การจัดการความมั่นคงทางเทคโนโลยีสารสนเทศ กรณีศึกษา การคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย*

INFORMATION TECHNOLOGY SECURITY MANAGEMENT: A CASE STUDY OF PERSONAL DATA PROTECTION IN ELECTRONIC TRANSACTION OF THAI COMMERCIAL BANKS

กริน ธัญญวิกรม
Karin Tunyavikrom
ธีระ กุลสวัสดิ์
Teera Kulsawat
มหาวิทยาลัยบูรพา
Burapha University, Thailand
E-mail: karin.tun4@gmail.com

บทคัดย่อ

บทความวิจัยฉบับนี้มีวัตถุประสงค์เพื่อ 1) ศึกษาวิเคราะห์บริบทสภาพปัญหาและบทบาทหน้าที่ มาตรการของภาครัฐในการจัดการความมั่นคงปลอดภัยสารสนเทศ 2) ศึกษาการดำเนินการและมาตรการของธนาคารพาณิชย์ไทยในการจัดการความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ และ 3) ศึกษาข้อเสนอแนะ แนวทางการดำเนินงานและมาตรการที่เหมาะสมกับการจัดการความมั่นคงปลอดภัยสารสนเทศเพื่อการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย โดยผู้วิจัยใช้การวิจัยเชิงคุณภาพ ประกอบด้วยการวิจัยเชิงเอกสารและการสัมภาษณ์เชิงลึก จากผู้บริหารหน่วยงานกำกับดูแลของรัฐ ผู้เชี่ยวชาญ และธนาคารพาณิชย์ไทย กรณีศึกษา 3 แห่ง รวม 10 ท่าน โดยการคัดเลือกแบบเจาะจง นำข้อมูลมาวิเคราะห์เชิงเนื้อหาและนำเสนอในรูปแบบเชิงพรรณนา ผลการศึกษาพบว่า 1) ปัญหาภัยคุกคามทางไซเบอร์ ที่สำคัญ คือ ปัญหาด้านความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์และความพร้อมในการรับมือต่อการสูญเสียอธิปไตยไซเบอร์ของชาติ โดยภาครัฐได้ออกกฎหมายสำคัญ 2 ฉบับ ในปี พ.ศ. 2562 คือ พ.ร.บ.ไซเบอร์ฯ และ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล และธนาคารแห่งประเทศไทยได้ออกกฎระเบียบต่าง ๆ ในการกำกับดูแลธนาคาร

* Received 25 November 2020; Revised 13 March 2021; Accepted 22 March 2021

พาณิชย์ไทย 2) การดำเนินงานของธนาคารพาณิชย์ไทย ได้จัดทำนโยบายและแนวทางการดำเนินการด้านการรักษาความปลอดภัยของข้อมูลและความมั่นคงปลอดภัยไซเบอร์ ตามมาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001:2013) และ 3) จากการศึกษาข้อเสนอแนะเพื่อให้แนวทางในการดำเนินงานตาม พ.ร.บ.ไซเบอร์ฯ ควรสอดคล้องกับ NIST Cybersecurity Framework และนำมาตรฐาน ISO/IEC 27701:2019 มาใช้เป็นมาตรการเพิ่มเติมสำหรับการคุ้มครองข้อมูลส่วนบุคคลที่มีความสอดคล้องกับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

คำสำคัญ: การจัดการ, ความมั่นคงทางเทคโนโลยีสารสนเทศ, การคุ้มครองข้อมูลส่วนบุคคล, ธุรกรรมทางอิเล็กทรอนิกส์, ธนาคารพาณิชย์ไทย

Abstract

The Objectives of this research article were to 1) study and analyze the context, condition, problems, and roles as well as the measure of the government sector in information security management, 2) study the actions and measures of Thai commercial bank in information security management and personal data protection, and 3) study recommendations and guidelines for the implementation and appropriate measures for information security management to protect personal information in electronic transactions of Thai commercial bank. The research is a qualitative research consisting of research on the documentation and in - depth interviews of 10 executives, government regulators, specialists and 3 case studies of Thai commercial bank, selected by purposive selection. The data content was analyzed and the results were presented in a descriptive format. The study found that 1) the major cyber threats are cybersecurity readiness and preparedness to cope with the loss of national cyber sovereignty. The government has issued two important laws in 2019, namely, the Cyber Act and the Personal Data Protection Act, and the Bank of Thailand has issued various regulations to supervise Thai commercial bank, 2) Thai commercial banks have established policies and operational guidelines for information security and cybersecurity in accordance with the Information Security Management Standard (ISO/IEC 27001: 2013), and 3) Based on the study of recommendations to provide guidelines for the implementation of Cyber Security Act, the NIST Cybersecurity Framework and ISO/IEC 27701: 2019 should

be applied as an additional measure for the protection of personal information that is in accordance with Personal Data Protection Act.

Keywords: Management, Information Technology Security, Personal Data Protection, Electronic Transactions, Thai Commercial Banks

บทนำ

ปัจจุบันเทคโนโลยีและบริบททางเศรษฐกิจและสังคมกำลังเปลี่ยนแปลงอย่างรวดเร็วไปสู่ยุคดิจิทัล และหลายประเทศทั่วโลก เช่น สหรัฐอเมริกา กลุ่มประเทศในสหภาพยุโรป ออสเตรเลีย สิงคโปร์ มาเลเซีย อินเดีย ฯลฯ กำลังแข่งขันกันพัฒนาและขับเคลื่อนประเทศด้วยเทคโนโลยีดิจิทัล สำหรับประเทศไทย มีความมุ่งหวังในการปฏิรูปประเทศไทยให้ทันต่อบริบทดังกล่าวด้วยเช่นกัน โดยการจัดทำแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมขึ้น เพื่อการสร้างระบบเศรษฐกิจและสังคมดิจิทัลที่ทุกคนมีส่วนร่วมตามแนวทางประชารัฐ และใช้ประโยชน์จากนวัตกรรมดิจิทัลอย่างเต็มศักยภาพจนถึงการผลักดันให้ประเทศไทย ซึ่งอยู่ในกลุ่มประเทศกำลังพัฒนาให้เป็นประเทศในกลุ่มประเทศพัฒนาแล้ว ที่สามารถใช้เทคโนโลยีดิจิทัลสร้างมูลค่าและขับเคลื่อนระบบเศรษฐกิจและสังคมอย่างยั่งยืนในระยะยาว (สำนักงานรัฐบาลอิเล็กทรอนิกส์, 2559)

