การบริหารจัดการความมั่นคงทางเทคโนโลยีสารสนเทศ: กรณีศึกษา การคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย
Information Technology Security Management: A Case Study of Personal Data Protection in Electronic Transactions of Thai Commercial Banks

ธวัช ไทรราหู[1], วันวสา วิโรจนารมย์[2*], กอบลาภ อารีศรีสม[3] และภาวิณี อารีศรีสม[4]
Thawat Sairahu[1], Wanwasa Wirojanarome[2*], Koblap Areesrisom[3] and Pawinee Areesrisom[4]
สาขาการจัดการและพัฒนาทรัพยากร คณะผลิตกรรมการเกษตร มหาวิทยาลัยแม่โจ้ จังหวัดเชียงใหม่
Division of Resources Management and Development, Faculty of Agricultural Production, Maejo University, Chiangmai, Thailand
*Corresponding Author E-mail: wanwasa.wi@hotmail.com
Received: 2025-6-27; **Revised:** 2025-10-10; **Accepted:** 2025-10-25

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์ เพื่อศึกษา 1. ปัจจัยที่มีอิทธิพลต่อความมั่นคงทางเทคโนโลยีสารสนเทศ และ 2. แนวทางการดำเนินงานและมาตรการที่เหมาะสมกับการจัดการความมั่นคงทางเทคโนโลยีสารสนเทศเพื่อการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย การวิจัยนี้ใช้วิธีการวิจัยแบบผสมผสาน โดยการสุ่มตัวอย่างแบบง่าย เครื่องมือการวิจัย คือ การวิเคราะห์ข้อมูล ใช้แบบจำลองสมการโครงสร้าง และการวิเคราะห์เนื้อหา

ผลการวิจัยพบว่า 1. การบริหารจัดการเทคโนโลยีสารสนเทศ มีอิทธิพลโดยรวมต่อความมั่นคงทางเทคโนโลยีสารสนเทศ มากที่สุด รองลงมาคือ บทบาทของธนาคารพาณิชย์ บทบาทภาครัฐ และบทบาทภาคประชาชน ตามลำดับ และ 2. แนวทางการจัดการความมั่นคงทางเทคโนโลยีสารสนเทศเพื่อคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทยประกอบด้วย (1) การกำหนดนโยบายและโครงสร้างการกำกับดูแล (2) การประเมินและจัดการความเสี่ยง (3) การควบคุมการเข้าถึงและการพิสูจน์ตัวตน (4) การเข้ารหัสข้อมูลและการจัดการกุญแจเข้ารหัส (5) การรักษาความมั่นคงปลอดภัยของเครือข่ายและระบบ (6) การพัฒนาระบบงานที่มั่นคงปลอดภัย (7) การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (8) การบริหารความต่อเนื่องทางธุรกิจ (9) การบริหารจัดการผู้ให้บริการภายนอก (10) การสร้างความตระหนักรู้และการฝึกอบรม (11) การปฏิบัติตามกฎหมายและมาตรฐานสากล (12) การตรวจสอบและประเมินประสิทธิผล (13) การบริหารจัดการทรัพย์สินสารสนเทศ (14) การรักษาความมั่นคงปลอดภัยทางกายภาพ (15) การบริหารจัดการข้อมูลส่วนบุคคล และ (16) การเฝ้าระวังภัยคุกคามใหม่

คำสำคัญ: ความมั่นคงทางเทคโนโลยีสารสนเทศ, ธนาคารพาณิชย์, ข้อมูลส่วนบุคคล

Abstract

This research aims to study 1. factors influencing information technology security, and 2. appropriate operational guidelines and measures for managing information technology security to protect personal data in electronic transactions of Thai commercial banks. This

research employed a mixed-methods approach using simple random sampling. The research instruments included data analysis using structural equation modeling and content analysis.

The research findings revealed that 1. information technology management had the greatest overall influence on information technology security, followed by the role of commercial banks, the role of government, and the role of citizens, respectively, and 2. the guidelines for managing information technology security to protect personal data in electronic transactions of Thai commercial banks consist of (1) policy formulation and governance structure (2) risk assessment and management (3) access control and authentication (4) data encryption and encryption key management (5) network and system security (6) secure system development (7) security incident management (8) business continuity management (9) external service provider management (10) awareness raising and training (11) compliance with laws and international standards (12) auditing and effectiveness evaluation (13) information asset management (14) physical security (15) personal data management, and (16) monitoring emerging threats.

Keywords: Information Technology Security, Commercial Bank, Personal Data

บทนำ

การเข้าใช้บริการข้อมูลสารสนเทศ จำเป็นต้องมีความมั่นคงปลอดภัยไซเบอร์ในระดับสูงเพื่อคุ้มครองประชาชนหรือประโยชน์ที่สำคัญของประเทศ ภาครัฐซึ่งมีหน้าที่กำกับดูแลและมีภารกิจในการคุ้มครองประชาชนผู้บริโภคด้านระบบบริการทางธุรกรรมทางการเงิน ส่งเสริมผู้ประกอบการด้านธุรกรรมทางการเงินซึ่งคือ ธนาคารพาณิชย์ ส่งเสริมการพัฒนานวัตกรรมดิจิทัล (Digital Innovation) รวมทั้งเป็นหน่วยงานควบคุมกำกับมาตรฐานระบบ ความมั่นคงปลอดภัยไซเบอร์ ดังนั้น เพื่อความเชื่อมั่นและมีความมั่นคงปลอดภัยด้านข้อมูล สารสนเทศ รวมทั้งส่งเสริมการทำธุรกรรมอิเล็กทรอนิกส์ด้านการเงิน ในการติดตาม ควบคุมกำกับความมั่นคงปลอดภัย (Enterprise Risk Management) ของระบบสารสนเทศ ที่กำหนดให้กรมสนับสนุนบริการสุขภาพผ่านเกณฑ์ ประเมินมาตรฐานความมั่นคงปลอดภัยสารสนเทศรวมทั้งเป็นการดำเนินงานตามพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ที่ประกาศในราชกิจจานุเบกษา เมื่อวันที่ 27 พฤษภาคม พ.ศ. 2562 แล้วนั้น เป็นการเพิ่มขีดความสามารถในการแข่งขัน การพัฒนาเศรษฐกิจดิจิทัลในการขับเคลื่อนยุทธศาสตร์ชาติอันเป็นนโยบายสำคัญเร่งด่วนของรัฐบาลและเพิ่ม รายได้สู่ประเทศตามนโยบายก้าวสู่เศรษฐกิจดิจิทัล (พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562)

ปัจจุบันธนาคารในประเทศไทยได้นำเทคโนโลยีดิจิทัลมาใช้มากขึ้นในการทำธุรกรรมทางการเงิน โดยเฉพาะระบบการชำระเงินถือว่าเป็นส่วนหนึ่งที่ประยุกต์เทคโนโลยีเข้ามาตอบสนองความต้องการของลูกค้าในรูปแบบดิจิทัลแบงก์กิ้ง (Digital banking) การให้บริการลูกค้าในการทำธุรกรรมกับธนาคาร โดยลูกค้าไม่จำเป็นต้องเดินทางมาธนาคาร เช่น การให้บริการทางโทรศัพท์ (Call Center) การทำธุรกรรมทางการเงินผ่านช่องทางตู้เอทีเอ็ม อินเทอร์เน็ตแบงก์กิ้ง (Internet Banking) และโมบายแบงก์กิ้ง (Mobile Banking) เป็นต้น การนำระบบดิจิทัลแบงก์กิ้งมาใช้ช่วยให้การทำธุรกรรมการเงินและการชำระเงินเป็นไปด้วยความสะดวกรวดเร็ว มีต้นทุนถูกลงและสามารถเข้าถึงบริการได้ง่ายขึ้นในทุกที่ทุกเวลาและทุกอุปกรณ์ (Anytime Anywhere Any device) (เทอดพงษ์ เปล่งศิริวัฒน์, 2558) แต่สิ่งที่มาพร้อมกับเทคโนโลยี คือ ภัยคุกคามทางไซเบอร์ (Cyber Threat) ที่ปัจจุบันเพิ่มขึ้นอย่างรวดเร็วหลายรูปแบบและมีความซับซ้อนมากขึ้น ส่งผลเสียหายต่อสถาบันการเงินและผู้ใช้บริการ ปัญหาภัยคุกคามทางไซเบอร์ในปัจจุบันเพิ่มขึ้นอย่างรวดเร็วและมี

