ไข และการตรวจติดตามต่อเนื่อง ซึ่งทุกรูปแบบที่ ธปท. ดำเนินการล้วนต้องการค้นหารอยรั่ว ช่องโหว่ จุดบกพร่องของการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ของสถาบันการเงิน เพื่อลดโอกาส ลดความเสี่ยงที่จะเกิดภัยคุกคามต่อระบบ สอดคล้องกับทฤษฎีควบคุมอาชญากรรมจากสภาพแวดล้อม (Theory of Crime Control Through Environmental Design)[3] ใช้หลักการพื้นฐานว่าด้วยการออกแบบสภาพแวดล้อมให้มีความเหมาะสมและมีประสิทธิภาพให้สามารถลดปัญหาการเกิดอาชญากรรม ทั้งที่เป็นรูปธรรม เช่น การออกแบบโครงสร้างของระบบเครือข่ายให้มีความรัดกุม มีสัญญาณเตือนภัยเมื่อมีภัยคุกคาม ซึ่งสิ่งเหล่านี้มีระบุในนโยบายที่ ธปท. ประกาศให้สภาบันการเงินปฏิบัติตาม และนามธรรม เช่น การเตือนภัยเพื่อนบ้าน ธปท. มีการระบุให้แจ้งทันทีเมื่อประสบเหตุภัยคุกคาม เพื่อที่จะได้แจ้งเตือนสถาบันการเงินอื่นให้ระมัดระวังเหตุได้ทันการณ์ เพื่อลดโอกาสการเกิดอาชญากรรม โดยการกำกับและตรวจสอบก็เป็นการดูว่าสถาบันการเงินทำตามข้อกำหนดด้วยหรือไม่ หากพกเจอรอยรั่ว หรือสิ่งผิดปกติเล็ก ๆ ที่เป็นจุดควบคุมที่สำคัญ หากจัดการไม่ดีอาจก่อให้เกิดความเสี่ยงที่มีนัยสำคัญได้ ธปท. จะแจ้งให้สถาบันการเงินเร่งแก้ไขปรับปรุงโดยทันที เพื่อไม่ให้รอยรั่วเล็ก ๆ กลายเป็นประตูให้อาชญากรเข้าสู่เครือข่ายที่มีความสำคัญของเหล่าสถาบันการเงินได้ สอดคล้องกับทฤษฎีหน้าต่างแตก (Broken Windows Theory) ที่ James Q. Wilson & George L. Kelling[4] กล่าวไว้ว่าสาเหตุของการเกิดอาชญากรรมนั้นมีปัจจัยส่วนหนึ่งมาจากการขาดระเบียบวินัยของสภาพเมือง ปล่อยกระจกหน้าต่างที่

---

[3] ปุระชัย เปี่ยมสมบูรณ์. **การควบคุมอาชญากรรมจากสภาพแวดล้อม: หลักทฤษฎีและมาตรการ.** (กรุงเทพฯ: สถาบันบัณฑิตพัฒนบริหารศาสตร์, 2525)

[4] Design Something, **The Broken Windows Theory ลดปัญหาอาชญากรรมในเมืองด้วย "ทฤษฎีกระจกแตก"** (ออนไลน์), 2016. แหล่งที่มา https://dsignsomething.com/2016/03/02/the-broken-windows-

แตกไว้ไม่ยอมซ่อมแซม จนกลายเป็นเป็นจุดชนวนให้เกิดรอยแตกอื่น ๆ ตามมา ซึ่งแสดงถึงการไม่มีใครใส่ใจ ทำให้ระดับการกระทำที่เลวร้ายค่อย ๆ เติบโตจนกลายเป็นอาชญากรรมที่รุนแรงในที่สุด

มิติที่ 4 การให้ความรู้แก่ภาคประชาชน

จากผลการศึกษา พบว่า ธปท. มีการให้ความรู้ด้านไซเบอร์แก่ประชาชนในหลากหลายกลุ่ม ทั้งกลุ่มคนจากธนาคารกลางต่างประเทศ สถาบันการเงินและหน่วยงานกำกับดูแล โดย ธปท. มีการจัดรูปแบบการถ่ายทอดความรู้ในรูปแบบที่แตกต่างกันให้เหมาะสมกับพื้นฐานความรู้และประสบการณ์ที่ผ่านมาของแต่ละบุคคล โดยรูปแบบการสื่อสารความรู้ด้านไซเบอร์ของ ธปท. มีทั้งการมอบความรู้ให้โดยตรงผ่านเป็นวิทยากรงานสัมมนาต่าง ๆ การทำโปรชัวร์ความรู้ผ่านช่องทางดิจิทัล จัดนิทรรศการให้เข้าร่วม การแลกเปลี่ยนมุมมอง ข้อมูลความรู้ระหว่างกันระหว่างกลุ่มสถาบันการเงิน หรือการจัดการกิจกรรมให้เรียนรู้ผ่านประสบการณ์จริง (Boot Camp) ซึ่งแต่ละกิจกรรมจะมีการจัดกลุ่มคัดเลือกบุคคลที่เหมาะสมให้เข้าร่วม และกิจกรรมที่จัดมีการจัดต่อเนื่องทุกปี