ปัจจุบันธนาคารได้นำเทคโนโลยีดิจิทัลมาใช้มากขึ้นในการทำธุรกรรมทางการเงิน โดยเฉพาะระบบ การชำระเงินถือว่าเป็นส่วนหนึ่งที่ประยุกต์เทคโนโลยีเข้ามาตอบสนองความต้องการของลูกค้าในรูปแบบดิจิทัลแบงก์กิ้ง (Digital banking) การให้บริการลูกค้าในการทำธุรกรรมกับธนาคาร โดยลูกค้าไม่จำเป็นต้องมาธนาคาร เช่น การให้บริการทางโทรศัพท์ (Call Center) การทำธุรกรรมทางการเงินผ่านช่องทางตู้เอทีเอ็ม อินเทอร์เน็ตแบงก์กิ้ง (Internet Banking) และโมบายแบงก์กิ้ง (Mobile Banking) เป็นต้น ดิจิทัลแบงก์กิ้งช่วยให้การทำธุรกรรมการเงินและการชำระเงินเป็นไปด้วยความสะดวก รวดเร็ว มีต้นทุนถูกลง และสามารถเข้าถึงบริการได้ง่ายขึ้นในทุกที่ทุกเวลาและทุกอุปกรณ์ (Anytime Anywhere Any device) (เทอดพงษ์ เปล่งศิริวัฒน์, 2558) แต่สิ่งที่มาพร้อมกับเทคโนโลยี คือ ภัยคุกคามทางไซเบอร์ (Cyber Threat) ที่ปัจจุบันเพิ่มขึ้นอย่างรวดเร็ว หลายรูปแบบและมีความซับซ้อนมากขึ้น ส่งผลเสียหายต่อสถาบันการเงินและผู้ใช้บริการ

ปัญหาภัยคุกคามทางไซเบอร์ที่ปัจจุบันเพิ่มขึ้นอย่างรวดเร็วและมีความซับซ้อนมากขึ้น สำหรับสถานการณ์ภัยคุกคามทางไซเบอร์ของโลก World Economic Forum ได้จัดทำ Global risk security reports 2020 ขึ้น ได้จัดให้ปัญหาภัยคุกคามทางไซเบอร์และการขโมยข้อมูลส่วนบุคคลมีความเสี่ยงที่สูง เป็น 1 ใน 10 ความเสี่ยงของโลกติดต่อกันมาหลายปี (World Economic Forum, 2020) ส่วนสถานการณ์ภัยคุกคามทางไซเบอร์ที่พบในประเทศไทยได้มุ่งเป้าไปยังหลายภาคส่วน โดยพบภัยคุกคามไซเบอร์ที่มีจุดประสงค์ทางการเงินใน

รูปแบบต่าง ๆ เช่น ฟิชชิ่งอีเมล เว็บไซต์ธนาคารปลอมเพื่อหลอกขโมยรหัสผ่านผู้ที่ใช้งานอิเล็กทรอนิกส์แบงก์กิ้ง (E - banking) การแพร่ระบาดของ มัลแวร์เรียกค่าไถ่ (Ransomware) สายพันธุ์ต่าง ๆ ที่เข้ารหัสลับข้อมูลในเครื่องทำให้เปิดใช้งานไม่ได้ ฯลฯ ซึ่งผู้ใช้งานและผู้ดูแลระบบที่ขาดความรู้ ความเข้าใจในการป้องกัน อาจตกเป็นเหยื่อจากภัยคุกคาม และส่งผลให้องค์กรได้รับความเสียหาย จากประเด็นปัญหาภัยคุกคามด้านไซเบอร์และภัยทางการเงินในปัจจุบัน สามารถสรุปเป็น 2 ประเภท คือ 1) การแฮ็คทางด้านเทคนิค (Technical Hacking) ซึ่งใช้การโจมตีที่อาศัยช่องโหว่ของซอฟต์แวร์ (Software) และ ฮาร์ดแวร์ (Hardware) 2) วิศวกรรมทางสังคม (Social Engineering) ซึ่งเป็นการโจมตีการรักษาความปลอดภัยโดยใช้เทคนิคทางจิตวิทยาสังคม ออกกลอุบายต่าง ๆ ให้ผู้เสียหายเปิดเผยหรือถูกขโมยข้อมูลส่วนตัวที่สำคัญ ด้วยความจำเป็นและความสำคัญดังกล่าวทำให้ธนาคารจำเป็นต้องทบทวนและปรับปรุงนโยบายทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศของตน โดยอาจจะอ้างอิงมาจากมาตรฐานที่เกี่ยวข้องกับความมั่นคงปลอดภัยของข้อมูลสารสนเทศในปัจจุบันซึ่งมีหลายมาตรฐานและเป็นที่ยอมรับว่าเป็นมาตรฐานที่มีความน่าเชื่อถือ เช่น มาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001) ที่เป็นที่ยอมรับในระดับสากล เข้ามาประยุกต์ใช้ในกระบวนการปฏิบัติงานในการให้บริการขององค์กร เพื่อให้องค์กรเกิดความมั่นคงปลอดภัย และเป็นการสร้างมาตรฐานให้ตัวองค์กรเอง ซึ่งจะช่วยให้องค์กรสามารถเตรียมพร้อมรับมือกับภัยคุกคามได้อย่างมีประสิทธิภาพ

ดังนั้นการจัดการความมั่นคงทางเทคโนโลยีจึงมีความสำคัญ เนื่องจากรัฐบาลมีการจัดทำแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมขึ้นเพื่อการสร้างระบบเศรษฐกิจและสังคมดิจิทัล และปัจจุบันธนาคารได้นำเทคโนโลยีดิจิทัลมาใช้มากขึ้นในการทำธุรกรรมทางการเงิน โดยเฉพาะระบบชำระเงิน แต่สิ่งที่มาพร้อมกับเทคโนโลยี คือ ภัยคุกคามทางไซเบอร์ (Cyber Threat) ที่ปัจจุบันเพิ่มขึ้นอย่างรวดเร็ว หลายรูปแบบและมีความซับซ้อนมากขึ้น ส่งผลเสียหายต่อสถาบันการเงินและผู้ใช้บริการ ผู้วิจัยจึงสนใจที่จะศึกษาบริบท สภาพปัญหา และมาตรการในการจัดการความมั่นคงปลอดภัยสารสนเทศของภาครัฐและการดำเนินการตามมาตรการในการคุ้มครองข้อมูลส่วนบุคคลจากปัญหาอาชญากรรม ภัยคุกคามทางไซเบอร์ ปัญหาข้อมูลส่วนบุคคลรั่วไหล และการขโมยข้อมูลด้วยวิธีวิศวกรรมสังคม (Social Engineering) ในการทำทุจริตธุรกรรมทางการเงินผ่านระบบออนไลน์หรือการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย เพื่อให้ข้อเสนอแนะ แนวทางการดำเนินงานและมาตรการที่เหมาะสมในการจัดการความมั่นคงของเทคโนโลยีสารสนเทศ เพื่อการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาวิเคราะห์บริบทสภาพปัญหาภัยคุกคามไซเบอร์และบทบาทหน้าที่มาตรการของภาครัฐในการจัดการความมั่นคงปลอดภัยสารสนเทศเพื่อการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย

2. เพื่อศึกษาการดำเนินการและมาตรการของธนาคารพาณิชย์ไทยในการจัดการความมั่นคงปลอดภัยสารสนเทศเพื่อการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์

3. เพื่อให้ข้อเสนอแนะ แนวทางการดำเนินงานและมาตรการที่เหมาะสมกับการจัดการความมั่นคงปลอดภัยสารสนเทศเพื่อการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย

วิธีดำเนินการวิจัย

การศึกษาครั้งนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) โดยผู้วิจัยศึกษาและรวบรวมข้อมูลจาก 2 แหล่งหลัก คือ