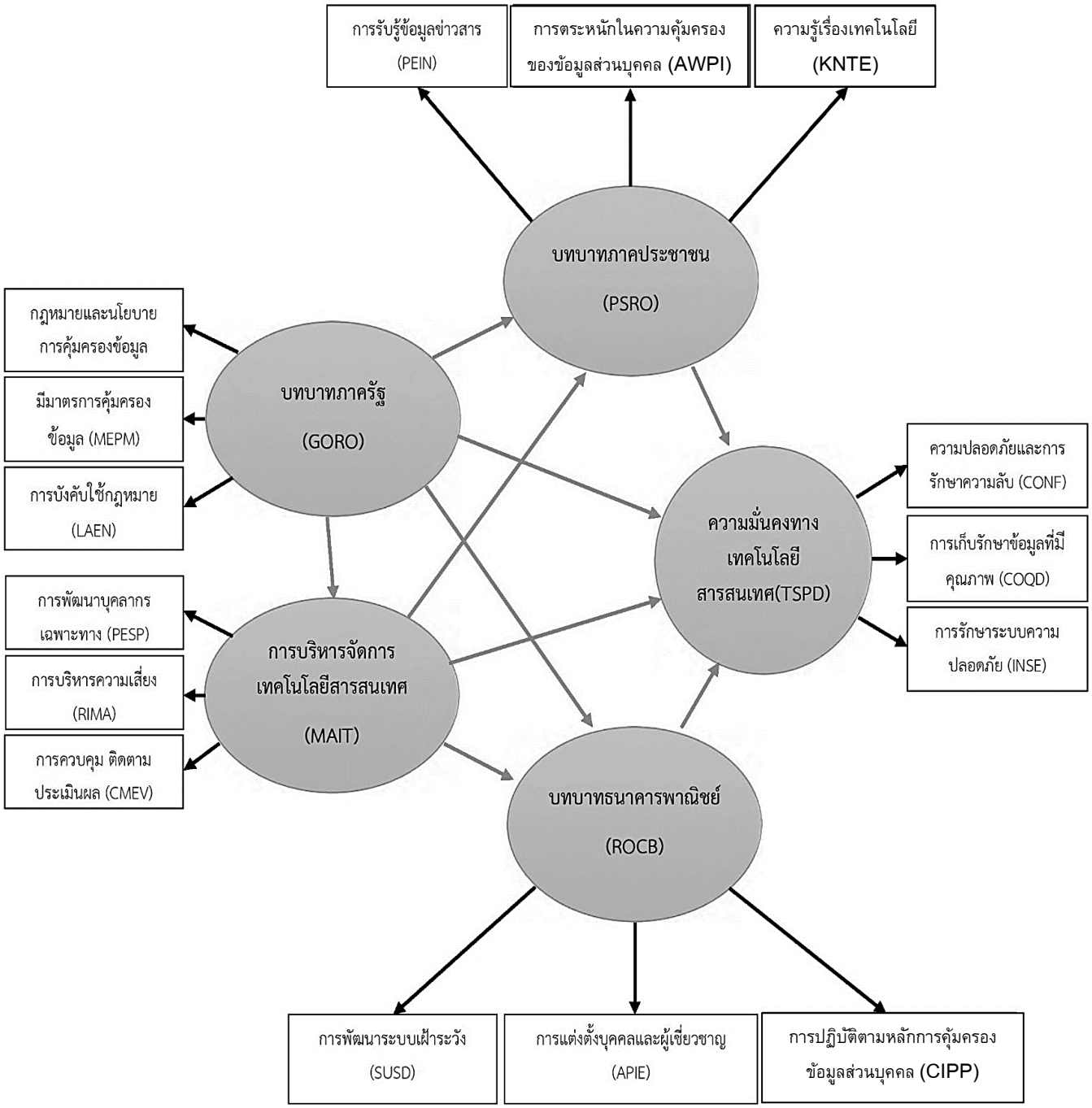
ความซับซ้อนมากขึ้น สำหรับสถานการณ์ภัยคุกคามทางไซเบอร์ของโลก World Economic Forum (2020) ได้จัดทำ Global risk security reports 2020 ขึ้น ได้จัดให้ปัญหาภัยคุกคามทางไซเบอร์และการขโมยข้อมูลส่วนบุคคลมีความเสี่ยงที่สูง เป็น 1 ใน 10 ความเสี่ยงของโลกติดต่อกันมาหลายปี (World Economic Forum, 2020) ส่วนสถานการณ์ภัยคุกคามทางไซเบอร์ที่พบในประเทศไทยได้มุ่งเป้าไปยังหลายภาคส่วน โดยพบภัยคุกคามไซเบอร์ที่มีจุดประสงค์ทางการเงินในรูปแบบต่าง ๆ เช่น ฟิชชิ่งอีเมลหรือ เว็บไซต์ธนาคารปลอมเพื่อหลอกขโมยรหัสผ่านผู้ที่ใช้งานอิเล็กทรอนิกส์แบงก์กิ้ง (E-banking) การแพร่ระบาดของมัลแวร์เรียกค่าไถ่ (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 ด้วยความจำเป็นและความสำคัญดังกล่าวทำให้ธนาคารจำเป็นต้องทบทวนและปรับปรุงนโยบายทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศของตนโดยอาจจะอ้างอิงมาจากมาตรฐานที่เกี่ยวข้องกับความมั่นคงปลอดภัยของข้อมูลสารสนเทศในปัจจุบันซึ่งมีหลายมาตรฐานและเป็นที่ยอมรับว่าเป็นมาตรฐานที่มีความน่าเชื่อถือ เช่น มาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001) ที่เป็นที่ยอมรับในระดับสากล เข้ามาประยุกต์ใช้ในกระบวนการปฏิบัติงานในการให้บริการขององค์กร เพื่อให้องค์กรเกิดความมั่นคงปลอดภัยและเป็นการสร้างมาตรฐานให้ตัวองค์กรเอง ซึ่งจะช่วยให้องค์กรสามารถเตรียมพร้อมรับมือกับภัยคุกคามได้อย่างมีประสิทธิภาพ ดังนั้นการจัดการความมั่นคงทางเทคโนโลยีจึงมีความสำคัญ เนื่องจากรัฐบาลมีการจัดทำแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมขึ้นเพื่อการสร้างระบบเศรษฐกิจและสังคมดิจิทัลและปัจจุบันธนาคารได้นำเทคโนโลยีดิจิทัลมาใช้มากขึ้นในการทำธุรกรรมทางการเงิน โดยเฉพาะระบบชำระเงิน แต่สิ่งที่มาพร้อมกับเทคโนโลยี คือ ภัยคุกคามทางไซเบอร์ (Cyber Threat) ที่ปัจจุบันเพิ่มขึ้นอย่างรวดเร็ว หลายรูปแบบและมีความซับซ้อนมากขึ้น ส่งผลเสียหายต่อสถาบันการเงินและผู้ใช้บริการการจัดการความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแล กิจการที่ดี โดยจะช่วยให้การบริหารงานและการตัดสินใจด้านต่าง ๆ เช่น การวางแผน การกำหนด กลยุทธ์ การติดตามควบคุมและวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่าง ๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่ องค์กร เทคโนโลยีสารสนเทศมีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กร ทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์ คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และ วิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่าง ๆ ภายใต้สภาวะการดำเนินงานของทุก ๆ องค์กร ล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมาย ขององค์กร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยง ว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร วิเคราะห์ความเสี่ยง จากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนดแนวทางใน การจัดการความเสี่ยง โดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

จากข้อมูลและสถานการณ์ข้างต้น ผู้วิจัยมีความสนใจศึกษาเรื่อง การบริหารจัดการความมั่นคงทางเทคโนโลยีสารสนเทศ กรณีศึกษา การคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย เพื่อให้ข้อเสนอแนะ แนวทางการดำเนินงานและมาตรการที่เหมาะสมในการจัดการความมั่นคงของเทคโนโลยีสารสนเทศ เพื่อการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาปัจจัยที่มีอิทธิพลต่อความมั่นคงทางเทคโนโลยีสารสนเทศ
2. เพื่อศึกษาแนวทางการดำเนินงานและมาตรการที่เหมาะสมกับการจัดการความมั่นคงทางเทคโนโลยีสารสนเทศเพื่อการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย

กรอบแนวคิดการวิจัย



ภาพที่ 1 กรอบแนวคิดการวิจัย

วิธีดำเนินการวิจัย

การวิจัยนี้ใช้วิธีการวิจัยแบบผสม ระหว่างการวิจัยเชิงปริมาณและการวิจัยเชิงคุณภาพ

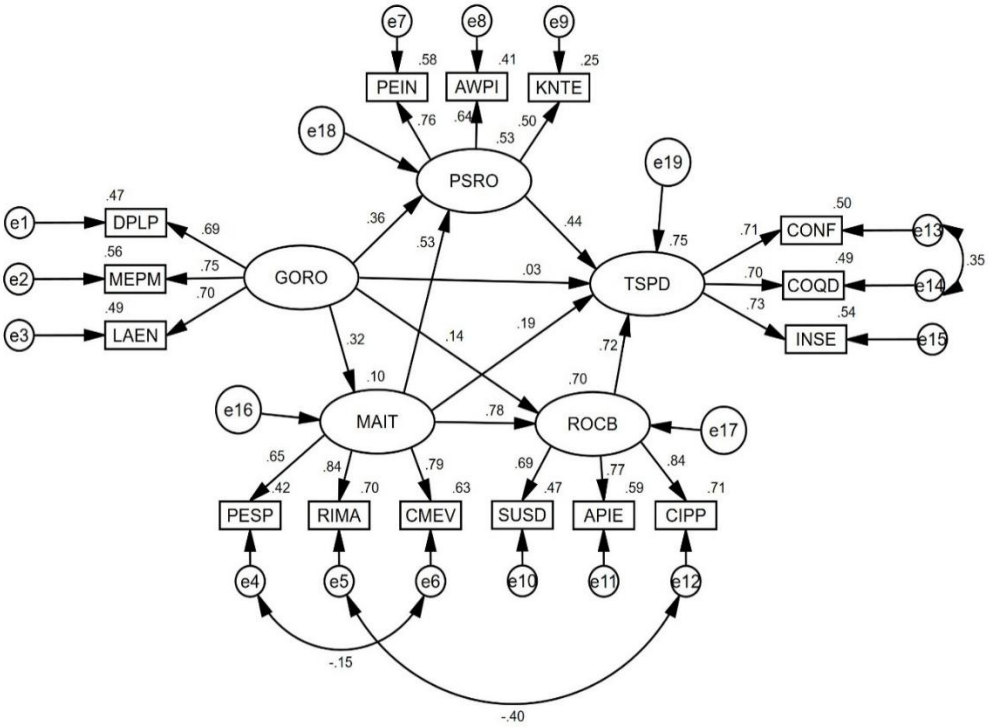
ประชากรในการวิจัยเชิงปริมาณ คือ เจ้าหน้าที่ธนาคารพาณิชย์ไทยที่เกี่ยวข้องกับการทำธุรกรรมทางอิเล็กทรอนิกส์ ในกรุงเทพมหานคร สำหรับการพิจารณาจำนวนที่เหมาะสมของกลุ่มตัวอย่างที่ใช้ในการวิจัยครั้งนี้ ผู้วิจัยได้ทำการพิจารณาถึงขนาดของกลุ่มตัวอย่างที่มีความเหมาะสมกับการวิเคราะห์ข้อมูลด้วยเทคนิคการวิเคราะห์โมเดลสมการโครงสร้าง (Structural Equation Modeling: SEM) ซึ่งผู้วิจัยใช้วิธีการกำหนดขนาดตัวอย่างตาม Comrey & Lee (1992) ได้แนะนำว่าขนาดของตัวอย่างที่ใช้ใน การวิจัยควรมีขนาดตัวอย่าง 10-20 เท่าของจำนวนตัวแปรสังเกตในงานวิจัยนั้น ๆ ซึ่งการวิจัยใน ครั้งนี้ ผู้วิจัยมีตัวแปรสังเกตจำนวน 15 ตัวแปร ขนาดตัวอย่างที่เหมาะสมและเพียงพอจึงควรมี อย่างน้อย 20 เท่า x 15 ตัวแปรสังเกต เท่ากับ 300 ตัวอย่าง ซึ่งจากผลการคำนวณเป็นขนาดของกลุ่มตัวอย่างขั้นต่ำที่สามารถนำมาใช้ในการวิเคราะห์ด้วยเทคนิคการวิเคราะห์โมเดลสมการโครงสร้าง ดังนั้น การวิจัยในครั้งนี้มีจำนวนกลุ่มตัวอย่าง 400 ตัวอย่าง ซึ่งมีจำนวนเพียงพอและมากกว่า ขนาดของกลุ่มตัวอย่างขั้นต่ำที่สามารถนำมาใช้ในการวิเคราะห์ด้วยเทคนิคการวิเคราะห์โมเดล สมการโครงสร้าง

วิธีการสุ่มแบบโควต้า เก็บข้อมูลด้วยแบบสอบถาม ผ่านการตรวจสอบความเที่ยงตรงตามเนื้อหา (content validity) มีค่า IOC ตั้งแต่ 0.80-1.00 ความเชื่อถือได้ของมาตรวัด พบว่า สัมประสิทธิ์ความเชื่อถือได้ (Cronbach’s alpha) ของมาตรวัดตัวแปรสังเกตที่ใช้ในการวิจัยครั้งนี้ มีค่าระหว่าง 0.804 ถึง 0.959 และทั้งฉบับมีค่าเท่ากับ 0.907 และวิเคราะห์ด้วยแบบจำลองสมการโครงสร้าง

การวิจัยเชิงคุณภาพ แบ่งการศึกษาเป็น 2 กลุ่ม คือ 1. กลุ่มผู้ให้ข้อมูลสำคัญ (Key Informant) จะเป็นผู้บริหารของหน่วยงานที่เกี่ยวข้องโดยตรงในการกำหนดนโยบายกำกับดูแลของภาครัฐและผู้เชี่ยวชาญ ได้แก่ 1) ผู้แทนปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม 2) ผู้บริหารและผู้เชี่ยวชาญของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) 3) สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ 4) สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล 5) ผู้บริหารธนาคารแห่งประเทศไทย 6) กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี 7) ผู้บริหารศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (TB-CERT) และ 8) ผู้แทนสมาคมความมั่นคงระบบสารสนเทศแห่งประเทศไทย รวม 8 คน กลุ่มที่ 2 เป็นการจัดสนทนากลุ่ม (Focus Group) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ของธนาคารพาณิชย์ไทย จำนวน 10 ท่าน เจ้าหน้าที่จากสมาคมธนาคารไทยจำนวน 4 คน จากธนาคารแห่งประเทศไทยจำนวน 2 คน เจ้าหน้าที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม 6 คน และประชาชนซึ่งเป็นลูกค้าธนาคาร ซึ่งไม่ใช่กลุ่มตัวอย่าง 8 คน รวมทั้งสิ้น 30 คน เครื่องมือ คือ แบบสัมภาษณ์แบบกึ่งโครงสร้าง และแบบบันทึกการสนทนากลุ่มวิเคราะห์ผลด้วยการวิเคราะห์เนื้อหา

ผลการวิจัย

ปัจจัยที่มีอิทธิพลต่อความมั่นคงทางเทคโนโลยีสารสนเทศ



Chi-square = 123.300, df = 78, Chi-square/df = 1.581, GFI = 0.949, AGFI= 0.921,
CFI = 0.974, RMR = 0.009, RMSEA = 0.044

ภาพที่ 2 แบบจำลองสมการโครงสร้างรูปแบบสัมประสิทธิ์ปรับมาตรฐาน

ผลการวิเคราะห์แบบจำลองสมการโครงสร้าง นำมาเสนอค่าอิทธิพลทางตรง และทางอ้อม และผลรวมของตัวแปรแฝงทุกตัว เพื่อแสดงอิทธิพลทางตรง และทางอ้อมระหว่างตัวแปรที่ศึกษา ดังตาราง 1

ตาราง 1 อิทธิพลรวม อิทธิพลทางตรง และอิทธิพลทางอ้อม

ตัวแปรตาม	อิทธิพล	ตัวแปรอิสระ				R^2
		GORO	MAIT	ROCB	PSRO	
MAIT	DE	0.32	-	-	-	0.10
	IE	-	-	-	-	
	TE	0.32	-	-	-	
ROCB	DE	0.14	0.78	-	-	0.70
	IE	0.25	-	-	-	
	TE	0.39	0.78	-	-	
PSRO	DE	0.36	0.53	-	-	0.53
	IE	0.17	-	-	-	
	TE	0.53	0.53	-	-	
TSPD	DE	-	-	0.72	0.42	0.75
	IE	0.44	0.79	-	-	
	TE	0.44	0.79	0.72	0.42	

ตัวแปรตาม	อิทธิพล	ตัวแปรอิสระ				R^2
		GORO	MAIT	ROCB	PSRO	
Chi-square = 123.300, df = 78, Chi-square/df = 1.581, GFI = 0.949, AGFI= 0.921, CFI = 0.974, RMR = 0.009, RMSEA = 0.044						

จากตาราง 1 พบว่า ความมั่นคงทางเทคโนโลยีสารสนเทศ (TSPD) ได้รับอิทธิพลทางตรงจาก บทบาทของธนาคารพาณิชย์ (ROCB) มากที่สุด มีขนาดอิทธิพลเท่ากับ 0.72 รองลงมาคือ บทบาทภาคประชาชน (PSRO) มีขนาดอิทธิพลเท่ากับ 0.42 ตามลำดับ

อิทธิพลทางอ้อมพบว่า ความมั่นคงทางเทคโนโลยีสารสนเทศ (TSPD) ได้รับอิทธิพลทางอ้อมจาก การบริหารจัดการเทคโนโลยีสารสนเทศ (MAIT) มากที่สุด มีขนาดอิทธิพลเท่ากับ 0.79 รองลงมาคือ บทบาทภาครัฐ (GORO) มีขนาดอิทธิพลเท่ากับ 0.44 ตามลำดับ

เมื่อพิจารณาอิทธิพลรวม พบว่า การบริหารจัดการเทคโนโลยีสารสนเทศ (MAIT) มีอิทธิพลโดยรวมต่อความมั่นคงทางเทคโนโลยีสารสนเทศ (TSPD) มากที่สุด มีขนาดอิทธิพลเท่ากับ 0.79 รองลงมาคือ บทบาทของธนาคารพาณิชย์ (ROCB) มีขนาดอิทธิพลเท่ากับ 0.72 บทบาทภาครัฐ (GORO) มีขนาดอิทธิพลเท่ากับ 0.44 และบทบาทภาคประชาชน (PSRO) มีขนาดอิทธิพลเท่ากับ 0.42 ตามลำดับ

แนวทางการดำเนินงานและมาตรการที่เหมาะสมกับการจัดการความมั่นคงทางเทคโนโลยีสารสนเทศเพื่อการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย

ผลการวิจัยในส่วนนี้ ได้มาจากการเก็บรวบรวมขอมูลเชิงคุณภาพ จากการสัมภาษณ์เชิงลึก (In-Depth Interview) กับผู้ให้ข้อมูลสำคัญ และจากสนทนากลุ่ม (Focus Group) แนวทางการดำเนินงานและมาตรการที่เหมาะสมกับการจัดการความมั่นคงทางเทคโนโลยีสารสนเทศเพื่อการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย สรุปสาระสำคัญได้ดังนี้

1. การกำหนดนโยบายและโครงสร้างการกำกับดูแล: กำหนดนโยบายรักษาความมั่นคงปลอดภัยสารสนเทศที่ชัดเจน ได้รับการอนุมัติจากคณะกรรมการธนาคาร และมีการทบทวนสม่ำเสมอ พร้อมจัดตั้งคณะกรรมการความมั่นคงปลอดภัยที่มีผู้บริหารระดับสูงกำกับดูแล