ซึ่งความรู้ที่ ธปท. ได้นำมาถ่ายทอดนั้น จะเป็นลักษณะการแบ่งปันประสบการณ์และทักษะร่วมกับผู้ที่ทำงานในสายงานเดียวกัน หรือ ที่ใช้ทักษะความรู้คล้ายคลึงกัน โดยถ่ายทอดผ่านการให้เรียนรู้จากการได้ปฏิบัติงานจริง รวมถึงการนำความรู้เชิงทฤษฎี แนวปฏิบัติ และมาตรฐานสากลมาถ่ายทอดอธิบายให้เห็นภาพ สังเคราะห์ให้ผู้รับสารสามารถเข้าใจได้ง่ายขึ้น ซึ่งสอดคล้องกับแนวคิดการจัดการความรู้ (Knowledge Management) ที่ Ikujiro Nonaka[5] กล่าวไว้ว่า ความรู้แบ่งได้เป็น 2 ประเภท คือ 1. ความรู้แบบฝังลึก (Tacit Knowledge) เป็นความรู้อย่างไม่เป็นทางการ ซึ่งเป็นทักษะหรือความรู้เฉพาะตัวของแต่ละบุคคล ยากแก่การสื่อสารแก่ผู้อื่น ดังที่ Michael Polanyi กล่าวไว้ว่าคนเราสามารถรู้ได้มากกว่าที่พูดออกไป 2. ความรู้แบบชัดแจ้ง (Explicit Knowledge) เป็นความรู้ที่เป็นทางการ มีลายลักษณ์อักษร เป็นระบบ จึงทำให้สื่อสารและถ่ายทอดได้ง่าย อย่างไรก็ตามการสื่อสารต้องอาศัยความรู้ทั้ง 2 ประเภทประกอบกันเพื่อถ่ายทอดให้กับผู้อื่น อาจจะมีกลไกในการเปลี่ยนความรู้ประเภทหนึ่งเป็นอีกประเภทหนึ่งเพื่อให้การถ่ายทอดความรู้มีประสิทธิภาพมากขึ้น ที่มีขั้นตอน ดังนี้

1. การแลกเปลี่ยนเรียนรู้ (Socialization) การเรียนรู้ แลกเปลี่ยนความรู้แบบฝังลึก ผ่านการแบ่งปันประสบการณ์ระหว่างกันในขณะที่อยู่ในสภาพแวดล้อมเดียวกัน โดยอีกฝ่ายสามารถรับรู้ได้จากการสังเกตการณ์ การฝึกปฏิบัติ ดังเช่นที่ ธปท. มีการจัดจัดการประชุมเชิงปฏิบัติการ (Workshop) ให้กับผู้ปฏิบัติงานของสถาบันการเงิน รวมทั้งจัด Boot camp ให้กับนักศึกษาได้ฝึกรับมือภัยคุกคามไซเบอร์ เพื่อให้คนเหล่านั้นได้เรียนรู้ความรู้แบบฝังลึกที่ถ่ายทอดได้ยากผ่านประสบการณ์จริง

---

[5] Ikujiro Nonaka, “The Knowledge-Creating Company,” Harvard Business Review (November-December 1991). p. 98-99.

2. การถ่ายทอดความรู้ (Articulation) การเปลี่ยนความรู้แบบฝังลึกที่อยู่ในคนให้กลายเป็นความรู้แบบชัดแจ้ง เพื่อให้สามารถสื่อสารกับผู้อื่นได้

3. การผสานความรู้ (Combination) จัดการความรู้ทั้งหมดเข้าด้วยกันให้เป็นองค์ความรู้ โดยจัดทำในรูปแบบของคู่มือ เช่นเดียวกับที่ ธปท. ได้ออกแนวปฏิบัติให้สถาบันการเงินดำเนินการตามที่ได้ผสานมาตรฐานสากล ร่วมกับบทเรียนจากประสบการณ์ที่ผ่านมาในอดีต

4. การซึมซับความรู้ (Internalization) การแบ่งปันความรู้ไปให้ผู้อื่น ก่อให้เกิดแนวคิดหรือทักษะความรู้ใหม่ ๆ ทำให้ความรู้ชัดแจ้งกลายเป็นความรู้แบบฝังลึกอีกครั้ง แต่เป็นการเพิ่มระดับของความรู้แบบฝังลึกมากขึ้น มีความเข้าใจลึกซึ้งและเชี่ยวชาญมากขึ้น ซึ่งวัตถุประสงค์ของการให้ความรู้ของ ธปท. มีทั้งการให้ความรู้เพื่อต่อยอดความรู้เดิมของเหล่าผู้บริหารและผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ของสถาบันการเงิน เพื่อให้คนเหล่านั้นไปสร้างสรรค์แนวคิด แนวปฏิบัติใหม่ ๆ ที่มีประสิทธิภาพในการดำเนินงานมากขึ้นกว่าเดิม รวมทั้งสามารถนำไปถ่ายทอดต่อไปให้ผู้อื่นได้ด้วย

5.3 อภิปรายผลการศึกษาแนวทางการสร้างความร่วมมือระหว่างกลุ่มสถาบันการเงินในการกำหนดมาตรการป้องกันอาชญากรรมไซเบอร์

จากผลศึกษาแนวทางการสร้างความร่วมมือระหว่างกลุ่มสถาบันการเงินในการกำหนดมาตรการป้องกันอาชญากรรมไซเบอร์ เห็นได้ว่า ธปท. มีการผลักดันให้จัดตั้งศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร หรือ Thailand Banking Sector CERT (TB-CERT) ส่งผลให้สถาบันการเงินมีศูนย์กลางร่วมกันที่มั่นคงแข็งแกร่งเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ มีการแบ่งปันข่าวสาร นำบทเรียน ประสบการณ์จากเหตุการณ์ภัยคุกคามที่แต่ละแห่งพบเจอมาเป็นบทเรียนร่วมกันพัฒนาแนวทางการป้องกันแก้ไขให้มีประสิทธิภาพมากขึ้น ซึ่งสอดคล้องกับทฤษฎีการเรียนรู้แบบร่วมมือ (Theory of Cooperative or Collaborative Learning) ที่ Johnson and Johnson[6] กล่าวไว้ว่า ปฏิสัมพันธ์ระหว่างผู้เรียนมี 3 ลักษณะ คือ