1. การศึกษาข้อมูลเอกสาร (Document Research) เป็นการศึกษา รวบรวมข้อมูลจากเอกสาร อาทิ ข้อมูลจากอินเทอร์เน็ต หนังสือ วารสาร บทความ ข้อมูลจากการประชุมสัมมนา กฎหมายในประเทศและต่างประเทศ และงานวิจัยที่เกี่ยวข้อง

2. การสัมภาษณ์ (Interview) ผู้ให้ข้อมูลสำคัญ (Key Informant) ประกอบด้วย 2 กลุ่ม ได้แก่ กลุ่มที่ 1 ผู้บริหารหน่วยงานกำกับดูแลของรัฐและผู้เชี่ยวชาญ จำนวน 7 ท่าน ได้แก่ ผู้บริหารและผู้เชี่ยวชาญของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ธนาคารแห่งประเทศไทย กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ผู้บริหารและผู้เชี่ยวชาญ จากภาคประชาสังคม ได้แก่ ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (TB - CERT) สมาคมความมั่นคงระบบสารสนเทศแห่งประเทศไทย และกลุ่มที่ 2 ผู้บริหารของธนาคารพาณิชย์ไทย กรณีศึกษา จำนวน 3 ท่าน รวมเป็น 10 ท่าน โดยการคัดเลือกแบบเจาะจง

3. เครื่องมือที่ใช้ในการวิจัย เป็นแบบสัมภาษณ์แบบไม่มีโครงสร้าง (Non-Structure Interview) สัมภาษณ์เชิงลึกจากผู้ให้ข้อมูลสำคัญ (Key Informant) กลุ่มที่ 1 ผู้บริหารหน่วยงานกำกับดูแลของรัฐและผู้เชี่ยวชาญ และแบบสัมภาษณ์แบบกึ่งโครงสร้าง (Semi - Structured Interviews) สัมภาษณ์ผู้บริหารธนาคารพาณิชย์ไทย กรณีศึกษา โดยจัดทำเครื่องมือที่ใช้ในการวิจัยเสนอให้อาจารย์ที่ปรึกษาและผู้ทรงคุณวุฒิ 3 ท่าน ตรวจสอบความเที่ยงตรงเชิงเนื้อหา (Content Validity) และความเหมาะสมของถ้อยคำ แล้วผู้วิจัย

นำเครื่องมือมาปรับปรุงแก้ไขตามข้อเสนอแนะก่อนนำเสนอขออนุมัติจากคณะกรรมการพิจารณาจริยธรรมการวิจัยในมนุษย์ มหาวิทยาลัยบูรพา

4. การวิเคราะห์ข้อมูล จากการเก็บรวบรวมข้อมูล ผู้วิจัยนำข้อมูลมาวิเคราะห์เชิงเนื้อหา (Content Analysis) และนำเสนอในรูปแบบเชิงพรรณนา

ผลการวิจัย

ผลการศึกษาตามวัตถุประสงค์ข้อที่ 1 พบว่า สถานการณ์ความพร้อมของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ สหภาพโทรคมนาคมสากล (International Telecommunication Union: ITU) ได้จัดอันดับดัชนีชี้วัดของการพัฒนาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ในรายงาน Global Cybersecurity Index: (GCI) 2018 เพื่อวัดระดับความเชื่อมั่นของประเทศทั่วโลกที่ตอบรับการสำรวจจากสมาชิกของ ITU ทั้งหมด 193 ประเทศ ในส่วนของประเทศไทย ถูกจัดอันดับอยู่ที่ 35 ตกลงมาจากปีก่อนซึ่งอยู่อันดับที่ 20 ในส่วนนี้ ผู้บริหารของ สพธอ. ให้ความเห็นในเรื่องนี้ว่า

“เนื่องจากในการสำรวจปี 2562 เป็นการสำรวจข้อมูลปี 2561 เรายังไม่มีกฎหมายไซเบอร์โดยเฉพาะอย่างยิ่ง NCSA เราตั้งไม่ทัน อาจทำให้คะแนนเราน้อยกว่าประเทศอื่นทำให้อันดับไม่ค่อยดีนัก ปีนี้เราต้องคอยดูการจัดอันดับหลังจากที่เรามีกฎหมายออกมาแล้วอันดับเราจะดีขึ้นหรือไม่ กฎหมายไซเบอร์ออกเดือนเมษายน ปี 2562 แต่ปีนี้ผลการสำรวจยังไม่ออกอาจจะติดปัญหาเรื่องสถานการณ์โควิค ทำให้ผลสำรวจออกมาล่าช้า” (ศุภโชค จันทรประทิน, 2563)

ส่วนเหตุการณ์สำคัญด้านภัยคุกคามไซเบอร์ของภาคการธนาคารทั่วโลก ปี พ.ศ. 2562 การโจมตีทางไซเบอร์ (Cyber Attack) เพื่อขโมยข้อมูลเป็นสำคัญ โดยส่วนใหญ่จะเป็นข้อมูลส่วนบุคคลของลูกค้าโดยเทคนิคของวิศวกรรมสังคม เช่น ฟิชชิ่ง มัลแวร์ (Phishing, Malware) และสถานการณ์ภัยคุกคามทางไซเบอร์ที่พบในประเทศไทยได้มุ่งเป้าไปยังหลายภาคส่วน โดยพบภัยคุกคามไซเบอร์ที่มีจุดประสงค์ทางการเงินในรูปแบบต่าง ๆ ที่พบมากที่สุด คือ ฟิชชิ่งอีเมล เพื่อหลอกให้กรอกข้อมูลสำคัญหรือการขโมยข้อมูล โดยการแพร่ระบาดของ มัลแวร์ (Malware) ที่ฝังตัวมากับอีเมล และปัจจุบันยังพบ มัลแวร์เรียกค่าไถ่ (Ransomware) สายพันธุ์ต่าง ๆ ที่เข้ารหัสลับข้อมูลในเครื่องทำให้เปิดใช้งานไม่ได้ ซึ่งวิธีการดังกล่าวเป็นการโจมตีโดยอาศัยวิธีวิศวกรรมสังคมซึ่งเป็นวิธีการโจมตีจุดอ่อนของคนที่ยังขาดความรู้ความเข้าใจและความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ต่าง ๆ ที่มีความซับซ้อนมากขึ้น

จากการสำรวจความต้องการบุคลากรด้านไอทีและการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) จากธนาคารสมาชิก TB - CERT จำนวน 22 ธนาคาร โดย TB - CERT

และธนาคารแห่งประเทศไทย พบว่าอัตราความต้องการบุคลากรเทียบกับที่มีในปัจจุบันเพิ่มขึ้นคิดเป็น 12% ประธานกรรมการ TB - CERT กล่าวถึงประเด็นนี้ว่า