2. การประเมินและจัดการความเสี่ยง: ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยครอบคลุมทั้งระบบงานและข้อมูลสำคัญ โดยพิจารณาทั้งปัจจัยภายในและภายนอก พร้อมจัดทำแผนบริหารจัดการความเสี่ยงที่เหมาะสม

3. การควบคุมการเข้าถึงและการพิสูจน์ตัวตน: ใช้หลักการ "need-to-know" และ "least privilege" ควบคุมการเข้าถึงข้อมูลสำคัญ พร้อมใช้ Multi-factor Authentication และบริหารจัดการสิทธิ์อย่างเป็นระบบ

4. การเข้ารหัสข้อมูลและการจัดการกุญแจเข้ารหัส: ใช้เทคโนโลยีการเข้ารหัสมาตรฐานสากลสำหรับข้อมูลสำคัญ เช่น ข้อมูลบัตรเครดิต พร้อมกระบวนการจัดการกุญแจเข้ารหัสที่ปลอดภัย

5. การรักษาความมั่นคงปลอดภัยของเครือข่ายและระบบ: ใช้ระบบป้องกันการบุกรุกและมัลแวร์ที่ทันสมัย พร้อมการเฝ้าระวังความปลอดภัยอย่างต่อเนื่อง และการติดตั้งแพตช์ช่องโหว่ทันทีที่มี

6. การพัฒนาระบบงานที่มั่นคงปลอดภัย: ใช้แนวทาง Security by Design ตั้งแต่การออกแบบ พร้อมแยกสภาพแวดล้อมการพัฒนา ทดสอบ และใช้งานจริง

7. การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย: ตั้งศูนย์ปฏิบัติการความมั่นคงปลอดภัย (SOC) และมีแผนรับมือเหตุการณ์พร้อมการซักซ้อมอย่างสม่ำเสมอ

8. การบริหารความต่อเนื่องทางธุรกิจ: จัดทำแผนบริหารความต่อเนื่องและกำหนดเวลาหยุดชะงักที่ยอมรับได้ พร้อมทดสอบแผนการกู้คืนระบบและข้อมูล

9. การบริหารจัดการผู้ให้บริการภายนอก: ประเมินความเสี่ยงและควบคุมการเข้าถึงข้อมูลของผู้ให้บริการภายนอก พร้อมทำข้อตกลงรักษาความลับที่ชัดเจน

10. การสร้างความตระหนักรู้และการฝึกอบรม: จัดอบรมและสร้างความตระหนักรู้เรื่องความมั่นคงปลอดภัยให้พนักงานทุกระดับ พร้อมคู่มือและสื่อการเรียนรู้

11. การปฏิบัติตามกฎหมายและมาตรฐานสากล: ปฏิบัติตามกฎหมาย เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และมาตรฐานสากล เช่น ISO/IEC 27001

12. การตรวจสอบและประเมินประสิทธิผล: ดำเนินการตรวจสอบภายในด้านความมั่นคงปลอดภัยสม่ำเสมอ โดยรายงานผลต่อคณะกรรมการ และติดตามแก้ไขปัญหา

13. การบริหารจัดการทรัพย์สินสารสนเทศ: จัดทำทะเบียนทรัพย์สินสารสนเทศพร้อมกำหนดผู้รับผิดชอบ และมีมาตรการควบคุมการนำอุปกรณ์ออกนอกองค์กร

14. การรักษาความมั่นคงปลอดภัยทางกายภาพ: ควบคุมการเข้าออกและติดตั้งระบบเฝ้าระวังในพื้นที่สำคัญ เช่น ศูนย์คอมพิวเตอร์ และห้องเครือข่าย

15. การบริหารจัดการข้อมูลส่วนบุคคล: ปกป้องข้อมูลส่วนบุคคลโดยปฏิบัติตามกฎหมายและมาตรการความปลอดภัยในการจัดเก็บและประมวลผลข้อมูล

16. การเฝ้าระวังภัยคุกคามใหม่: ติดตามภัยคุกคามใหม่และปรับปรุงมาตรการความมั่นคงปลอดภัยให้ทันสมัยต่อเนื่อง

อภิปรายผล

1. ผลการวิจัยพบว่า การบริหารจัดการเทคโนโลยีสารสนเทศ มีอิทธิพลต่อความมั่นคงทางเทคโนโลยีสารสนเทศ ด้านการคุ้มครองข้อมูลส่วนบุคคลทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย เหตุเป็นเพราะเนื่องมาจากการจัดการเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพเป็นพื้นฐานสำคัญในการรักษาความปลอดภัยของข้อมูลในระบบธุรกรรมทางอิเล็กทรอนิกส์ การพัฒนาบุคลากรเฉพาะทางช่วยให้มีผู้เชี่ยวชาญที่สามารถดูแลและปรับปรุงระบบความปลอดภัยอย่างเหมาะสม ซึ่งสอดคล้องกับแนวคิดที่ว่า ความเชี่ยวชาญของบุคลากรในด้านเทคโนโลยีสารสนเทศเป็นหนึ่งในปัจจัยที่ช่วยลดความเสี่ยงจากการโจมตีทางไซเบอร์ได้อย่างมีนัยสำคัญ

นอกจากนี้ การบริหารความเสี่ยงในกระบวนการจัดการข้อมูลมีบทบาทสำคัญในการคาดการณ์และป้องกันปัญหาที่อาจเกิดขึ้นก่อนที่จะส่งผลกระทบต่อระบบ ซึ่งช่วยเสริมสร้างความปลอดภัยของข้อมูลและรักษาความต่อเนื่องของบริการ อีกทั้งการควบคุม ติดตาม และประเมินผลยังเป็นกระบวนการที่ช่วยให้สามารถปรับปรุงมาตรการความปลอดภัยได้อย่างต่อเนื่อง โดยอาศัยข้อมูลจากการตรวจสอบเพื่อแก้ไขช่องโหว่และเพิ่มประสิทธิภาพของมาตรการป้องกันความเสี่ยง

ดังนั้น การบริหารจัดการเทคโนโลยีสารสนเทศมีอิทธิพลต่อความมั่นคงด้านการคุ้มครองข้อมูลส่วนบุคคลจึงสะท้อนให้เห็นถึงความสำคัญของการวางกลยุทธ์บริหารทรัพยากรเทคโนโลยีและบุคลากรเพื่อให้ธนาคารสามารถป้องกันและจัดการภัยคุกคามได้อย่างมีประสิทธิภาพและทันต่อสถานการณ์ที่เปลี่ยนแปลงอย่างรวดเร็วในสภาพแวดล้อมทางดิจิทัล

จากผลการวิจัยที่พบว่าความมั่นคงทางเทคโนโลยีสารสนเทศด้านการคุ้มครองข้อมูลส่วนบุคคลในธนาคารพาณิชย์ไทยได้รับอิทธิพลจากการบริหารจัดการเทคโนโลยีสารสนเทศ สอดคล้องกับแนวคิดของทฤษฎีต่าง ๆ ที่มุ่งเน้นการจัดการความเสี่ยงและการพัฒนาบุคลากรเฉพาะทาง รวมถึงการควบคุม ติดตาม และประเมินผล เพื่อให้การรักษาความปลอดภัยข้อมูลเป็นไปอย่างมีประสิทธิภาพ เช่น ทฤษฎีการบริหารความเสี่ยง (Risk Management Theory) ของ Aven (2008) ระบุว่า การประเมินและบริหารความเสี่ยงเป็นกระบวนการที่

สำคัญในการป้องกันภัยคุกคามต่าง ๆ ซึ่งในกรณีนี้การบริหารความเสี่ยงช่วยให้ธนาคารสามารถรับมือกับภัยคุกคามทางไซเบอร์และความเสี่ยงจากการโจมตีทางเทคโนโลยีได้อย่างมีประสิทธิภาพ การประเมินและจัดการความเสี่ยงที่ดีจะช่วยสร้างความมั่นคงในระบบการคุ้มครองข้อมูลส่วนบุคคล สอดคล้องกับทฤษฎีการพัฒนาทรัพยากรมนุษย์ (Human Resource Development Theory) ของ Swanson & Holton (2009) ที่มุ่งเน้นการพัฒนาบุคลากรในด้านต่าง ๆ ให้มีทักษะเฉพาะทางและความเชี่ยวชาญสูงในการบริหารจัดการเทคโนโลยีสารสนเทศ ช่วยให้สามารถจัดการกับปัญหาความปลอดภัยข้อมูลในธนาคารได้อย่างมีประสิทธิภาพ การพัฒนาทักษะของบุคลากรเฉพาะทางจะเป็นส่วนสำคัญในการเสริมสร้างความมั่นคงของระบบเทคโนโลยีสารสนเทศ และสอดคล้องกับทฤษฎีการควบคุมภายใน (Internal Control Theory) ซึ่งอธิบายถึงการสร้างระบบควบคุมภายในที่มีประสิทธิภาพในการติดตามและประเมินผลการปฏิบัติงานทุกขั้นตอน (COSO, 2013) ทฤษฎีนี้สอดคล้องกับผลการวิจัยที่ระบุถึงการควบคุม ติดตาม และประเมินผลในการคุ้มครองข้อมูลส่วนบุคคล ซึ่งการประเมินและการปรับปรุงอย่างต่อเนื่องเป็นส่วนสำคัญในการรักษามาตรฐานความปลอดภัยและความเป็นส่วนตัวของข้อมูล