1. ลักษณะแข่งขันกัน
2. ลักษณะต่างคนต่างเรียน
3. ลักษณะร่วมมือกันหรือช่วยกันในการเรียนรู้

ซึ่งการมีปฏิสัมพันธ์แบบร่วมมือหรือช่วยเหลือกันในการเรียนรู้ตรงกับลักษณะความร่วมกันระหว่างกลุ่มสถาบันการเงินที่ต่างคนต่างรับผิดชอบความมั่นคงทางไซเบอร์ของตน เรียนรู้จากเหตุการณ์ต่าง ๆ ที่พบเจอ ขณะเดียวกันก็นำประสบการณ์นั้นมาแบ่งปันให้ผู้อื่นรับทราบ และคอยช่วยเหลือองค์กรอื่นให้ได้เรียนรู้ไปด้วยกัน ได้มีการหารือปรึกษากัน และแบ่งปันแนวปฏิบัติที่มี

[6] ทิศนา แขมมณี, ศาสตร์การสอน (กรุงเทพฯ: สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย, 2554)

ประสิทธิภาพ หรือทักษะที่แตกต่าง ซึ่งสอดคล้องกับ Graham & Wright[7] ที่ได้ศึกษาความหมายของความร่วมมือจากการสอบถามความคิดเห็นของผู้เชี่ยวชาญ และพบว่าตัวบ่งชี้ของความร่วมมือประกอบด้วย 1. การวางแผน (Planning) 2. การแบ่งปัน (Sharing) และ 3. การดำเนินการเพื่อให้บรรลุเป้าหมาย (Goal Achieving Activities) ซึ่งแน่นอนว่าเป้าหมายของทุกคนองค์กรที่เป็นสมาชิก TB-CERT คงหนีไม่พ้นระบบและเครือข่ายของตนมีความมั่นคงปลอดภัยทางไซเบอร์ อย่างไรก็ตาม การที่ ธปท. ไม่เข้าร่วมเป็นสมาชิกของ TB-CERT เป็นการหลีกเลี่ยงไม่ให้สถาบันการเงินที่เป็นสมาชิกเกิดความอึดอัดใจในการร่วมมือกันดำเนินการตามวัตถุประสงค์การจัดตั้งองค์กร สอดคล้องกับงานวิจัยของนิรันดร์ จงวุฒิเวศย์[8] ได้ศึกษาเรื่องการมีส่วนร่วมของประชาชนในการพัฒนา ผลการศึกษาพบว่าความร่วมมือนั้นจะต้องมีเงื่อนไขที่สำคัญอย่างน้อย 3 ประการ คือ ทุกคนจะต้องมีอิสรภาพที่จะให้ความร่วมมือ ทุกคนมีความสามารถที่จะให้ความร่วมมือ และทุกคนต้องเต็มใจต่อการร่วมมือ

นอกเหนือจากความร่วมมือระหว่างกลุ่มสถาบันการเงินกันเองแล้ว ธปท. ยังได้ร่วมมือกับองค์กรภาคธุรกิจอื่นทั้งในและต่างประเทศ มีทั้งแบบลงนามสัญญาอย่างเป็นทางการ และร่วมมืออย่างไม่เป็นทางการ โดยมีวัตถุประสงค์ร่วมกันด้านความมั่นคงปลอดภัยไซเบอร์ ไม่ว่าจะเป็นการพัฒนาบุคลากรให้มีทักษะเท่าทันเทคโนโลยี แลกเปลี่ยนความรู้ ซึ่งองค์กรต่าง ๆ ที่ ธปท. ได้ร่วมมือด้วยนั้นต่างมีหน้าที่ความรับผิดชอบบางอย่างที่เชื่อมโยงกัน ซึ่งรูปแบบความร่วมมือกันอย่างเป็นทางการที่มีการลงนามบันทึกระหว่างผู้บริหารหรือผู้แทนองค์กรนั้น สอดคล้องกับทฤษฎีประโยชน์จากการประสานความร่วมมือ (Collaborative Advantage Theory) ที่ Vangen & Huxham[9] กล่าวว่าความร่วมมือเกิดจาการสนับสนุนขององค์กรให้บรรลุจุดมุ่งหมายที่ตั้งเอาไว้ โดยการตัดสินใจเข้าร่วมมือนั้นเกิดจากผู้นำขององค์กรนั้น ๆ และเป็นการพัฒนากิจกรรม/โครงการที่สร้างขึ้น โดยส่วนใหญ่แล้วความร่วมมือนั้นเป็นความร่วมมือระหว่างภาครัฐและองค์กรที่ไม่แสวงหาผลกำไร หรือภาครัฐกับรัฐวิสาหกิจ แต่ก็รวมถึงภาครัฐและภาคเอกชนด้วย และเมื่อเกิดความร่วมมือระหว่างองค์กรขึ้นผลประโยชน์ทางธุรกิจก็จะเกิดตามมา ซึ่ง Vangen & Huxham ได้ระบุผลประโยชน์ที่เกิดจากความร่วมมือไว้ซึ่งมีความสอดคล้องกับผลการศึกษา ได้แก่

---

[7] พิฑูรย์ ทองฉิม, “แนวคิดการจัดการความร่วมมือด้านการท่องเที่ยวโดยชุมชนเกาะลันตา จังหวัดกระบี่,” (วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาการจัดการการท่องเที่ยว คณะบริหารธุรกิจ มหาวิทยาสงขลานครินทร์, 2558)

[8] นิรันดร์ จงวุฒิเวศย์, การมีส่วนร่วมของประชาชนในการพัฒนา (กรุงเทพฯ: สำนักพิมพ์มหาวิทยาลัยมหิดล, 2527)

[9] Siv Vangen and Chris Huxham, “Introducing the theory of collaborative advantage” in The New Public Governance? Emerging Perspectives on the Theory and Practice of Public Governance, Stephen P. Osborne (London: Routledge, 2010), p. 163-184.