“ในการสำรวจนี้ได้แบ่งกลุ่มสายงานตามมาตรฐาน NIST Special Publication 800-181 ปัญหาเรื่องการขาดแคลนบุคลากรและทักษะความรู้ด้านไอทีและไอทีซิเคียวริตี้ ไม่ใช่ปัญหาเฉพาะของภาคการธนาคาร เป็นปัญหาขององค์กรทั่วโลก ความต้องการบุคคลากรด้านนี้เพิ่มมากขึ้นเป็นผลมาจากการที่สังคมในปัจจุบันได้ก้าวเข้าสู่ยุคดิจิทัลและการพัฒนาเทคโนโลยีทำให้หลาย ๆ องค์กรมีการปรับตัวเพื่อเพิ่มประสิทธิภาพการทำงาน สำหรับธนาคารเองก็เช่นกัน” (กิตติ โฆษะวิสุทธิ์, 2563)

จากประเด็นปัญหาดังกล่าวสามารถสรุปปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ในระดับชาติ ได้เป็น 2 ปัญหาใหญ่ ๆ คือ 1) ความไม่พร้อมในการปกป้อง รับมือและแก้ไขภัยคุกคามทางไซเบอร์ และ 2) ความไม่พร้อมในการรับมือต่อการสูญเสียอธิปไตยไซเบอร์ของชาติ จากปรากฏการณ์โซเชียลมีเดียแหล่งใหม่ของซอฟต์พาวเวอร์ จากประเด็นอธิปไตยทางไซเบอร์ กรรมการผู้ทรงคุณวุฒิ คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ให้ความเห็นว่า

“เรามาพูดถึงอธิปไตยที่เราไม่มีอยู่อย่างแท้จริง เพราะเราต้องเอาข้อมูลไปเก็บบนแพลตฟอร์มของคนอื่น เช่น Facebook, Google ฉะนั้นเราต้องระวังเวลาเราให้สิทธิ์ ถ้าเขาเอาข้อมูลเราไปแล้ว ให้เขาไปแล้วเขาก็เอาข้อมูลของเราไปใช้ ได้เลย กลับกันถ้าเราเป็นเจ้าของแพลตฟอร์มถ้าเราเป็นแบงก์ เราทำ Mobile Banking ก็เป็นแพลตฟอร์ม เราจะเอาข้อมูลลูกค้าของแบงก์มาใช้ทำอะไร เราต้องบอกกล่าวลูกค้าของแบงก์ก่อน กลับกันทั้งคนใช้และคนถูกใช้” (ปริญญา หอมเอนก, 2563)

หน่วยงานภาครัฐที่การกำกับดูแลของภาครัฐ มี 2 หน่วยงานหลัก คือ

1. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) มีการดำเนินงานตามมาตรการต่าง ๆ ได้แก่ มาตรการทางกฎหมาย มาตรการทางเทคนิค มาตรการด้านโครงสร้างองค์กร มาตรการด้านการพัฒนาศักยภาพบุคลากร และมาตรการด้านการสร้างความร่วมมือ

มาตรการทางกฎหมายที่สำคัญ ในการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล ได้แก่ ชุดกฎหมายธุรกรรมทางอิเล็กทรอนิกส์ เพื่อส่งเสริมธุรกรรมทางอิเล็กทรอนิกส์อย่างมั่นคงปลอดภัยและมีความน่าเชื่อถือ และผลักดันกฎหมายสำคัญ 2 ฉบับ คือ 1) พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพและเพื่อให้มีมาตรการป้องกัน รับมือ และลด

ความเสี่ยงจากภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ และ 2) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพและเพื่อให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ ในส่วนของมาตรการทางเทคนิค ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ กำหนดให้จัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ แห่งชาติ และมาตรการด้านโครงสร้างองค์กร กฎหมาย 2 ฉบับนี้ได้จัดตั้งหน่วยงานกำกับดูแลของรัฐขึ้นมา 2 หน่วยงาน คือ สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เพื่อกำหนดนโยบาย แผนงานและการดำเนินงานต่าง ๆ ซึ่งทั้ง 2 หน่วยงาน ยังอยู่ในช่วงการจัดตั้งสำนักงานถาวร และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มีการเลื่อนการบังคับใช้ในหลายมาตราสำคัญออกไปอีก 1 ปี จากวันที่ 28 พฤษภาคม พ.ศ. 2563 เป็น วันที่ 1 มิถุนายน พ.ศ. 2564 เนื่องจากการดำเนินการที่ล่าช้า ยังไม่มีความพร้อมทั้งภาครัฐและภาคเอกชน เนื่องจากปัญหาการแพร่ระบาดของโรคโควิด-19 และมาตรการทางเทคนิค พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ นอกจาก สพธอ.นี้ยังมีมาตรการส่งเสริมสนับสนุนในด้านการพัฒนาศักยภาพบุคลากร การจัดฝึกอบรม การสัมมนาและความร่วมมือกับภาคการศึกษามหาวิทยาลัยต่าง ๆ และมาตรการด้านการสร้างความร่วมมือส่งเสริมระหว่างหน่วยงานสำคัญด้านกำกับดูแลของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ เช่น กลุ่มการเงิน ฯลฯ เพื่อร่วมกันผลักดันให้เกิดความร่วมมือในการแก้ไขปัญหาภัยคุกคามไซเบอร์ที่อาจกระทบต่อความมั่นคงและเสถียรภาพของประเทศและสร้างเครือข่ายความร่วมมือกับหน่วยงานต่างประเทศ เช่น JPCERT/CC

2. ธนาคารแห่งประเทศเทศไทย มาตรการกำกับดูแลของธนาคารแห่งประเทศเทศไทย ได้ออกประกาศและแนวปฏิบัติที่เกี่ยวข้อง เพื่อใช้ในการกำกับดูแลธนาคารพาณิชย์ไทย ในด้านการบริหารจัดการความเสี่ยงของเทคโนโลยีสารสนเทศ ซึ่งให้ความสำคัญกับการกำกับดูแลในด้านการใช้เทคโนโลยีสารสนเทศให้สอดคล้องกับกลยุทธ์ขององค์กรและให้กำหนดความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นความเสี่ยงในระดับองค์กร เพื่อให้ธนาคารพร้อมรับมือกับภัยคุกคามทางไซเบอร์

กฎระเบียบและแนวทางปฏิบัติที่สำคัญของธนาคารแห่งประเทศเทศไทย ได้แก่ 1) ประกาศเลขที่ สนส.21/2562 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน และแนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก 2) ประกาศเรื่อง การจัดทำ จัดเก็บและจัดส่งข้อมูลอิเล็กทรอนิกส์ของสถาบันการเงิน 3) แนวนโยบายการรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ 4) แนวปฏิบัติการทดสอบเจาะระบบ Intelligence-led 5) กรอบการประเมินความพร้อมการรับมือภัยคุกคามไซ

เบอร์ โดยทำการสำรวจความเสี่ยงของทุกธนาคารโดยใช้กรอบมาตรฐานสากลของ NIST Cybersecurity Framework 6) แนวทางการเปิดเผยข้อมูลสถิติระบบเทคโนโลยีสารสนเทศขัดข้องที่กระทบต่อการให้บริการสำคัญของธนาคารพาณิชย์ 7) แนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ในการให้บริการทางการเงิน และ 8) แนวปฏิบัติที่ดี IT Best Practices สำหรับการควบคุมความเสี่ยงของกระบวนการทำธุรกิจหลัก ธุรกรรมการเงินผ่านช่องทางอิเล็กทรอนิกส์ การให้บริการการเงินและการชำระเงินทางอิเล็กทรอนิกส์