จากผลการวิจัยที่พบว่า การบริหารจัดการความมั่นคงทางเทคโนโลยีสารสนเทศ ที่เกี่ยวข้องกับการพัฒนาบุคลากรเฉพาะทาง การบริหารความเสี่ยง และการควบคุม ติดตาม และประเมินผลนั้นมีอิทธิพลต่อความมั่นคงของข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ในธนาคารพาณิชย์ไทย สอดคล้องกับงานวิจัยของ Peltier (2010) ที่ศึกษาการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศในองค์กร พบว่า การบริหารความเสี่ยงที่มีประสิทธิภาพช่วยลดภัยคุกคามและป้องกันไม่ให้ข้อมูลส่วนบุคคลของลูกค้าถูกเปิดเผยหรือสูญหาย โดยการประเมินความเสี่ยงและการดำเนินการป้องกันภัยคุกคามที่เหมาะสมทำให้ข้อมูลในระบบของธนาคารมีความปลอดภัย ซึ่งงานวิจัยนี้สอดคล้องกับผลการวิจัยที่พบว่า การบริหารความเสี่ยงมีอิทธิพลต่อความมั่นคงของข้อมูล และงานวิจัยของ Von Solms & Van Niekerk (2013) กล่าวถึงการควบคุมภายในและการประเมินผลในระบบการจัดการความมั่นคงทางเทคโนโลยีสารสนเทศ พบว่า การใช้ระบบการควบคุมและติดตามผลช่วยให้การปกป้องข้อมูลส่วนบุคคลเป็นไปตามมาตรฐานที่กำหนดและสามารถตรวจสอบได้ การประเมินผลอย่างสม่ำเสมอช่วยให้สามารถตอบสนองต่อภัยคุกคามและการละเมิดข้อมูลได้อย่างรวดเร็วและมีประสิทธิภาพ ซึ่งตรงกับผลการวิจัยที่พบว่า การควบคุม ติดตาม และประเมินผลเป็นปัจจัยที่สำคัญในการรักษาความมั่นคงของข้อมูลในธนาคาร

ผลการวิจัยดังกล่าวจึงสอดคล้องกับงานวิจัยที่กล่าวถึงการพัฒนาและการจัดการทรัพยากรบุคคลในด้านเทคโนโลยีสารสนเทศ การบริหารความเสี่ยง และการติดตามและประเมินผล ซึ่งล้วนเป็นปัจจัยสำคัญในการสร้างความมั่นคงให้กับข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ในธนาคารพาณิชย์

2. ผลการวิจัยพบว่า บทบาทของธนาคารพาณิชย์ มีอิทธิพลต่อความมั่นคงทางเทคโนโลยีสารสนเทศด้านการคุ้มครองข้อมูลส่วนบุคคลทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย เหตุเป็นเพราะความสำคัญของบทบาทเชิงกลยุทธ์ที่ธนาคารต้องมีในยุคที่ธุรกรรมทางการเงินออนไลน์เติบโตอย่างรวดเร็ว ธนาคารพาณิชย์เป็นสถาบันที่มีหน้าที่จัดการและรักษาข้อมูลส่วนบุคคลของลูกค้า ซึ่งข้อมูลเหล่านี้ถือเป็นสินทรัพย์ที่มีคุณค่าทางเศรษฐกิจและเสี่ยงต่อการถูกโจมตีหรือเข้าถึงโดยไม่ได้รับอนุญาต หากขาดการป้องกันที่เพียงพอ อาจส่งผลกระทบต่อความน่าเชื่อถือของธนาคาร รวมถึงความเชื่อมั่นของลูกค้าในการใช้บริการ หนึ่งในปัจจัยสำคัญที่ส่งผลต่อความมั่นคงคือการพัฒนาระบบเฝ้าระวังที่ทันสมัยและมีประสิทธิภาพ เนื่องจากระบบดังกล่าวช่วยตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างรวดเร็ว นอกจากนี้ การแต่งตั้งบุคคลที่มีความเชี่ยวชาญเฉพาะด้านยังมีบทบาทสำคัญในการวางแผนและจัดการระบบความปลอดภัย ตลอดจนการปฏิบัติตามหลักการคุ้มครองข้อมูลข่าวสาร ซึ่งสอดคล้องกับข้อกำหนดทางกฎหมายและมาตรฐานสากล ช่วยให้ธนาคารลดความเสี่ยงจากการละเมิดข้อมูลและการถูกลงโทษทางกฎหมาย

การที่ธนาคารพาณิชย์ต้องเผชิญกับความท้าทายจากภัยคุกคามทางไซเบอร์ที่ซับซ้อนยิ่งขึ้น ทำให้การดำเนินการเพื่อเสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศต้องพึ่งพาบทบาทเชิงรุกและความรับผิดชอบจากภายในองค์กรเอง ดังนั้น ผลการวิจัยที่ชี้ว่าความมั่นคงของระบบได้รับอิทธิพลจากบทบาทของธนาคารพาณิชย์จึง

สอดคล้องกับความจำเป็นที่ธนาคารต้องพัฒนากลยุทธ์เชิงป้องกันและปรับปรุงกระบวนการจัดการข้อมูลอย่างต่อเนื่อง เพื่อให้สอดรับกับแนวโน้มภัยคุกคามที่เปลี่ยนแปลงไปและสร้างความเชื่อมั่นแก่ผู้ใช้บริการ

ผลการวิจัยที่แสดงว่าความมั่นคงทางเทคโนโลยีสารสนเทศด้านการคุ้มครองข้อมูลส่วนบุคคลทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทยได้รับอิทธิพลจากบทบาทของธนาคารพาณิชย์ สอดคล้องกับแนวคิดเรื่อง Confidentiality, Integrity, and Availability (CIA Triad) ซึ่งเป็นกรอบแนวคิดพื้นฐานในการจัดการความปลอดภัยทางสารสนเทศ (Stallings & Brown, 2023) อธิบายว่า องค์กรต้องสร้างความมั่นใจว่าข้อมูลมีความปลอดภัยจากการเข้าถึงโดยไม่ได้รับอนุญาต (Confidentiality) มีความถูกต้องและน่าเชื่อถือ (Integrity) และสามารถเข้าถึงได้เมื่อมีความต้องการใช้งาน (Availability) ผลการวิจัยที่ชี้ให้เห็นว่า การพัฒนาระบบเฝ้าระวัง การแต่งตั้งผู้เชี่ยวชาญ และการปฏิบัติตามหลักการคุ้มครองข้อมูลข่าวสาร ช่วยเสริมสร้างความปลอดภัยและคุณภาพของการจัดการข้อมูล ตรงกับแนวคิดนี้ที่เน้นความสมดุลระหว่างองค์ประกอบทั้งสามในการปกป้องข้อมูล เช่นเดียวกับทฤษฎี Technology-Organization-Environment (TOE) Framework ที่สนับสนุนผลการวิจัย โดยระบุว่า การนำเทคโนโลยีมาใช้ในองค์กรขึ้นอยู่กับปัจจัยสามด้าน ได้แก่ เทคโนโลยี องค์กร และสิ่งแวดล้อม บทบาทของธนาคารพาณิชย์ที่พัฒนาระบบเฝ้าระวังและแต่งตั้งบุคลากรผู้เชี่ยวชาญสะท้อนถึงปัจจัยด้านองค์กรที่เน้นการจัดการทรัพยากรบุคคลและระบบภายในเพื่อเพิ่มขีดความสามารถในการคุ้มครองข้อมูล ขณะที่ปัจจัยทางเทคโนโลยีเชื่อมโยงกับการปรับใช้ระบบความปลอดภัย (Tornatzky, & Fleischer, 1990) และแนวคิด Information Security Management Systems (ISMS) ตามมาตรฐาน ISO/IEC 27001 (International Organization for Standardization, 2018) ยังสอดคล้องกับการปฏิบัติตามหลักการคุ้มครองข้อมูลข่าวสารที่ระบุในผลการวิจัย เนื่องจาก ISMS เป็นกรอบการจัดการที่มุ่งเน้นการควบคุมและปกป้องข้อมูลอย่างเป็นระบบและสอดคล้องกับข้อกำหนดด้านกฎหมายและมาตรฐานสากล