การเข้าถึงทรัพยากรและความเชี่ยวชาญ (Gaining access to resource and expertise) ธปท. และองค์กรที่ร่วมมือมีแบ่งปันทรัพยากรด้านข้อมูลร่วมกันทั้งภัยคุกคามที่ประสบ แนวคิดหรือแนวทางป้องกันแก้ไขที่แต่ละองค์กรมี ทักษะความเชี่ยวชาญของบุคลากรในองค์กรเพื่อช่วยพัฒนา ถ่ายทอดความรู้ให้กับองค์กรอื่น หรือหากประสบภัยคุกคามย่อมสามารถขอความช่วยเหลือทั้งด้านทักษะความรู้ หรือบุคลากรที่มีความเชี่ยวชาญเข้าช่วยเหลือได้

การแบ่งปันความเสี่ยง (Sharing risk) ทุกองค์กรที่เข้าร่วมมือกันในวัตถุประสงค์เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ ความเสี่ยงหนึ่งที่ทุกองค์กรมีเหมือนกันคือความเสี่ยงด้านการถูกคุกคามทางไซเบอร์ต่อระบบและเครือข่ายของตน การร่วมมือกันจะทำให้เห็นมุมมองความเสี่ยงและการบริหารความเสี่ยงของแต่ละองค์กรที่แตกต่างกัน ซึ่งสามารถนำการแนวคิดการบริหารความเสี่ยงขององค์กรอื่นไปประยุกต์ใช้เพื่อลดความเสี่ยงขององค์กรของตนได้

พัฒนาการประสานงาน (Improving coordination in service provision) การร่วมมือกันระหว่างองค์กรย่อมต้องมีการสื่อสารที่มีประสิทธิภาพ มีความชัดเจน ตรงไปตรงมา เพื่อให้เกิดความเข้าใจ บรรลุวัตถุประสงค์เดียวกัน รวมทั้งเกิดความเชื่อใจ ส่งผลต่อการสัมพันธภาพระหว่างองค์กร บางองค์กรอาจจะไม่เคยหรือมีโครงการร่วมมือกับองค์กรอื่นน้อย ก็จะได้เรียนรู้ทักษะด้านการประสานงานระหว่างองค์กรเพิ่มขึ้นด้วย

เพิ่มประสิทธิภาพ (Increasing efficiency) การร่วมมือกันระหว่างองค์กรช่วยทำให้แต่ละองค์กรได้รับผลประโยชน์ด้านไซเบอร์มากมาย อาทิ ข้อมูล ความรู้ บทเรียน การพัฒนาทักษะของบุคลากร แนวปฏิบัติ ซึ่งสิ่งเหล่านี้แต่ละองค์กรสามารถนำไปบริหารจัดการภายในเพื่อพัฒนานโยบายและการปฏิบัติงานภายในองค์กรด้านความมั่นคงปลอดภัยไซเบอร์ให้มีประสิทธิภาพมากขึ้นได้

5.4 ข้อเสนอแนะและแนวทางแก้ไข

ในส่วนข้อเสนอแนะและแนวทางแก้ไข ผู้วิจัยได้แบ่งเป็น 3 ส่วน ดังนี้

5.4.1 ข้อเสนอแนะและแนวทางแก้ไขเชิงปฏิบัติการ

จากการศึกษาพบว่า การป้องกันภัยคุกคามไซเบอร์ของสถาบันการเงินค่อนข้างมีความเข้มแข็ง มีการกำหนดมาตรการป้องกันภัยอย่างรัดกุม รวมทั้งการตรวจจับภัยคุกคามไซเบอร์สามารถปฏิบัติได้ค่อนข้างดี นอกเหนือจากการป้องกัน และการตรวจจับแล้ว การรับมือภัยคุกคามก็มีความสำคัญเช่นเดียวกัน ดังนั้นสถาบันการเงินควรมีการฝึกซ้อมรับมือภัยคุกคามไซเบอร์เป็นประจำสม่ำเสมอ เพื่อให้เมื่อเกิดเหตุการณ์คุกคามแล้วสามารถตอบสนอง และบริหารจัดการได้อย่างรวดเร็ว สามารถลดผลกระทบและความเสียหายที่จะเกิดขึ้น เนื่องจากการฝึกซ้อมจะทำให้สถาบันการเงินสามารถเห็นจุดอ่อนที่เกิดขึ้นในแต่ละครั้ง และนำจุดอ่อนของการฝึกซ้อมรับมือนั้น ๆ มาปรับปรุงและพัฒนาแนวปฏิบัติให้ดีขึ้น จนในที่สุดจะสามารถรับมือภัยคุกคามไซเบอร์ได้อย่างเข้มแข็ง