ผลการศึกษาตามวัตถุประสงค์ข้อที่ 2 พบว่า การดำเนินงานของธนาคารพาณิชย์ไทย กรณีศึกษา มีการปฏิบัติสอดคล้องตามกฎหมายและกฎระเบียบ แนวทางปฏิบัติของธนาคารแห่งประเทศไทย โดยจัดทำนโยบายความมั่นคงปลอดภัยด้านสารสนเทศและความปลอดภัยไซเบอร์ขึ้นตามกรอบมาตรฐานสากล ISO/IEC 27001:2013 และได้ผ่านการรับรองมาตรฐานสากลนี้ เพื่อปฏิบัติตามกฎหมายและประกาศ แนวทางปฏิบัติดังกล่าว และเพื่อใช้เป็นแนวทางในการบริหารจัดการด้านการรักษาความปลอดภัยของข้อมูลและรับมือกับการโจมตีทางไซเบอร์อย่างมีประสิทธิภาพ นอกจากนี้ การดำเนินงานของธนาคารพาณิชย์ไทย มีการดำเนินงานที่สำคัญ ๆ ในหลายด้าน เช่น ด้านการสร้างวัฒนธรรมองค์กร การสร้างความตระหนักด้านความปลอดภัยของข้อมูลภายในธนาคารเอง และลูกค้าผู้ใช้บริการผ่านสื่อออนไลน์และออฟไลน์ และการดำเนินงานในการป้องกันปัญหาภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพ เช่น การจัดการทดสอบ Phishing Drill เพื่อทดสอบและสร้างความตระหนักเป็นการฝึกวิธีการรับมือเมื่อพนักงานได้รับอีเมลปลอมในสถานการณ์จริงอย่างสม่ำเสมอ ให้มีความระมัดระวังในการสังเกต ฟิชชิ่งอีเมล เพิ่มมากขึ้น เพื่อแก้ไขปัญหาภัยคุกคามทางไซเบอร์ที่พบบ่อยมากที่สุด คือ เทคนิคของการโจมตีด้วยวิธีวิศวกรรมสังคม (Social Engineering) เช่น ฟิชชิ่ง ซึ่งเน้นโจมตีจุดอ่อนของคน

ผลการศึกษาตามวัตถุประสงค์ข้อที่ 3 พบว่า ข้อเสนอแนะ แนวทางการดำเนินงานและมาตรการที่เหมาะสมกับการจัดการความมั่นคงปลอดภัยสารสนเทศเพื่อการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย จากการศึกษาสามารถสรุปผลได้ ดังนี้

1. ข้อเสนอแนะ แนวทางการดำเนินการตาม พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ 2562

พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ มีแนวความคิดมาจาก กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสหรัฐ (NIST Cybersecurity Framework: NIST CSF) โดยจะเห็นปรากฏอยู่ในมาตรา 13 ของ พ.ร.บ. ได้แก่ 1) การระบุความเสี่ยง 2) การป้องกันความเสี่ยง 3) การตรวจสอบและเฝ้าระวัง 4) การเผชิญเหตุ และ 5) การรักษาและฟื้นฟูความเสียหาย (Recovery)

ดังนั้น แนวทางในการดำเนินการ ควรจะสอดคล้องกับ NIST CSF ดังกล่าว ควรมีกิจกรรม ดังต่อไปนี้ 1) การกำหนดแนวทางการกำกับดูแลด้านไซเบอร์ 2) กำหนดโครงสร้างการกำกับดูแลและนโยบาย 3) การกำหนดกรอบการบริหารความเสี่ยงและการประเมินความเสี่ยง 4) การกำหนดแนวทางบริหารจัดการความเสี่ยงของผู้ให้บริการ 5) การทดสอบด้านความมั่นคงปลอดภัย การตรวจสอบช่องโหว่ และทดสอบเจาะระบบ 6) การตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ 7) การพัฒนาคู่มือการปฏิบัติงานและการเฝ้าระวังในภาวะปกติและในภาวะฉุกเฉิน 8) การเสริมสร้างความรู้ ความตระหนักให้กับพนักงานในองค์กรทุกระดับ คู่ค้าและผู้ใช้บริการ 9) จัดให้มีระบบเฝ้าระวังและจัดการภัยคุกคามไซเบอร์ 10) การพัฒนาแผนบริหารจัดการเหตุการณ์ภัยไซเบอร์ การพัฒนาแผนรองรับภัยคุกคามไซเบอร์ระดับไม่ร้ายแรง ระดับร้ายแรง ระดับวิกฤติ 11) การกำหนดกรอบการประสานกับไทยเซิร์ต, TB-CERT หน่วยงานกำกับดูแล 12) การแจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

2. สรุปข้อเสนอแนะแนวทางดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ซึ่งมีแนวคิดมาจาก หลักการด้านการคุ้มครองข้อมูลส่วนบุคคล OECD Privacy Principles ทั้ง 8 ข้อ และ กฎหมาย GDPR ของสหภาพยุโรป ดังนั้นองค์กรควรมีการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Policy) มีการจัดทำแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล โดยนโยบายคุ้มครองข้อมูลส่วนบุคคลขององค์กรควรสอดคล้องกับหลักการด้านการคุ้มครองข้อมูลส่วนบุคคล OECD Privacy Principles ทั้ง 8 ข้อ

การดำเนินการตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ควรมีกิจกรรม ดังต่อไปนี้ 1) แนวทางการกำกับดูแลในการคุ้มครองข้อมูลส่วนบุคคล 2) โครงสร้างการกำกับดูแลและนโยบายการคุ้มครองข้อมูลส่วนบุคคล 3) การกำหนดผู้ควบคุมข้อมูลส่วนบุคคล 4) การกำหนดเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) 5) การกำหนดผู้ประมวลผลข้อมูลส่วนบุคคล 6) การพิจารณาแยกแยะข้อมูลเพื่อกำหนดข้อมูลส่วนบุคคลที่ต้องดำเนินการตามกฎหมาย 7) การพัฒนากรอบการกำกับดูแลและการจัดการข้อมูล 8) กรอบการบริหารความเสี่ยงและการประเมินความเสี่ยง 9) การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA) 10) การพัฒนาวิธีปฏิบัติ ขั้นตอนปฏิบัติ คู่มือการปฏิบัติงาน 11) การให้ความรู้ สร้างความตระหนักรู้ ให้กับบุคคลากรทุกระดับในองค์กร 12) กรอบการประสานกับหน่วยงานกำกับดูแล หน่วยงานภาครัฐ และหน่วยงานความร่วมมืออื่น ๆ

3. สรุปข้อเสนอแนะปัญหาด้านความมั่นคงปลอดภัยไซเบอร์

ปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ ที่เป็นปัญหาในระดับชาติ สรุปได้เป็น 2 ปัญหาใหญ่ ๆ คือ 1) ความไม่พร้อมในการปกป้อง รับมือและแก้ไขภัยคุกคามทางไซเบอร์ และ 2) ความไม่พร้อมในการรับมือต่อการสูญเสียอธิปไตยไซเบอร์ของชาติ แนวทางใน