ผลการวิจัยดังกล่าวยังสอดคล้องกับงานวิจัยของ Bulgurcu, Cavusoglu, & Benbasat (2010) เรื่อง nformation security policy compliance: An empirical study of rationality-based beliefs and information security awareness ระบุว่าการปฏิบัติตามกฎหมายและนโยบายด้านความปลอดภัยของข้อมูลเป็นปัจจัยสำคัญที่ช่วยลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ซึ่งสอดคล้องกับผลการวิจัยที่เน้นการปฏิบัติตามหลักการคุ้มครองข้อมูลข่าวสารเพื่อเพิ่มความปลอดภัยของระบบข้อมูล สอดคล้องกับงานวิจัยของ Karyda, Mitrou, & Quirchmayr (2005) ระบุว่าการจัดการความปลอดภัยของข้อมูลที่มีประสิทธิภาพต้องอาศัยการพัฒนาโครงสร้างการเฝ้าระวัง การใช้เทคโนโลยีที่ทันสมัย และการมีแผนการจัดการที่เหมาะสม ซึ่งสอดคล้องกับผลการวิจัยที่ชี้ว่า การพัฒนาระบบเฝ้าระวังเป็นปัจจัยสำคัญในการเสริมสร้างความมั่นคงของข้อมูลในธนาคารพาณิชย์ เช่นเดียวกับงานวิจัยของ Dhillon, & Backhouse (2001) ที่ย้ำถึงบทบาทของบุคลากรที่มีความเชี่ยวชาญในการปฏิบัติตามมาตรฐานด้านความปลอดภัยและการจัดการข้อมูลที่มีความอ่อนไหว ซึ่งสนับสนุนผลการวิจัยเกี่ยวกับการแต่งตั้งบุคลากรที่มีความเชี่ยวชาญในการรักษาความปลอดภัยของข้อมูล และสอดคล้องกับงานวิจัยของ กริน ธัญญวิกรม และธีระ กุลสวัสดิ์ (2564) ที่พบว่า ปัญหาภัยคุกคามทางไซเบอร์ที่สำคัญ คือ ปัญหาด้านความพร้อมในการรักษาความมั่นคงปลอดภัย ไซเบอร์และความพร้อมในการรับมือต่อการสูญเสียอธิปไตยไซเบอร์ของชาติ โดยภาครัฐได้ออกกฎหมายสำคัญ 2 ฉบับ ในปี พ.ศ. 2562 คือ พ.ร.บ. ไซเบอร์ฯ และ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล และธนาคารแห่งประเทศไทยได้ออกกฎระเบียบต่าง ๆ ในการกำกับดูแลธนาคารพาณิชย์ไทย การดำเนินงานของธนาคารพาณิชย์ไทย ได้จัดทำนโยบายและแนวทางการดำเนินการด้านการรักษาความปลอดภัยของข้อมูลและความมั่นคงปลอดภัยไซเบอร์ ตามมาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001:2013) และในการดำเนินงานตาม พ.ร.บ.ไซเบอร์ฯ ควรสอดคล้องกับ NIST Cybersecurity Framework และนำมาตรฐาน ISO/IEC 27701:2019 มาใช้เป็นมาตรการเพิ่มเติมสำหรับการคุ้มครองข้อมูลส่วนบุคคลที่มีความสอดคล้องกับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

3. ผลการวิจัยพบว่า บทบาทภาครัฐ มีอิทธิพลต่อความมั่นคงทางเทคโนโลยีสารสนเทศ ด้านการคุ้มครองข้อมูลส่วนบุคคลทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย เหตุเป็นเพราะ ธนาคารพาณิชย์เป็นหนึ่งในองค์กรที่ต้องจัดการกับข้อมูลที่มีความอ่อนไหวสูง เช่น ข้อมูลประจำตัวและข้อมูลทางการเงินของลูกค้า ซึ่งหากเกิดการรั่วไหลหรือการโจรกรรมข้อมูล อาจส่งผลกระทบอย่างร้ายแรงต่อความเชื่อมั่นของลูกค้าและเสถียรภาพของระบบการเงิน ดังนั้น การบริหารจัดการด้านความปลอดภัยของข้อมูลจึงไม่อาจอาศัยเพียงมาตรการภายในขององค์กรเพียงอย่างเดียว แต่จำเป็นต้องพึ่งพากรอบการกำกับดูแลจากภาครัฐที่ชัดเจนและมีประสิทธิภาพ บทบาทของภาครัฐที่ส่งผลต่อการบริหารจัดการข้อมูลส่วนบุคคลของธนาคารพาณิชย์ประกอบด้วยองค์ประกอบหลักสามประการ ได้แก่ กฎหมายและนโยบายการคุ้มครองข้อมูล มาตรการคุ้มครองข้อมูล และการบังคับใช้กฎหมาย กฎหมายและนโยบายที่ชัดเจน เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ช่วยกำหนดกรอบแนวทางปฏิบัติสำหรับองค์กรในการจัดการข้อมูล โดยระบุถึงสิทธิของเจ้าของข้อมูล บทบาทของผู้ควบคุมข้อมูล และมาตรฐานด้านความปลอดภัย นอกจากนี้ มาตรการคุ้มครองข้อมูล เช่น การกำหนดข้อกำหนดสำหรับระบบความปลอดภัยในการจัดเก็บและส่งผ่านข้อมูล ยังช่วยให้ธนาคารมีแนวทางที่เป็นรูปธรรมในการออกแบบและปรับปรุงระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับมาตรฐานความปลอดภัยที่ได้รับการยอมรับในระดับสากล

การบังคับใช้กฎหมายอย่างมีประสิทธิภาพเป็นอีกปัจจัยสำคัญที่ส่งเสริมให้ธนาคารพาณิชย์ต้องดำเนินการอย่างจริงจังเพื่อป้องกันความเสี่ยงจากการละเมิดข้อมูลส่วนบุคคล การมีบทลงโทษที่ชัดเจนและสอดคล้องกับความเสียหายที่อาจเกิดขึ้นช่วยลดแรงจูงใจในการละเมิดหรือเพิกเฉยต่อข้อกำหนดทางกฎหมาย ทั้งนี้ ความมั่นคงทางเทคโนโลยีสารสนเทศและการบริหารจัดการข้อมูลที่มีประสิทธิภาพไม่เพียงแต่ช่วยรักษาความปลอดภัยของข้อมูลเท่านั้น แต่ยังส่งผลต่อภาพลักษณ์และความน่าเชื่อถือของธนาคารในสายตาของลูกค้าและคู่ค้า

ดังนั้น บทบาทภาครัฐและการบริหารจัดการความมั่นคงทางเทคโนโลยีสารสนเทศของธนาคารพาณิชย์สะท้อนให้เห็นถึงความสำคัญของกรอบกฎหมายที่มีประสิทธิภาพและการบังคับใช้ที่เข้มงวด ซึ่งทำให้ธนาคารสามารถจัดการกับความท้าทายในการปกป้องข้อมูลส่วนบุคคลได้อย่างเหมาะสมและตอบสนองต่อความเสี่ยงในยุคดิจิทัลได้อย่างมีประสิทธิผล

ผลการวิจัยข้างต้น สามารถเชื่อมโยงและอธิบายได้โดยทฤษฎีระบบนิเวศของการกำกับดูแลข้อมูล (Information Governance Ecosystem) ซึ่งเน้นว่าความปลอดภัยของข้อมูลเป็นผลลัพธ์จากการทำงานร่วมกันระหว่างองค์กรและหน่วยงานภายนอก โดยเฉพาะบทบาทของภาครัฐในการกำหนดกรอบกฎหมายและนโยบาย (Von Solms & Van Niekerk, 2013) กฎหมายและนโยบาย เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ของประเทศไทย เป็นตัวอย่างของการกำกับดูแลที่มีเป้าหมายในการสร้างมาตรฐานที่ชัดเจนสำหรับองค์กรเพื่อปกป้องข้อมูลส่วนบุคคล สอดคล้องกับ แนวคิดด้านการบริหารจัดการความเสี่ยงทางเทคโนโลยีสารสนเทศ (Information Security Risk Management) ซึ่งกล่าวถึงความสำคัญของการปฏิบัติตามกฎระเบียบและมาตรการที่กำหนดโดยหน่วยงานกำกับดูแลในการลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Baskerville, 1991) ชี้ให้เห็นว่า ความปลอดภัยและการรักษาความลับ การจัดการข้อมูลที่มีคุณภาพ และการบำรุงรักษาระบบความปลอดภัย จำเป็นต้องมีโครงสร้างเชิงนโยบายที่สนับสนุนอย่างชัดเจน การศึกษาโดย Siponen & Willison (2009) ยังสนับสนุนแนวคิดนี้ โดยชี้ให้เห็นว่า การบังคับใช้กฎหมายและการสร้างมาตรการเชิงป้องกันที่เข้มงวดช่วยลดการกระทำผิดเกี่ยวกับการละเมิดข้อมูล

นอกจากนี้ ผลการวิจัยยังสอดคล้องกับแนวคิดของ Gürses & Ralph (2018) ที่ชี้ให้เห็นว่าการปฏิบัติตามกฎหมายด้านการคุ้มครองข้อมูลช่วยยกระดับมาตรฐานความปลอดภัยและส่งเสริมความไว้วางใจในระบบธุรกรรมทางอิเล็กทรอนิกส์

ผลการวิจัยดังกล่าวสอดคล้องกับงานวิจัยของ Hedström, Kolkowska, Karlsson, & Allen (2011) ซึ่งเน้นว่ากฎหมายและนโยบายที่มีความชัดเจนมีบทบาทสำคัญในการยกระดับมาตรฐานการรักษาความปลอดภัย

ของข้อมูลในองค์กร ธนาคารพาณิชย์ที่ปฏิบัติตามมาตรฐานเหล่านี้สามารถลดความเสี่ยงจากการละเมิดข้อมูลได้อย่างมีประสิทธิภาพ นอกจากนี้ ผลการวิจัยสอดคล้องกับงานวิจัยของ Bélanger & Crossler (2011) โดยระบุว่าการคุ้มครองข้อมูลส่วนบุคคลที่มีประสิทธิภาพต้องอาศัยกฎหมายและมาตรการควบคุมที่เข้มงวดซึ่งส่งผลให้ผู้ใช้บริการมีความไว้วางใจในการทำธุรกรรมทางอิเล็กทรอนิกส์มากยิ่งขึ้น