ซึ่งวิวัฒนาการของเทคโนโลยีในปัจจุบันเปลี่ยนแปลงอย่างรวดเร็ว ส่งผลให้อาชญากรรมไซเบอร์ได้พัฒนาเปลี่ยนรูปแบบไปด้วย หลายครั้งผู้ใช้บริการตกเป็นเหยื่อกลายเป็นผู้เปิดประตูนำอันตรายทางไซเบอร์มาสู่ระบบหรือเครือข่ายของสถาบันการเงินโดยไม่ได้ตั้งใจ อาจเกิดจากความประมาท ขาดความรู้ความเข้าใจ หรือไม่ระมัดระวังเพียงพอ เช่น บอกชื่อบัญชี (Username) และรหัสผ่าน (Password) ให้อาชญากร คลิกลิงค์ (Link) ปลอมกลายเป็นช่องทางให้อาชญากรสามารถเข้าถึงข้อมูลส่วนบุคคลและเข้าถึงระบบหรือเครือข่ายของสถาบันการเงิน ดังนั้นการสร้างความตระหนัก (Awareness) ให้กับประชาชนผู้ใช้บริการเป็นสิ่งหนึ่งที่สำคัญที่สามารถปิดช่องโหว่เพื่อรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้ ซึ่งการให้ความรู้และสร้างความตระหนักนี้ควรดำเนินการเพิ่มขึ้นและดำเนินการในเชิงรุก เพื่อให้สามารถเข้าถึงประชาชนได้จริง ประชาชนได้ปฏิบัติจริง เข้าใจสถานการณ์ที่อาจเกิดขึ้น เช่น การสร้างอีเมลปลอม (Phishing mail) ส่งไปให้ประชาชน สุ่มทำอย่างสม่ำเสมอโดยเปลี่ยนสถานการณ์ในการหลอกลวงไม่ให้ซ้ำเดิม และวัดผลการดำเนินการแต่ละครั้งว่ามีผู้ตกเป็นเหยื่อมากน้อยเพียงใด จากนั้นออกแบบมาตรการเพื่อสร้างความตระหนักให้เหมาะสมต่อไป

ทรัพยากรบุคคลเป็นสิ่งหนึ่งที่มีความสำคัญเป็นกำลังสำคัญในการร่วมออกแบบมาตรการที่มีประสิทธิภาพ และสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับระบบและเครือข่าย ดังนั้นควรจัดหาหรือพัฒนาทักษะของบุคลากรให้มีความรู้และทักษะที่เท่าทันอาชญากรไซเบอร์ ซึ่งอาจจำเป็นต้องมีผู้เชี่ยวชาญหลายด้านร่วมมือกัน นอกเหนือจากความเชี่ยวชาญแล้ว คนเหล่านั้นต้องมีวิสัยทัศน์ต่อความมั่นคงปลอดภัยไซเบอร์ที่ดีด้วย การสรรหาบุคลากรใหม่ ๆ เข้ามาร่วมทีมทำงานนั้น ส่วนใหญ่บุคคลเหล่านั้นมักมีพื้นฐานหรือจบการศึกษาเกี่ยวกับเทคโนโลยีสารสนเทศ จากนั้นนำมาต่อยอดความคิดประสบการณ์ต่อไป ซึ่งในปัจจุบันนักศึกษาที่ศึกษาด้านเทคโนโลยีสารสนเทศอาจไม่ได้ให้ความสนใจ ที่จะเข้ามาทำงานร่วมกับองค์กรภาคการเงิน การวางแผนทางก้าวหน้าในสายอาชีพ (Career Path) จึงมีส่วนสำคัญที่จะทำให้กลุ่มคนเหล่านี้มองเห็นถึงความก้าวหน้าในสายอาชีพ และให้ความสนใจเข้ามาทำงานในองค์กรภาคการเงินมากขึ้น ธปท. และสถาบันการเงินจึงควรเข้าไปสร้างความเชื่อมโยงกับคนที่มีทักษะ ความรู้ด้านเทคโนโลยีสารสนเทศเหล่านี้ให้เข้าสู่ภาคการเงินให้มากขึ้น นำมาพัฒนาให้กลายเป็นผู้เชี่ยวชาญ เพื่อร่วมเป็นกำลังสำคัญในการพัฒนาความมั่นคงปลดภัยไซเบอร์

5.4.2 ข้อเสนอแนะและแนวทางแก้ไขเชิงนโยบาย

ธปท. ควรเพิ่มบทลงโทษของการไม่ปฏิบัติตามตามประกาศ หรือแนวปฏิบัติที่ได้ออกใช้ เพื่อให้สถาบันการเงินมีความเกรงกลัว และปฏิบัติตามอย่างเคร่งครัด เนื่องจากปัจจุบัน ธปท. ไม่ได้กำหนดบทลงโทษใด เป็นเพียงการขอความร่วมมือให้สถาบันการเงินปฏิบัติตามมาตรการที่ ธปท. กำหนดเท่านั้น

ธปท. ควรออกประกาศ เกณฑ์ แนวปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ให้ครอบคลุมทุกกลุ่มสถาบันการเงินและผู้ให้บริการทางการเงินรายย่อย เช่น ผู้ให้บริการ e-payment เนื่องจากปัจจุบันเทคโนโลยีบล็อกเชน (Blockchain) ได้เข้ามามีบทบาทมากขึ้น ส่งผลให้มีผู้ให้บริการทางการเงินรายย่อยเข้ามาสู่ธุรกิจภาคการเงินมากขึ้น และมีแนวโน้มที่จะมากขึ้นเรื่อย ๆ ในอนาคต

รวมทั้งจะเพิ่มบทบาทในระบบการเงิน ดังนั้นการกำกับดูแลผู้ให้บริการทางการเงินรายย่อยก็เป็นสิ่งที่สำคัญไม่น้อยกว่าการกำกับดูแลสถาบันการเงินรายใหญ่