การแก้ปัญหาและข้อเสนอแนะต่อภาครัฐ ดังนี้ 1) การสร้างความตระหนักรู้ถึงความสำคัญในเรื่องการใช้ชีวิตอย่างปลอดภัยในโลกไซเบอร์ 2) การสร้างระบบการศึกษาด้านความมั่นคงปลอดภัยไซเบอร์ 3) การพัฒนากฎหมายและกฎระเบียบที่เกี่ยวข้องกับ เสนอให้รัฐควรสนับสนุน โครงการเร่งรัดการบังคับใช้กฎหมาย โดยการออกกฎหมายลูกและ ประกาศมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคล 3) การสร้างความร่วมมือขององค์กรทั้งภายในประเทศและต่างประเทศ 4) รัฐควรสนับสนุนและส่งเสริมให้มีการแข่งขันในการพัฒนาแพลตฟอร์มระดับประเทศ

อภิปรายผล

1. จากการศึกษาวิเคราะห์ บริบทสภาพปัญหาและบทบาทหน้าที่ มาตรการของภาครัฐในการจัดการความมั่นคงปลอดภัยสารสนเทศ พบว่า สถานการณ์ภัยคุกคามทางไซเบอร์ที่พบในประเทศไทย มีจุดประสงค์ทางการเงินในรูปแบบต่าง ๆ ที่พบมากที่สุด คือ ฟิชชิ่งอีเมล เพื่อหลอกให้กรอกข้อมูลสำคัญ หรือการขโมยข้อมูล โดยการแพร่ระบาดของ มัลแวร์ (Malware) ที่ฝังตัวมากับอีเมล และปัจจุบันยังพบมัลแวร์เรียกค่าไถ่ (Ransomware) ที่เข้ารหัสลับข้อมูลในเครื่องทำให้เปิดใช้งานไม่ได้ ซึ่งวิธีการดังกล่าวเป็นการโจมตีโดยอาศัยวิธีวิศวกรรมสังคมซึ่งเป็นวิธีการโจมตีจุดอ่อนของคนที่ยังขาดความรู้ความเข้าใจ จิตสำนึกและความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ต่าง และจากการศึกษามาตรการของรัฐ ด้านมาตรการทางกฎหมาย เพื่อแก้ปัญหาในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล ได้แก่ การออก พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล และมาตรการเสริมสร้างจิตสำนึกและความตระหนักรู้ สอดคล้องกับงานวิจัยของ นคร เสรีรัตน์ ได้ทำการศึกษาวิจัยเรื่อง การคุ้มครองข้อมูลส่วนบุคคล ข้อเสนอเพื่อการพัฒนาสิทธิรับรู้ข้อมูลข่าวสารในกระบวนการธรรมรัฐไทย การออกมาตรการทางกฎหมายเพื่อการคุ้มครองข้อมูลส่วนบุคคลเป็นเรื่องสำคัญ และจำเป็นในระดับนโยบายของรัฐ (National Policy) อย่างไรก็ตามมาตรการทางกฎหมายและการดำเนินการบังคับใช้กฎหมาย ยากที่จะสัมฤทธิ์ผลถ้าไม่มีการเสริมสร้างความรู้ความเข้าใจ และการสร้างความตระหนักรู้และเสริมสร้างจิตสำนึกของเจ้าหน้าที่ของรัฐและประชาชนควบคู่ไปกับการใช้มาตรการทางกฎหมาย (นคร เสรีรักษ์, 2548)

นอกจากนี้ยังมีมาตรการการกำกับดูแลของธนาคารแห่งประเทศไทย มีการออกประกาศ กฎระเบียบและแนวทางปฏิบัติ ที่สำคัญ ๆ เช่น ประกาศ เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน แนวปฏิบัติการทดสอบเจาะระบบแบบ Intelligence-led และมีการทดสอบอีเมลปลอมแบบเสมือนจริง (Phishing Drill) ภายในหน่วยงานของธนาคารแห่งประเทศไทยเอง ซึ่งเป็นมาตรการและการดำเนินงานดังกล่าว สอดคล้องกับงานวิจัยของ Stephen Lineberry

ทำการศึกษาเรื่อง “The Human Element The weakest Linkin information Security” ความจำเป็นขององค์กรต่าง ๆ ที่ต้องมีการประเมินความเสี่ยงทางด้านความปลอดภัยข้อมูลสารสนเทศด้วยกระบวนการต่าง ๆ เช่นการสแกนระบบเพื่อหาช่องโหว่ของระบบสารสนเทศ (Vulnerability Assessment) การทดลองเจาะระบบเครือข่ายขององค์กร (Network Penetration) และโดยเฉพาะอย่างยิ่งการทดสอบการจารกรรมข้อมูลสารสนเทศด้วยวิธีวิศวกรรมสังคม (Social Engineering Testing) เนื่องจากคนนั้นถือเป็นจุดอ่อนที่สุดในระบบสารสนเทศ ซึ่งสามารถเปิดโอกาสให้ผู้ไม่ประสงค์ดีสามารถขโมยข้อมูลสำคัญขององค์กรออกไปได้ (Stephen Lineberry, 2007)

2. จากการศึกษาการดำเนินการและมาตรการของธนาคารพาณิชย์ไทยในการจัดการความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ พบว่า การศึกษาการดำเนินการของธนาคารพาณิชย์ไทยมีความสอดคล้องตามกฎหมายและกฎระเบียบของธนาคารแห่งประเทศไทย โดยมีการประยุกต์กรอบการดำเนินงานตามมาตรฐานสากล ISO/IEC 27001:2013 เพื่อใช้เป็นแนวทางในการบริหารจัดการด้านการรักษาความปลอดภัยของข้อมูลและรับมือกับการโจมตีทางไซเบอร์อย่างมีประสิทธิภาพและได้ผ่านรับการรับรองมาตรฐานมาตรฐานสากลนี้ จากผลการศึกษานี้ สอดคล้องกับงานวิจัยของ Azuwa, M.P. et al. ศึกษาเรื่อง Technical Security Metrics Model (TSMM) สำหรับการปฏิบัติตามมาตรฐาน ISO/IEC 27001 ซึ่งเป็นกาวัดผลรูปแบบหนึ่งที่ใช้ยืนยันประสิทธิภาพของระบบการป้องกันระบบข้อมูลข่าวสาร ผลการวิจัยพบว่า รัฐบามาเลเซียได้มองเห็นถึงความสำคัญขององค์กรด้าน Critical National Information Infrastructure (CNII) ทีจะต้องป้องกันระบบข้อมูลที่สำคัญ โดยในปี 2010 รัฐบาลได้มีคำสั่งให้ระบบขององค์กรเหล่านั้นต้องได้รับการรับรองเป็น ISO/IEC 27001 ภายในเวลา 3 ปี (Azuwa, M.P. et al., 2012) และสอดคล้องกับงานวิจัยของ Manar Abu et al. ศึกษาเรื่อง คำแนะนำ ISO/IEC 27001 กรณีศึกษาของประเทศสหรัฐอาหรับอมิเรตส์ (UAE) ผลการวิจัยพบว่า ISO/IEC 27001 เป็นมาตรฐานที่มีการใช้มากที่สุดในองค์กรและถูกใช้โดยองค์กรที่ทำหน้าที่ประมวลผล จัดการข้อมูลแทนองค์กรอื่น เพื่อใช้ยืนยันการป้องกันข้อมูลที่สำคัญของลูกค้า (Manar Abu et al., 2012)