4. ผลการวิจัยพบว่า บทบาทภาคประชาชน มีอิทธิพลต่อความมั่นคงทางเทคโนโลยีสารสนเทศ ด้านการคุ้มครองข้อมูลส่วนบุคคลทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย เหตุเป็นเพราะ การรับรู้ข้อมูลข่าวสารเป็นปัจจัยสำคัญที่ช่วยให้ผู้บริโภคสามารถตระหนักถึงความเสี่ยงในการทำธุรกรรมออนไลน์ รวมถึงแนวทางปฏิบัติที่ปลอดภัย เช่น การตรวจสอบความน่าเชื่อถือของเว็บไซต์หรือระบบการชำระเงิน ซึ่งส่งผลให้สามารถหลีกเลี่ยงการโจมตีทางไซเบอร์และการโจรกรรมข้อมูลได้ นอกจากนี้ ความตระหนักในความคุ้มครองของข้อมูลส่วนบุคคลเป็นตัวแปรสำคัญที่มีผลต่อพฤติกรรมผู้บริโภคในการปฏิบัติตามคำแนะนำหรือมาตรการป้องกันของธนาคาร เช่น การตั้งรหัสผ่านที่มีความซับซ้อนหรือการตรวจสอบสิทธิ์แบบสองชั้น หากประชาชนไม่ให้ความสำคัญกับมาตรการเหล่านี้ ความเสี่ยงต่อการถูกละเมิดข้อมูลจะเพิ่มขึ้นอย่างมีนัยสำคัญ และความรู้เรื่องเทคโนโลยีส่งผลโดยตรงต่อความสามารถของผู้ใช้งานในการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ ผู้ที่มีทักษะทางเทคโนโลยีสูงมักจะเข้าใจวิธีการป้องกันที่เหมาะสมและสามารถระบุสัญญาณของการโจมตีได้ดีกว่า บุคคลที่ขาดความรู้ดังกล่าวอาจตกเป็นเป้าหมายของการฉ้อโกงหรือการหลอกลวงทางออนไลน์ได้ง่ายขึ้น เมื่อประชาชนมีบทบาทอย่างแข็งขันในด้านการรับรู้ ตระหนักรู้ และมีทักษะในการป้องกันตนเอง ย่อมทำให้ความมั่นคงของระบบข้อมูลในธุรกรรมทางอิเล็กทรอนิกส์มีประสิทธิภาพยิ่งขึ้น ซึ่งเป็นเหตุผลที่ผลการวิจัยชี้ให้เห็นถึงความสัมพันธ์เชิงบวกระหว่างบทบาทของภาคประชาชนกับความมั่นคงทางเทคโนโลยีสารสนเทศในการคุ้มครองข้อมูลส่วนบุคคล

ผลการวิจัยดังกล่าว สอดคล้องกับแนวคิดและทฤษฎีที่เกี่ยวข้องกับการบริหารจัดการความปลอดภัยของข้อมูลและพฤติกรรมผู้บริโภคในโลกดิจิทัล เช่น แนวคิดเรื่อง Technology Acceptance Model (TAM) ของ Davis (1989) ซึ่งอธิบายว่าการยอมรับและการใช้งานเทคโนโลยีของผู้ใช้นั้นขึ้นอยู่กับปัจจัยการรับรู้ประโยชน์และการใช้งานง่าย แนวคิดนี้สอดคล้องกับผลการวิจัยที่แสดงให้เห็นว่าการรับรู้ข้อมูลข่าวสารและความรู้เรื่องเทคโนโลยีมีผลต่อพฤติกรรมของผู้ใช้ในการป้องกันข้อมูลส่วนบุคคล นอกจากนี้ แนวคิดของ Protection Motivation Theory (PMT) โดย Rogers (1975) อธิบายถึงกระบวนการจูงใจให้บุคคลมีพฤติกรรมป้องกันตัวเองจากภัยคุกคาม โดยปัจจัยที่สำคัญ ได้แก่ การรับรู้ความเสี่ยง (perceived threat) และการประเมินประสิทธิภาพของการป้องกัน (perceived efficacy) ซึ่งสอดคล้องกับผลการวิจัยที่ชี้ว่าความตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลช่วยให้ผู้ใช้มีพฤติกรรมปฏิบัติตามมาตรการป้องกันที่ธนาคารกำหนด ทั้งนี้ การเน้นบทบาทของบุคคลในด้านการรักษาความปลอดภัยของข้อมูลสอดคล้องกับ the Socio-Technical Systems Theory ซึ่งเน้นว่าระบบความปลอดภัยที่มีประสิทธิภาพจะต้องอาศัยปฏิสัมพันธ์ระหว่างบุคคล กระบวนการ และเทคโนโลยี โดยภาคประชาชนถือเป็นองค์ประกอบสำคัญในระบบนี้ (Bostrom & Heinen, 1977)

องค์ความรู้ใหม่

ผลการวิจัยครั้งนี้ได้สร้างองค์ความรู้ใหม่ที่สำคัญต่อแวดวงการบริหารจัดการความมั่นคงทางเทคโนโลยีสารสนเทศ โดยเฉพาะในมิติของการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย 1. งานวิจัยชี้ให้เห็นว่าการบริหารจัดการเทคโนโลยีสารสนเทศเป็นปัจจัยที่มีอิทธิพลสูงสุดต่อความมั่นคงทางเทคโนโลยีสารสนเทศ สะท้อนให้เห็นว่าโครงสร้างการจัดการ กระบวนการควบคุม และการตัดสินใจเชิงนโยบายในระดับองค์กรมีบทบาทสำคัญมากกว่าปัจจัยภายนอก ทั้งในด้านบทบาทของธนาคารพาณิชย์เอง บทบาทของภาครัฐ และบทบาทของภาคประชาชน ความรู้นี้ชี้ว่าองค์กรจำเป็นต้องสร้างระบบบริหารจัดการที่เป็นระบบและบูรณาการ เพื่อยกระดับความมั่นคงทางดิจิทัลอย่างแท้จริง 2. การศึกษานี้นำเสนอแนวทางการจัดการความมั่นคงทางเทคโนโลยีสารสนเทศที่ครอบคลุมมากถึง 16 ด้าน ซึ่งรวมตั้งแต่การกำหนดนโยบาย การจัดการ

ความเสี่ยง การเข้ารหัสและควบคุมการเข้าถึง การพัฒนาระบบงานที่มั่นคง ไปจนถึงการสร้างวัฒนธรรมองค์กรที่ให้ความสำคัญกับการฝึกอบรมและการตระหนักรู้ สิ่งนี้ถือเป็นการบูรณาการมิติทางเทคนิค มิติการบริหารจัดการ และมิติด้านบุคลากรเข้าไว้ด้วยกัน ทำให้เห็นภาพแนวทางที่ครบวงจรและสามารถนำไปประยุกต์ใช้ได้จริงในธนาคารพาณิชย์ไทย องค์ความรู้ใหม่จึงไม่เพียงตอบโจทย์ด้านความปลอดภัยเชิงเทคนิค แต่ยังขยายความเข้าใจในด้านการกำกับดูแล การสร้างมาตรฐาน และการเชื่อมโยงกับการปฏิบัติตามกฎหมายและมาตรฐานสากล ซึ่งเป็นกรอบความรู้ที่มีคุณูปการต่อทั้งนักวิชาการและผู้ปฏิบัติในวงการธนาคารพาณิชย์

สรุป

บทความนี้ได้ชี้ให้เห็นประเด็นสำคัญเกี่ยวกับการบริหารจัดการความมั่นคงทางเทคโนโลยีสารสนเทศในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการธนาคารพาณิชย์ไทย โดยผลการวิจัยยืนยันว่าปัจจัยด้านการบริหารจัดการเทคโนโลยีสารสนเทศมีอิทธิพลมากที่สุดต่อความมั่นคงทางดิจิทัล รองลงมาคือบทบาทของธนาคารพาณิชย์ที่ต้องปรับปรุงระบบบริการให้มีมาตรฐานสูงขึ้น ตามมาด้วยบทบาทของภาครัฐในการกำกับดูแลและกำหนดมาตรการเชิงนโยบาย และบทบาทของภาคประชาชนที่เกี่ยวข้องกับการสร้างวัฒนธรรมการใช้งานที่ปลอดภัยและมีความตระหนักรู้ ผลลัพธ์นี้สะท้อนให้เห็นว่าความมั่นคงทางเทคโนโลยีไม่อาจพึ่งพาเพียงปัจจัยภายนอก แต่จำเป็นต้องเริ่มจากการเสริมสร้างระบบการจัดการที่เข้มแข็งภายในองค์กรเอง บทความนี้ได้เสนอกรอบการจัดการความมั่นคงทางเทคโนโลยีสารสนเทศที่ประกอบด้วย 16 มิติ ซึ่งครอบคลุมทั้งโครงสร้างการกำกับดูแล การจัดการความเสี่ยง การเข้ารหัสและควบคุมการเข้าถึง การปกป้องเครือข่ายและระบบ การพัฒนาระบบงานอย่างมั่นคง ตลอดจนการสร้างวัฒนธรรมด้านความตระหนักรู้ของบุคลากรและผู้ใช้งาน แนวทางดังกล่าวถือเป็นกรอบเชิงปฏิบัติที่สามารถนำไปใช้ในการยกระดับมาตรฐานการรักษาความมั่นคงของธนาคารพาณิชย์ไทยให้ทัดเทียมกับมาตรฐานสากล อีกทั้งยังช่วยสร้างความมั่นใจแก่ผู้ใช้บริการในการทำธุรกรรมทางอิเล็กทรอนิกส์ สุดท้าย การวิจัยนี้ตอกย้ำว่าการสร้างความมั่นคงทางเทคโนโลยีสารสนเทศต้องเป็นความร่วมมือที่เชื่อมโยงทั้งองค์กร ภาครัฐ และประชาชน เพื่อให้ระบบการเงินดิจิทัลของประเทศมีความปลอดภัย ยั่งยืน และพร้อมรับมือกับภัยคุกคามใหม่ในอนาคต

ข้อเสนอแนะ

ข้อเสนอแนะเชิงนโยบาย

1. ภาครัฐ โดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ร่วมกับธนาคารแห่งประเทศไทย ควรเร่งพัฒนากรอบนโยบายและมาตรฐานการรักษาความปลอดภัยทางไซเบอร์ที่เป็นมาตรฐานกลาง เพื่อให้ธนาคารพาณิชย์ทุกแห่งสามารถนำไปปฏิบัติได้อย่างเป็นรูปธรรม โดยควรมีการปรับปรุงกฎหมายและระเบียบที่เกี่ยวข้องให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยี รวมถึงกำหนดบทลงโทษที่ชัดเจนสำหรับกรณีละเมิดข้อมูลส่วนบุคคล ทั้งนี้ เพื่อสร้างความเชื่อมั่นให้กับผู้ใช้บริการและป้องปรามการกระทำผิด

2. ผู้บริหารระดับสูงของธนาคารพาณิชย์ควรจัดสรรงบประมาณและทรัพยากรอย่างเพียงพอในการพัฒนาระบบรักษาความปลอดภัยที่ทันสมัย โดยเฉพาะการลงทุนในเทคโนโลยีการเข้ารหัสข้อมูล ระบบตรวจจับการบุกรุก และระบบสำรองข้อมูล เนื่องจากภัยคุกคามทางไซเบอร์มีความซับซ้อนและรุนแรงมากขึ้น การลงทุนในด้านนี้จึงถือเป็นการป้องกันความเสียหายที่อาจเกิดขึ้นในอนาคต

3. ธนาคารพาณิชย์ สถาบันการเงินแต่ละแห่งควรจัดตั้งหน่วยงานเฉพาะที่รับผิดชอบด้านความมั่นคงปลอดภัยทางไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล พร้อมทั้งพัฒนาบุคลากรให้มีความรู้ความเชี่ยวชาญอย่างต่อเนื่อง นอกจากนี้ ควรมีการจัดทำแผนรับมือเหตุฉุกเฉินและทดสอบระบบความปลอดภัยอย่างสม่ำเสมอ เพื่อให้สามารถตอบสนองต่อเหตุการณ์ละเมิดความปลอดภัยได้อย่างรวดเร็วและมีประสิทธิภาพ

4. หน่วยงานที่เกี่ยวข้องทั้งภาครัฐและธนาคารพาณิชย์ควรร่วมมือกันในการให้ความรู้และสร้างความตระหนักเกี่ยวกับการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์อย่างปลอดภัย โดยควรมีการจัดทำสื่อประชาสัมพันธ์ในรูปแบบที่เข้าใจง่าย และเผยแพร่ผ่านช่องทางที่หลากหลาย เพื่อให้ประชาชนทุกกลุ่มสามารถเข้าถึงข้อมูลได้ ทั้งนี้เพราะความรู้ความเข้าใจของผู้ใช้บริการเป็นด่านแรกในการป้องกันการละเมิดข้อมูลส่วนบุคคล

ข้อเสนอแนะเชิงการปฏิบัติ

1. ผู้บริหารธนาคาร ควรมีการกำหนดโครงสร้างการบริหารจัดการความมั่นคงปลอดภัยที่ชัดเจน โดยแต่งตั้งผู้บริหารระดับสูงที่รับผิดชอบด้านความมั่นคงปลอดภัยทางไซเบอร์โดยตรง (Chief Information Security Officer: CISO) และจัดตั้งคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์ที่มีการประชุมอย่างสม่ำเสมอ เพื่อติดตามสถานการณ์และกำหนดแนวทางการรับมือกับภัยคุกคามที่อาจเกิดขึ้น

2. ฝ่ายทรัพยากรบุคคลของธนาคารพาณิชย์ควรร่วมมือกับฝ่ายเทคโนโลยีสารสนเทศในการจัดทำแผนพัฒนาความรู้และทักษะด้านความมั่นคงปลอดภัยให้แก่พนักงานทุกระดับ โดยเฉพาะการฝึกอบรมเชิงปฏิบัติการที่เน้นการจำลองสถานการณ์จริง เช่น การจัดการกับการโจมตีทางไซเบอร์ การตรวจจับการรั่วไหลของข้อมูล และการตอบสนองต่อเหตุการณ์ละเมิดความปลอดภัย

3. ฝ่ายเทคโนโลยีของธนาคารพาณิชย์ควรดำเนินการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ โดยอาจว่าจ้างผู้เชี่ยวชาญภายนอกมาทดสอบเจาะระบบ (Penetration Testing) อย่างน้อยปีละครั้ง พร้อมทั้งนำผลการทดสอบมาปรับปรุงระบบป้องกันให้แข็งแกร่งยิ่งขึ้น นอกจากนี้ ควรมีการติดตั้งระบบเฝ้าระวังภัยคุกคามแบบ Real-time และจัดทำแผนสำรองข้อมูลที่มีประสิทธิภาพ

4. การปฏิบัติงานประจำวันของพนักงานธนาคารพาณิชย์ ควรมีการกำหนดขั้นตอนการปฏิบัติงาน (Standard Operating Procedures) ที่ชัดเจนสำหรับการจัดการข้อมูลส่วนบุคคลของลูกค้า โดยระบุว่าใครมีสิทธิเข้าถึงข้อมูลใดบ้าง ต้องผ่านการอนุมัติจากใคร และมีขั้นตอนการตรวจสอบการใช้งานข้อมูลอย่างไร รวมถึงการกำหนดระยะเวลาในการเก็บรักษาและทำลายข้อมูลที่ไม่จำเป็นต้องใช้งานแล้ว

5. ฝ่ายบริการลูกค้าของธนาคารพาณิชย์ควรจัดทำคู่มือการใช้บริการธุรกรรมอิเล็กทรอนิกส์ที่เข้าใจง่าย พร้อมทั้งจัดตั้งศูนย์ช่วยเหลือลูกค้าที่สามารถให้คำแนะนำและแก้ไขปัญหาได้ตลอด 24 ชั่วโมง โดยเฉพาะในกรณีที่ลูกค้าพบเห็นความผิดปกติหรือสงสัยว่าข้อมูลของตนอาจถูกละเมิด

6. สำหรับการประสานงานกับหน่วยงานภายนอก ธนาคารพาณิชย์ควรมีการจัดทำบันทึกข้อตกลง (MOU) กับหน่วยงานที่เกี่ยวข้อง เช่น ศูนย์ไซเบอร์ของประเทศไทย (Thailand Computer Emergency Response Team: ThaiCERT) เพื่อแลกเปลี่ยนข้อมูลเกี่ยวกับภัยคุกคามและแนวทางการป้องกัน รวมถึงการขอความช่วยเหลือในกรณีเกิดเหตุฉุกเฉิน

เอกสารอ้างอิง

กริน ธัญญวิกรม และธีระ กุลสวัสดิ์. (2564). การจัดการความมั่นคงทางเทคโนโลยีสารสนเทศ กรณีศึกษา การคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรม ทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย. *วารสารสังคมศาสตร์และมานุษยวิทยาเชิงพุทธ, 6*(3), 371-386.

เทอดพงษ์ เปล่งศิริวัฒน์. (2558). *Cyber Attack ภัยคุกคามของสถาบันการเงินไทยในยุคดิจิทัล*. ธนาคารแห่งประเทศไทย. สืบค้น 19 ธันวาคม 2567, จาก https://www.bot.or.th/th/research-and-publications/articles-and-publications/articles/Article_17Dec2015.html.

พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. *ราชกิจจานุเบกษา* เล่ม 136 ตอนพิเศษ 91 ง วันที่ 27 พฤษภาคม 2562.

Aven, T. (2008). Risk analysis: Assessing uncertainties beyond expected values and probabilities. Wiley.

Baskerville, R. (1991). Risk analysis: An interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems, 1*, 121-130.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017-1041.

Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective-part I: The Causes. *MIS Quarterly, 1*(3), 17-32.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

Comrey, A. L., & Lee, H. B. (1992). *A first course in factor analysis* (2nd ed.). Hillsdale, NJ: Lawrence Erlbaum.

COSO (2013). *Internal control – integrated framework: Executive summary*. Committee of Sponsoring Organizations of the Treadway Commission.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Toward socio-organizational perspectives. *Information Systems Journal, 11*(2), 127-153.

Gürses, S., & van Hoboken, J. (2018). Privacy after the Agile Turn. The Cambridge Handbook of Consumer Privacy. Cambridge University Press.

Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). Value conflicts for information security management. *Journal of Strategic Information Systems, 22*(4), 373-388.

International Organization for Standardization. (2018). *ISO/IEC 27001: Information security management systems – requirements.* Retrieved December 14, 2024, from https://www.iso.org/standard/27001.

Karyda, M., Mitrou, L., & Quirchmayr, G. (2005). Information systems security policies: A contextual perspective. *Computers & Security, 24*(3), 246-260.

Peltier, J. W. (2010). *Information security risk management* (3rd ed.). New York: Auerbach Publications.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology: Interdisciplinary and Applied, 91*(1), 93-114.

Siponen, M., & Willison, R. (2009). *Information security management standards: Problems and solutions*. *Information & Management, 46*(5), 267-270.

Stallings, W., & Brown, L. (2023). *Computer security: Principles and practice* (5th ed.). Pearson.

Swanson, R. A., & Holton, E. F. (2009). *Foundations of human resource development (2nd ed.).* Berrett-Koehler Publishers.

Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington: Lexington Books.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102.

World Economic Forum. (2020). *The Global Competitiveness Report 2020*. New York: Oxford University Press.