ธปท. ควรทบทวนประกาศ เกณฑ์ แนวปฏิบัติเป็นประจำ และพัฒนามาตรการด้านความมั่นคงปลอดภัยไซเบอร์ให้หลากหลาย เท่าทันกับเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว เพื่อสามารถรองรับภัยคุกคามไซเบอร์ใหม่ ๆ ที่อาจพัฒนามาในรูปแบบที่แตกต่างไปจากเดิม ซึ่งเทคโนโลยีใหม่จะทำให้สถาบันการเงินและผู้ให้บริการทางการเงินพัฒนาผลิตภัณฑ์ทางการเงินใหม่ ๆ และประชาชนมีช่องทางในการเข้าถึงระบบและเครือข่ายสถาบันการเงินได้ง่ายมากยิ่งขึ้น

ควรเร่งสร้างความร่วมมือกับภาครัฐเพื่อปรับหลักสูตรการเรียนการสอนให้มีการบรรจุบทเรียนในเรื่องภัยคุกคามไซเบอร์และความมั่นคงปลอดภัยทางไซเบอร์เข้าไปในหลักสูตร เนื่องจาก ในปัจจุบันกลุ่มเยาวชนที่อยู่ในวัยเรียนรู้ หรือ กลุ่ม Gen Z เป็นกลุ่มที่เกิดและเติบโตมาในสังคมที่ใช้เทคโนโลยีสารสนเทศขับเคลื่อนชีวิตประจำวัน การสร้างให้เกิดการเรียนรู้ตั้งแต่ในสถานศึกษาจะส่งผลให้เยาวชนเหล่านี้ มีภูมิคุ้มกันต่อภัยคุกคามทางไซเบอร์ อีกทั้งยังส่งผลให้เกิดการส่งต่อความรู้ไปยังกลุ่มคนในครอบครัว ให้ขยายวงกว้างจนกลายเป็นภูมิคุ้มกันหมู่ในสังคมในที่สุด

5.4.3 ข้อเสนอแนะสำหรับการวิจัยครั้งถัดไป

ควรศึกษาเพิ่มเติมโดยเปรียบเทียบกับมาตรการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ของธนาคารกลางในต่างประเทศเพื่อเห็นถึงความเหมือนและความแตกต่างที่อาจนำมาจุดเด่นหรือข้อดีของแต่ละประเทศมาเสนอแนะเพื่อพัฒนามาตรการกำกับดูแลของประเทศไทยต่อไป

ควรเพิ่มขอบเขตของกลุ่มตัวอย่างของบุคคลผู้เชี่ยวชาญให้มีความหลากหลายมากยิ่งขึ้น โดยศึกษาจากองค์กรกำกับดูแลอื่น เพื่อทราบบทบาทที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่อาจแตกต่างไปจากบทบาทของธนาคารแห่งประเทศไทย

ควรศึกษาตัวอาชญากรไซเบอร์ ถึงแรงจูงใจให้ก่ออาชญากรรมต่อกลุ่มสถาบันการเงิน ทั้งปัจจัยภายในตัวบุคคล และปัจจัยภายนอก รวมถึงการเลือกเหยื่อในการกระทำความผิด เพื่อนำมาประมวลวิเคราะห์เพื่อหาแนวทางในการป้องกันที่เหมาะสม

บรรณานุกรม

(องค์การมหาชน), สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. "พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พุทธศักราช 2560." https://ictlawcenter.etda.or.th/de_laws/detail/de-laws-computer-related-crime-act.

———. "ร่างกฎหมายเศรษฐกิจดิจิทัล " https://ictlawcenter.etda.or.th/de_laws.

Alfred D. Chandler, Jr. *Strategy and Structure: Chapters in the History of the Industrial Enterprise.* Cambridge: The MIT Press, 1962.

Bouveret, Antoine. "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment." IMF 2018.

GMBiZ. "Cyber Security & Fintech." https://gmlive.com/CyberSecurity-Fintech.

Huxham, Siv Vangen and Chris. *"Introducing the Theory of Collaborative Advantage" in the New Public Governance? Emerging Perspectives on the Theory and Practice of Public Governance.* London2010.

Kaspersky Lab. "Cyberthreat Real-Time Map " https://cybermap.kaspersky.com.

LawTeacher. "The Dark Figure of Crime " https://www.lawteacher.net/free-law-essays/criminology/the-dark-figure-of-crime.php.

Marion, Joshua B. Hill and Nancy E. *Introduction to Cybercrime.* California: ABC –CLIO LLC, 2016.

Nation, The. "Omise First in Thailand to Get Milestone Card Security Compliance Certification." (22 November 2016): 5.

News, Thai PBS. "เผยบังคลาเทศก็เคยเจอแฮกเกอร์เจาะแบงก์ สูญเกือบ 3 พันล้าน." http://news.thaipbs.or.th/content/255180.

NIST. "Cybersecurity Framework " https://www.nist.gov/cyberframework.

Nonaka, Ikujiro. *The Knowledge-Creating Company.* Harvard Business Review 1991.

OECD. "Introductory Handbook for Undertaking Regulatory Impact Analysis (Ria) ", 2008.

Parker, Don B. *Crime by Computer* New York: Charles Scribner's Sons, 1976.

Payne, Brian K. *White - Collar Crime* California: SAGE Publication, Inc, 2017.

Power, Gráinne Kirwan and Andrew. *Cybercrime.* Cambridge: Cambridge University Press, 2013.

Rachna Buch, Dhatri Ganda, Pooja Kalola and Nirala Borad. "World of Cyber Security and Cybercrime." *STM Journals* 4, no. 2 (August 2018): 18-23.

REDDY, G.NIKHITA REDDY and G.J.UGANDER. "Cyber Security Challenges and Its Emerging Trends on Latest Technologies." 2014.