นอกจากนี้พบว่า การดำเนินงานของธนาคารพาณิชย์ไทยมีการดำเนินงานที่สำคัญ ๆ ในหลายด้าน เช่น ด้านการสร้างวัฒนธรรมองค์กร การสร้างความตระหนักด้านความปลอดภัยของข้อมูล และการดำเนินงานในการป้องกันปัญหาภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพ เช่น การจัดการทดสอบ Phishing Drill โดยส่งอีเมลปลอมให้กับพนักงานของธนาคาร เพื่อแก้ไขปัญหาภัยคุกคามทางไซเบอร์ที่พบบ่อยมากที่สุดพบ คือ เทคนิคของการโจมตีด้วยวิธีวิศวกรรมสังคม (Social engineering) เช่น ฟิชชิ่ง ซึ่งเน้นโจมตีจุดอ่อนของคน สอดคล้องกับงานวิจัยของ Bevis, J. ทำการศึกษาเรื่อง “Extreme Social Engineering-combating the Insider

Security Threat-A Security Awareness Exercise” ศึกษาถึง จุดอ่อนของพฤติกรรมของมนุษย์ที่ส่งผลต่อความปลอดภัยของข้อมูลสารสนเทศและทรัพยากรระบบขององค์กร ผลเสียที่เกิดขึ้นกับองค์กรจากการที่พนักงานในองค์กรนั้นขาดความตระหนักในเรื่องความปลอดภัยของข้อมูลสารสนเทศขององค์กร พร้อมทั้งเสนอแนะวิธีการป้องกันการจารกรรมข้อมูลสารสนเทศโดยอาศัยวิธีวิศวกรรมสังคม ซึ่งไม่ได้การลงทุนไปกับเทคโนโลยีการรักษาความปลอดภัยระบบสารสนเทศชั้นสูง แต่หมายถึงการป้องกันปัญหาที่เกิดขึ้นกับคน (Bevis, J., 2007) และสอดคล้องกับงานวิจัยของ อัญรัตน์ จันทร์เจริญสุข ได้ทำการศึกษาวิจัยเรื่อง เทคนิคการจารกรรมข้อมูลสารสนเทศผ่านทางกระบวนการทางสังคม กรณีศึกษา ธนาคารพาณิชย์แห่งหนึ่ง วิธีในการรับมือและป้องกันการจารกรรมข้อมูลสารสนเทศผ่านกระบวนการทางสังคม (Social Engineering) นั้น พบว่า การมีกระบวนการหรือระเบียบวิธีในการปฏิบัติงานที่มีประสิทธิภาพและรัดกุมควบคู่กับการสร้างความตระหนักรู้เรื่องความปลอดภัยของข้อมูลสารสนเทศให้กับบุคลากรในองค์กรนั้นเป็นวิธีในการรับมือและป้องกันการจารกรรมข้อมูลสารสนเทศผ่านกระบวนการทางสังคมที่มีประสิทธิภาพมากที่สุด (อัญรัตน์ จันทร์เจริญสุข, 2552)

3. จากการศึกษาข้อเสนอแนะ เพื่อให้แนวทางการดำเนินงานและมาตรการที่เหมาะสมกับการจัดการความมั่นคงปลอดภัยสารสนเทศ ได้นำเสนอแนวทางการดำเนินการและมาตรการของรัฐ เพื่อรองรับปัญหาต่าง ๆ ดังนี้

ปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ สามารถสรุปเป็นปัญหาในระดับชาติได้ 2 ด้าน คือ ปัญหาด้านความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์และความพร้อมในการรับมือต่อการสูญเสียอธิปไตยไซเบอร์ของชาติ ซึ่งมีข้อเสนอแนะ แนวทางในการแก้ปัญหาต่อภาครัฐ ดังนี้ 1) การสร้างความตระหนักรู้ในเรื่องการใช้ชีวิตในโลกไซเบอร์อย่างปลอดภัย 2) การสร้างระบบการศึกษาด้านความมั่นคงปลอดภัยไซเบอร์ 3) การพัฒนากฎหมายและกฎระเบียบที่เกี่ยวข้อง เร่งรัดการบังคับใช้กฎหมาย โดยการออกกฎหมายลูก และประกาศมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล 4) ส่งเสริมการสร้างความร่วมมือขององค์กรทั้งภายในประเทศและต่างประเทศ 5) สนับสนุนและส่งเสริมให้มีการแข่งขันในการพัฒนาแอปพลิเคชันและแพลตฟอร์มระดับประเทศ สอดคล้องกับงานวิจัยของ หยาดพิรุณ นาชัยสินธุ์ ได้ทำการศึกษาวิจัยเรื่อง ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย ได้นำเสนอยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย ในด้านต่าง ๆ เช่น 1) การเสริมสร้างการวิจัยเพื่อการพัฒนาทางไซเบอร์ 2) การจัดการศึกษาในการสร้างพื้นฐานของประชาชนในประเทศไทย 3) ยุทธศาสตร์การสร้างการตระหนักรู้ทางไซเบอร์ให้กับประชาชน 4) ยุทธศาสตร์การส่งเสริมความร่วมมือระหว่างภาครัฐ ภาคเอกชน และภาคประชาชน 5) ยุทธศาสตร์การกำหนดใช้กฎหมายทางไซเบอร์และการบังคับใช้กับประชาชน (หยาดพิรุณ นาชัยสินธุ์, 2559)

นอกเหนือจากการนำเสนอข้อเสนอแนะ แนวทางการดำเนินการและมาตรการของรัฐ ผู้วิจัยได้นำเสนอแนวทางการเตรียมองค์กรสำหรับ พ.ร.บ.การรักษาความมั่นคงไซเบอร์และ พ.ร.บ คุ้มครองข้อมูลส่วนบุคคล และแนวคิดที่สำคัญ คือ ความมั่นคงปลอดภัยไซเบอร์เป็นพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคล ไม่สามารถแยกออกจากกันได้ และเมื่อพูดถึงความปลอดภัยของข้อมูล เราต้องคำนึงถึงองค์ประกอบพื้นฐาน 3 ประการ คือ 1) การรักษาความลับของข้อมูล (Confidentiality) 2) การรักษาความสมบูรณ์ของข้อมูล (Integrity) และ 3) ความพร้อมใช้งานของข้อมูล (Availability) และแนวคิดที่สำคัญ คือ ความปกติแบบใหม่ (The New Normal) ที่เกิดขึ้นบนโลกไซเบอร์ ซึ่งองค์กรต้องเปลี่ยนความคิดใหม่ในการวางมาตรการให้รองรับกับภัยไซเบอร์ที่องค์กรอาจจะถูกคกุคามอย่างเลี่ยงไม่ได้ เพียงแต่ว่าจะเกิดขึ้นเมื่อใด ดังนั้นองค์กรต้องเตรียมพร้อมและบริหารจัดการความเสี่ยงที่จะเกิดนี้ ซึ่งข้อเสนอแนะ แนวทางการดำเนินการและแนวคิดดังกล่าว สามารถนำไปประยุกต์ใช้สถาบันการเงิน และองค์กรอื่น ๆ ได้

สรุป/ข้อเสนอแนะ

กล่าวโดยสรุปได้ว่า ปัจจุบันการทำธุรกรรมทางการเงินของธนาคารพาณิชย์นั้น ได้ถูกขับเคลื่อนด้วยระบบดิจิทัลแบงกิ้ง (Digital banking) แต่สิ่งที่มาพร้อมกับเทคโนโลยี คือ ภัยคุกคามทางไซเบอร์ ที่เพิ่มขึ้นอย่างรวดเร็วและมีความซับซ้อนมากขึ้น ส่งผลกระทบต่อทุกภาคส่วน จนเป็นปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ที่สำคัญระดับชาติ ในด้านความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์และความพร้อมในการรับมือต่อการสูญเสียอธิปไตยไซเบอร์ของชาติ และจากมาตรการกำกับดูแลของรัฐ การดำเนินการและมาตรการต่าง ๆ ของธนาคารพาณิช์ ในการรองรับปัญหาดังกล่าว ผู้วิจัยเห็นว่าควรมีข้อเสนอแนะที่เป็นนัยยะในเชิงนโยบายที่สำคัญ ดังนี้ 1) รัฐควรเร่งรัดการบังคับใช้ พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ และ พ.ร.บ. การคุ้มครองข้อมูลส่วนบุคคล โดยการออกกฎหมายลูกและประกาศกฎเกณฑ์ต่าง ๆ เพื่อให้การดำเนินการมีความสอดคล้องและเป็นไปในทิศทางเดียว 2) ธนาคารควรส่งเสริมให้ความรู้และตะหนักถึงภัยคุกคามไซเบอร์ และภัยคุกคามทางการเงินในการทำธุรกรรมการเงินทางอิเล็กทรอนิกส์ให้กับประชาชนและลูกค้าของธนาคารให้มากขึ้น 3) ภาคประชาชนควรจะเรียนรู้และตะหนักถึงภัยคุกคามไซเบอร์ ภัยคุกคามทางการเงินในการทำธุรกรรมการเงินทางอิเล็กทรอนิกส์ และจากผลการศึกษาที่ได้ ผู้วิจัยหวังว่าจะเป็นประโยชย์ต่อทุกภาคส่วน สามารถนำไปใช้ในการวางนโยบายและแนวทางปฏิบัติในการจัดการความมั่นคงของเทคโนโลยีสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล ในการทำธุรกรรมทางอิเล็กทรอนิกส์ของสถาบันการเงินอื่น ๆ และสามารถนำไปใช้ในการรับมือกับภัยคุกคามทางการเงินในการทำธุรกรรมการเงินทางอิเล็กทรอนิกส์ได้ สำหรับข้อเสนอแนะในการวิจัยครั้งต่อไป ผู้วิจัยมีความเห็นว่าจะเป็นประโยชน์อย่างมาก หากมีการศึกษาวิจัยเพิ่มเติมในส่วนของหน่วยงานกำกับดูแล

ธนาคารพาณิชย์อื่น ๆ ที่นอกเหนือจากการวิจัยในครั้งนี้ เช่น สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เพื่อให้ครอบคลุมธุรกิจของธนาคาร และควรศึกษาหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศให้ครอบคลุมทุกประเภท เนื่องจากภัยคุกคามไซเบอร์สำหรับธุรกิจแต่ละประเภทอาจจะมีปัญหาและผลกระทบที่แตกต่างกัน

เอกสารอ้างอิง

กิตติ โฆษะวิสุทธิ์. (23 กันยายน 2563). ปัญหาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ภาคการธนาคาร. (กริน ธัญญวิกรม, ผู้สัมภาษณ์)

เทอดพงษ์ เปล่งศิริวัฒน์. (2558). Cyber Attack ภัยคุกคามของสถาบันการเงินไทยในยุคดิจิทัล. เรียกใช้เมื่อ 25 กันยายน 2562 จาก https://www.bot.or.th/Thai/ResearchAndPublications/DocLib_/Article17_12_58.pdf

นคร เสรีรักษ์. (2548). การคุ้มครองข้อมูลส่วนบุคคล: ข้อเสนอเพื่อการพัฒนาสิทธิรับรู้ข้อมูลข่าวสารในกระบวนการธรรมรัฐไทย. ใน วิทยานิพนธ์ปรัชญาดุษฎีบัณฑิต สาขาสหวิทยาการ. มหาวิทยาลัยธรรมศาสตร์.

ปริญญา หอมเอนก. (25 กันยายน 2563). การรักษาอธิปไตยไซเบอร์ของชาติ และการเตรียมองค์กรสำหรับ พ.ร.บ.ไซเบอร์และ พ.ร.บ คุ้มครองข้อมูลส่วนบุคคล. (กริน ธัญญวิกรม, ผู้สัมภาษณ์)

ศุภโชค จันทรประทิน. (17 กันยายน 2563). ผลการจัดอันดับดัชนีชี้วัดของการพัฒนาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย. (กริน ธัญญวิกรม, ผู้สัมภาษณ์)

สำนักงานรัฐบาลอิเล็กทรอนิกส์. (2559). แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม. (พิมพ์ครั้งที่ 1). กรุงเทพมหานคร: ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา.

หยาดพิรุณ นาชัยสินธุ์. (2559). ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย. ใน ดุษฎีนิพนธ์รัฐศาสตรดุษฎีบัณฑิต สาขายุทธศาสตร์และความมั่นคง. มหาวิทยาลัยบูรพา.

อัญรัตน์ จันทร์เจริญสุข. (2552). เทคนิคการจารกรรมข้อมูลสารสนเทศผ่านทางกระบวนการทางสังคม กรณีศึกษา ธนาคารพาณิชย์แห่งหนึ่ง. ใน สารนิพนธ์วิทยาศาสตรมหาบัณฑิต สาขาวิชาการบริหารเทคโนโลยี วิทยาลัยนวัตกรรม. มหาวิทยาลัยธรรมศาสตร์.

Bevis, J. (2007). xtreme Social Engineering-combating the Insider Security Threat-A Security Awareness Exercise. Retrieved June 26, 2017, fromhttps://jtbevis. files.wordpress.com /2007/09/article-social-eng-v-7921.pdf

Azuwa, M.P. et al. (2012). Technical Security Metrics Model in Compliance with ISO/IEC 27001 Standard. International Journal of Cyber-Security and Digital Forensics (IJCSDF), 1(4), 280-288.

Manar Abu et al. (2012). Guide to ISO 27001: UAE Case Study. Informing Science and Information Technology, 7(1), 331-347.

Stephen Lineberry. (2007). The Human Element The weakest Linkin information Security Online Magazine Journal of Accountancy. Retrieved June 26, 2017, from http://www.journalofaccountancy.com/issues/2007/nov/

World Economic Forum. (2020). Global risk security reports 2020. Retrieved November 1, 2020, from https://www.weforum.org/reports/the-global-risks-report-2020