Reuters. "Ukraine Central Bank Warns of New Cyber-Attack Risk " https://www.reuters.com/article/us-cyber-ukraine-banking/ukraine-central-bank-warns-of-new-cyber-attack-risk-idUSKCN1AY0Y4.

Russell G. Smith, Peter Grabosky and Gregor Urbas. *Cyber Criminals on Trial.* Cambridge: Cambridge University Press, 2004.

Something, Design. "The Broken Windows Theory ลดปัญหาอาชญากรรมในเมืองด้วย “ทฤษฎีกระจกแตก”." 2016.

Stallings, William. *Effective Cybersecurity* Pearson Education, Inc., , 2019.

TechTalkThai. "แฮ็คระบบ Swift ธนาคารยูเครน ขโมยเงินไปกว่า 350 ล้านบาท." https://www.techtalkthai.com/ukranian-bank-swift-hacked/.

———. "สรุปผลวิเคราะห์มัลแวร์ที่โจมตีตู้ Atm ธนาคารออมสินจาก Ncr " https://www.techtalkthai.com/malware-attack-in-thailand-by-ncr/.

Transport Journal. "แฮกเกอร์โจมตีแบงค์บังคลาเทศผ่านช่องทาง Swift ซอฟต์แวร์." 2559, 16.

Valvo, Anna Lucia. "Cybercrimes and Network Governance." (2016).

"เก็บเบี้ยใต้ถุนร้าน: ผุดศูนย์ป้องกันไซเบอร์กันแบงก์เสียหาย สร้างความมั่นใจลูกค้า." วารสารดอกเบี้ย, ตุลาคม 2560, 70-71.

เปี่ยมสมบูรณ์., ปุระชัย. การควบคุมอาชญากรรมจากสภาพแวดล้อม: หลักทฤษฎีและมาตรการ. กรุงเทพฯ: สถาบันบัณฑิตพัฒนบริหารศาสตร์, 2525.

แขมมณี, ทิศนา. ศาสตร์การสอน. กรุงเทพฯ: สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย, 2554.

"แนวทางการเข้าร่วมทดสอบและพัฒนานวัตกรรมที่นำเทคโนโลยีใหม่มาสนับสนุนการให้บริการทางการเงิน (Regulatory Sandbox)." edited by ประกาศธนาคารแห่งประเทศไทย ที่ ธปท.ฝทง.ว. 311/2562, 2562.

"แนวทางปฏิบัติสำหรับรักษาความปลอดภัยและควบคุมความเสี่ยงของระบบเทคโนโลยีสารสนเทศ (Information Technology Risk Management) และความเสี่ยงด้านภัยคุกคามทางไซเบอร์

(Cybersecurity)." edited by สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย, 2560.

"แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ." edited by ธนาคารแห่งประเทศไทย, 2563.

"แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลัก (It Best Practices) Phase 2: ธุรกรรมการเงินผ่านชองทางอิเล็กทรอนิกส การใหบริการการเงินและการชำระเงินทางอิเล็กทรอนิกส (E-Banking และ E-Payment) ". edited by ธนาคารแห่งประเทศไทย, 2563.

"แผนยุทธศาสตร์ 3 ปี ธปท. พ.ศ. 2560 - 2562 ". edited by ธนาคารแห่งประเทศไทย, 2560.

"แผนยุทธศาสตร์ ธปท. พ.ศ. 2563 - 2565." edited by ธนาคารแห่งประเทศไทย, 2563.

และกิจการโทรคมนาคมแห่งชาติ, สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์. "ยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ National Cybersecurity Strategy." https://www.nbtc.go.th/News/Information/National-Cybersecurity-Strategy-.aspx.

โพสต์ทูเดย์. "โจรไฮเทคพุ่งเป้า เจาะเอทีเอ็มทั่วโลก." 28 สิงหาคม 2559 2559, 3.

"กรอบการประเมินความพร้อมในการรับมือภัยคุกคามไซเบอร์." edited by ธนาคารแห่งประเทศไทย, 2562.

กรุงเทพธุรกิจ. "รัฐตั้งทีมป้องกันไซเบอร์ระดับชาติ " กรุงเทพธุรกิจ, 5 สิงหาคม 2560 2560, 3.

ขุขันธิน, วีรวดี. "การใช้งานสื่อสังคมออนไลน์สาธารณะมีผลกระทบต่อความมั่นคงปลอดภัยของกองทัพไทย." วิทยาลัยการทัพบก, 2560.

จงวุฒิเวศย์, นิรันดร์. การมีส่วนร่วมของประชาชนในการพัฒนา. กรุงเทพฯ สำนักพิมพ์มหาวิทยาลัยมหิดล, 2527.

จุฑารัตน์ เอื้ออำนวย. "การบริหารงานยุติธรรม: วิธีการศึกษา วิเคราะห์ และเปรียบเทียบการบริหารงานยุติธรรม." 2560.

ซามูเอล กรีนการ์ด. *The Internet of Things:* อินเทอร์เน็ตแห่งสรรพสิ่ง Translated by ทีปกร วุฒิพิทยามงคล. กรุงเทพฯ: โอเพ่นเวิลด์ส, 2560.

ทองฉิม, พิฑูรย์. "แนวคิดการจัดการความร่วมมือด้านการท่องเที่ยวโดยชุมชนเกาะลันตา จังหวัดกระบี่." มหาวิทยาสงขลานครินทร์, 2558.

"บันทึกข้อตกลงความร่วมมือด้านการยกระดับความพร้อมรับมือภัยคุกคามไซเบอร์ (Cert Readiness) ต่อภาคธุรกิจ การค้า อุตสาหกรรม และโครงสร้างพื้นฐานสำคัญของประเทศ." 2559.

"บันทึกข้อตกลงความร่วมมือด้านการยกระดับความพร้อมรับมือภัยคุกคามไซเบอร์ (Cert Readiness) ต่อภาคธุรกิจการเงิน การลงทุน และการประกันภัย."

"บันทึกข้อตกลงความร่วมมือด้านการยกระดับความพร้อมรับมือภัยคุกคามไซเบอร์ (Cert Readiness) ต่อภาคธุรกิจการเงิน การลงทุน และการประกันภัย." 2559.

บุญเจริญ, วรณัฐ. "มาตรการทางกฎหมายของอาเซียนเพื่อการคุ้มครองและป้องกันอาชญากรรมทางคอมพิวเตอร์." มหาวิทยาลัยแม่ฟ้าหลวง, 2557.

บุญโญภาส, วีระพงษ์. อาชญากรรมทางเศรษฐกิจ กรุงเทพ: สำนักพิมพ์นิติธรรม, 2549.

"ประกาศ ก.ล.ต. ที่ นป. 3/2559 เรื่องแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ." edited by สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, 2559.

"ประกาศ ก.ล.ต. ที่ สธ. 37/2559 เรื่องข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ." edited by สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, 2559.

"ประกาศธนาคารแห่งประเทศไทย ที่ สนช. 11/2561 นโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ ". edited by ธนาคารแห่งประเทศไทย, 2561.

"ประกาศธนาคารแห่งประเทศไทย ที่ สนส. 21/2562 เรื่องหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน." edited by ธนาคารแห่งประเทศไทย, 2562.

ประณีตพลกรัง, วิภารัตน์ ปทักขินัง และประสงค์. "การพัฒนาระบบสารสนเทศสำหรับการประเมินระดับความเสี่ยงและความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร." มหาวิทยาลัยศรีปทุม, 2557.

"พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562." 2562.

"พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560." 2560.

"พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550." 2550.

"พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544." 2544.

ภาชีรัตน์, ชญานิศ. "อาชญากรรมเศรษฐกิจที่เกี่ยวกับสถาบันการเงิน: ศึกษากรณีเปรียบเทียบมาตรการในการบังคับใช้กฎหมายของต่างประเทศและประเทศไทย." จุฬาลงกรณ์มหาวิทยาลัย, 2543.

มติชน. ""ไขปริศนา 'มัลแวร์' ตัวร้าย ดูดเงิน 'เอทีเอ็ม." มติชน, 25 สิงหาคม 2559, 9.

———. "ออมสินรับถูกแฮกเอทีเอ็ม 12 ล. โดนไวรัส200ตู้-สั่งปิดบริการชี้แก๊งยูเครน-ควบคุมจากสวิส ธปท.มึนสกัดล้วงอีแบงก์ยาก." 24 สิงหาคม 2559 2559, 1,7,12.

ราชกิจจานุเบกษา. "ประกาศ คปภ. เรื่องหลักเกณฑ์ วิธีการออกกรมธรรม์ประกันภัย การเสนอขายกรมธรรม์ประกันภัยและการชดใช้เงิน หรือค่าสินไหมทดแทนตามสัญญาประกันภัย โดยใช้วิธีการทางอิเล็กทรอนิกส์ พ.ศ. 2560 ", 2560.

———. "ประกาศ คปภ. เรื่องหลักเกณฑ์ วิธีการออกกรมธรรม์ประกันภัย การเสนอขายกรมธรรม์ประกันภัยและการชดใช้เงินตามสัญญาประกันชีวิต โดยใช้วิธีการทางอิเล็กทรอนิกส์ พ.ศ. 2560." 2560.

———. "พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล " http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF.

———. "พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์." http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0020.PDF.

วารสารดอกเบี้ย. "เก็บเบี้ยใต้ถุนร้าน: ผุดศูนย์ป้องกันไซเบอร์กันแบงก์เสียหาย สร้างความมั่นใจลูกค้า." วารสารดอกเบี้ย, ตุลาคม 2560, 70-71.

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย. "Fbi เผย ธนาคารกลางบังคลาเทศถูกเจาะระบบ เหตุฝีมือคนในร่วมด้วย." https://www.thaicert.or.th/newsbite/2016-05-11-01.html#2016-05-11-01.

สนธิ, ศรวัสย์. "ความรู้ ความเข้าใจด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ กรณีศึกษา: ข้าราชการ กองบัญชาการกองทัพไทย." มหาวิทยาลัยธุรกิจบัณฑิตย์, 2557.

สำนักงานสภาความมั่นคงแห่งชาติ. "นโยบายความมั่นคงแห่งชาติ พ.ศ. 2558-2564 " http://www.nsc.go.th/Download1/policy58.pdf.

"หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน." edited by ประกาศธนาคารแห่งประเทศไทย ที่ สนส. 19/2560, 2560

อัศวิน แสงพิกุล. "จริยธรรมการวิจัย." วารสารสุทธิปริทัศน์ มกราคม-มีนาคม 2556 2556, 136-46.

ประวัติผู้เขียน

ชื่อ-สกุล	พันจ่าเอกปรมัตถ์ ไวรักษ์
วัน เดือน ปี เกิด	21 ธันวาคม 2530
สถานที่เกิด	จังหวัดพะเยา
วุฒิการศึกษา	สำเร็จการศึกษาปริญญาตรี หลักสูตรรัฐประศาสนศาสตรบัณฑิต สาขาวิชารัฐประศาสนศาสตร์ คณะมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยราชภัฏเชียงใหม่