

การวิจัยเชิงเอกสารเพื่อสังเคราะห์องค์ประกอบของแนวคิดการจัดการความเสี่ยง

จากภัยคุกคามไซเบอร์ในยุค Digital Disruption

A Documentary Research on Synthesizing the Components of Cyber Risk Management Concepts in the Era of Digital Disruption

Received: 24/05/2569

Revised: 26/06/2569

Accepted: 27/06/2569

ธัญวรัตน์ คงนุ่น¹ และ ธนัสตา โรจนตระกูล²

Tunvarat Kongnun¹ and Tanastha Rojanatrakul²

บทคัดย่อ

ยุค Digital Disruption ได้เปลี่ยนภูมิทัศน์ด้านความมั่นคงไซเบอร์ของภาครัฐอย่างมีนัยสำคัญ โดยเทคโนโลยีเกิดใหม่ เช่น Cloud Computing, Artificial Intelligence (AI), Artificial Intelligence (AI), Big Data และ Blockchain แม้ช่วยเพิ่มประสิทธิภาพการให้บริการสาธารณะ แต่กลับขยายพื้นที่เสี่ยงและเพิ่มความซับซ้อนของภัยคุกคามไซเบอร์ งานวิจัยนี้มีวัตถุประสงค์เพื่อ (1) สังเคราะห์องค์ประกอบแนวคิดการจัดการความเสี่ยงไซเบอร์ในภาครัฐ และ (2) วิเคราะห์ความเชื่อมโยงระหว่าง Digital Disruption กับ Cyber Resilience ในบริบทภาครัฐไทยและต่างประเทศ โดยใช้ระเบียบวิธีวิจัยเชิงเอกสาร (Documentary Research) จากงานวิชาการ มาตรฐานสากล รายงานนโยบาย และฐานข้อมูลนานาชาติที่เกี่ยวข้อง

ผลการวิเคราะห์พบว่า การจัดการความเสี่ยงไซเบอร์ของภาครัฐประกอบด้วยองค์ประกอบหลัก 7 ประการ ได้แก่ การกำกับดูแลและนโยบาย การประเมินความเสี่ยง มาตรการป้องกัน ระบบเฝ้าระวังและตรวจจับ การตอบสนองและฟื้นฟู มนุษย์และวัฒนธรรมองค์กร และความยืดหยุ่นทางดิจิทัล ทั้งนี้ Digital Disruption ได้ทำให้ความเสี่ยงไซเบอร์กลายเป็นความเสี่ยงเชิงยุทธศาสตร์ของรัฐ ไม่ใช่เพียงประเด็นด้านเทคโนโลยี โดยมีลักษณะเป็น Shared Risk เชื่อมโยงเป็น Ecosystem และต้องใช้แนวทางบริหารแบบ Proactive และ Predictive มากขึ้น

อย่างไรก็ตาม ยังพบช่องว่างทางวิชาการ ได้แก่ การมุ่งเน้นด้านเทคนิคมากกว่าปัจจัยเชิงสังคม ความสัมพันธ์เชิงสาเหตุระหว่าง Digital Disruption และ Cyber Resilience ที่ยังมีจำกัดและการขาดกรอบวิเคราะห์ผลกระทบเชิงเศรษฐกิจและความมั่นคงมนุษย์ ซึ่งเป็นโอกาสสำหรับการศึกษวิจัยในอนาคต ทั้งในระดับนโยบาย องค์กร และสังคม

คำสำคัญ: การจัดการความเสี่ยง, ภัยคุกคามไซเบอร์, ดิจิทัล ดิสรัปชัน

¹อาจารย์หลักสูตรรัฐประศาสนศาสตร์ คณะสังคมศาสตร์และการพัฒนาท้องถิ่น มหาวิทยาลัยราชภัฏพิบูลสงคราม

¹Lecturer, Public Administration Program, Faculty of Social Sciences and Local Development, Pibulsongkram Rajabhat University, Thailand

²อาจารย์หลักสูตรรัฐประศาสนศาสตร์ คณะสังคมศาสตร์และการพัฒนาท้องถิ่น มหาวิทยาลัยราชภัฏพิบูลสงคราม

²Lecturer, Public Administration Program, Faculty of Social Sciences and Local Development, Pibulsongkram Rajabhat University, Thailand

*E-mail: tanastha.r@psru.ac.th

ABSTRACT

The era of Digital Disruption has significantly transformed the cybersecurity landscape of the public sector. Emerging technologies such as Cloud Computing, the Internet of Things (IoT), Artificial Intelligence (AI), Big Data, and Blockchain have enhanced efficiency, accessibility, and transparency in government services; however, they have simultaneously expanded attack surfaces and increased the complexity of cyber threats. This study aims to (1) synthesize the conceptual components of cyber risk management in the public sector, and (2) examine the relationship between Digital Disruption and Cyber Resilience across national and international governmental contexts. A documentary research method was employed, drawing on academic literature, global cybersecurity frameworks, policy reports, and international research databases.

The findings reveal seven core components of cyber risk management in the public sector: governance and policy, risk identification and assessment, preventive measures, monitoring and detection, incident response and recovery, human cyber awareness, and digital resilience. Digital Disruption has shifted cyber risk from a technical concern to a strategic state-level issue characterized by interdependence, shared vulnerabilities, and cross-organizational ecosystems, requiring proactive and predictive security approaches supported by data analytics and AI.

Despite growing scholarly attention, research gaps remain-particularly the dominance of technical perspectives over behavioral and societal dimensions, limited empirical studies on causal relationships between Digital Disruption and Cyber Resilience, and the absence of integrated analytical frameworks linking cyber risk to economic stability, public trust, and human security. These gaps present opportunities for future research, especially in developing public policy, organizational models, and resilience-based cybersecurity strategies.

Keywords: Risk Management, Cybersecurity, Digital Disruption

บทนำ

ในบริบทของการบริหารภาครัฐและภาคธุรกิจ การบริหารความเสี่ยงถือเป็นกลไกสำคัญที่ช่วยให้องค์กรสามารถดำเนินงานได้อย่างมีประสิทธิภาพ โปร่งใส และบรรลุวัตถุประสงค์ตามหลักการบริหารกิจการบ้านเมืองที่ดี ตามพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. 2545 การบริหารความเสี่ยงที่มีประสิทธิภาพช่วยลดความสูญเสีย เพิ่มมูลค่าให้แก่องค์กร และสร้างความเชื่อมั่นแก่ ผู้มีส่วนได้เสีย (Narumon Saardchom, 2007; Innoppakoon & Yenyuak, 2020; Al-Nimer et al., 2021)

อย่างไรก็ตาม การเปลี่ยนแปลงของสภาพแวดล้อมการดำเนินงานในยุค Digital Disruption โดยเฉพาะความก้าวหน้าทางเทคโนโลยีสารสนเทศ ได้ก่อให้เกิดความเสี่ยงรูปแบบใหม่ที่มีความซับซ้อนและรุนแรงมากขึ้น

หน่วยงานทั้งภาครัฐและเอกชนต้องเผชิญกับภัยคุกคามไซเบอร์ เช่น การโจมตีด้วยมัลแวร์ การโจรกรรมและการละเมิดข้อมูลส่วนบุคคล รวมถึงการโจมตีโครงสร้างพื้นฐานที่สำคัญ ซึ่งอาจส่งผลกระทบต่อเศรษฐกิจ สังคม และความมั่นคงของประเทศ

ความเสี่ยงด้านไซเบอร์ได้รับการยอมรับว่าเป็นหนึ่งในความเสี่ยงระดับโลกที่มีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง รายงานของ World Economic Forum (2022) ชี้ให้เห็นว่า องค์กรจำเป็นต้องพัฒนาระบบการบริหารจัดการความเสี่ยงไซเบอร์อย่างเป็นระบบ ควบคู่กับการสร้างวัฒนธรรมความเสี่ยง (Risk culture) เพื่อรองรับความไม่แน่นอนในสภาพแวดล้อมดิจิทัลที่เปลี่ยนแปลงอย่างรวดเร็ว

แม้จะมีแนวคิดและกรอบการจัดการความเสี่ยงไซเบอร์หลากหลาย แต่ยังขาดการสังเคราะห์องค์ประกอบและการอธิบายความเชื่อมโยงของแนวคิดเหล่านั้นอย่างเป็นระบบ การวิจัยเชิงเอกสารเพื่อสังเคราะห์องค์ประกอบของแนวคิดการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ในยุค Digital Disruption จึงมีความสำคัญทั้งในเชิงวิชาการและเชิงปฏิบัติ เนื่องจากสามารถใช้เป็นฐานความรู้สำหรับการพัฒนานโยบาย กลยุทธ์ และแนวทางการบริหารความเสี่ยงไซเบอร์ที่เหมาะสมกับบริบทขององค์กรในยุคดิจิทัล

ความเสี่ยงด้านไซเบอร์ได้รับการยอมรับว่าเป็นหนึ่งในความเสี่ยงสำคัญของโลกที่ทุกองค์กรต้องให้ความสำคัญ โดยรายงานของ World Economic Forum (2022) ระบุว่าภัยคุกคามไซเบอร์เป็นความเสี่ยงที่มีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง ทั้งในด้านความถี่และความรุนแรง องค์กรจึงจำเป็นต้องพัฒนาระบบการบริหารความเสี่ยงไซเบอร์ที่ครอบคลุมทั้งด้านการกำกับดูแล การบริหารจัดการเทคโนโลยี การพัฒนาบุคลากร และการสร้าง วัฒนธรรมความเสี่ยง (Risk Culture) เพื่อเสริมสร้างความสามารถในการรับมือกับความไม่แน่นอนในยุคดิจิทัล แม้จะมีกรอบแนวคิดและมาตรฐานการจัดการความเสี่ยงไซเบอร์ที่ได้รับการยอมรับในระดับสากล เช่น NIST Cybersecurity Framework, ISO/IEC 27005 และ COBIT 2019 แต่งานวิชาการส่วนใหญ่ยังมุ่งศึกษาเฉพาะการประยุกต์ใช้แต่ละกรอบแนวคิดหรือการประเมินประสิทธิภาพของเครื่องมือแต่ละประเภท ขณะที่ยังขาดการสังเคราะห์องค์ประกอบหลักและการอธิบายความสัมพันธ์เชิงบูรณาการของแนวคิดการจัดการความเสี่ยงไซเบอร์ในบริบทของยุค Digital Disruption ซึ่งมีการเปลี่ยนแปลงอย่างรวดเร็วและเชื่อมโยงหลายมิติ

ดังนั้น การวิจัยเชิงเอกสารเพื่อสังเคราะห์องค์ประกอบของแนวคิดการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ในยุค Digital Disruption จึงมีความสำคัญทั้งในเชิงวิชาการและเชิงปฏิบัติ เนื่องจากจะช่วยพัฒนาองค์ความรู้เชิงบูรณาการเกี่ยวกับองค์ประกอบของการบริหารความเสี่ยงไซเบอร์ อธิบายความสัมพันธ์ระหว่างแนวคิดสำคัญจากทฤษฎีและมาตรฐานสากล และสามารถใช้เป็นฐานในการพัฒนานโยบาย กลยุทธ์ และแนวทางการบริหารความเสี่ยงไซเบอร์ที่เหมาะสมกับบริบทขององค์กรภาครัฐและภาคธุรกิจในยุคดิจิทัล รวมทั้งเป็นพื้นฐานสำหรับการศึกษาวิจัยเชิงประจักษ์และการพัฒนาแบบจำลองการบริหารความเสี่ยงไซเบอร์ในอนาคต

วัตถุประสงค์ของการศึกษา

1. เพื่อสังเคราะห์องค์ประกอบของแนวคิดการจัดการความเสี่ยงไซเบอร์
2. เพื่อศึกษาความเชื่อมโยงของแนวคิดการจัดการความเสี่ยงไซเบอร์ในยุค Digital Disruption

วิธีการวิจัย

การศึกษาเรื่อง การวิจัยเชิงเอกสารเพื่อสังเคราะห์องค์ประกอบและวิเคราะห์ความสัมพันธ์ของแนวคิดการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ในยุค Digital Disruption ผู้วิจัยได้กำหนดระเบียบวิธีวิจัยไว้ดังนี้

1. รูปแบบการวิจัย

งานวิจัยนี้เป็นการวิจัยเชิงเอกสาร (Documentary Research) โดยมุ่งเน้นการรวบรวมและวิเคราะห์ข้อมูลจากเอกสารระดับทุติยภูมิ (Secondary Data) เพื่อสังเคราะห์องค์ความรู้ตามวัตถุประสงค์ที่กำหนด

2. แหล่งข้อมูลและขอบเขตเอกสาร

ประชากรที่ใช้ในการศึกษา ได้แก่ บทความวิจัย บทความวิชาการ วิทยานิพนธ์ และรายงานวิจัยที่เกี่ยวข้องกับการจัดการความเสี่ยงไซเบอร์ โดยกำหนดขอบเขตเนื้อหาครอบคลุม 5 ประเด็นหลัก ได้แก่ (1) แนวคิดการจัดการความเสี่ยง (Risk Management Concept) (2) NIST Cybersecurity Framework (CSF) (3) ISO/IEC 27005: การจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (4) Enterprise Risk Management (ERM) (5) ทฤษฎี Game Theory และสรุปความสัมพันธ์ระหว่างแนวคิด

3. เครื่องมือที่ใช้ในการวิจัย

ขั้นตอนการพัฒนาเครื่องมือสำหรับการวิเคราะห์เอกสาร (Document Analysis Form) โดยอธิบายหลักเกณฑ์ในการกำหนดประเด็นวิเคราะห์ แหล่งที่มาของกรอบแนวคิด การสร้างหมวดหมู่ข้อมูล (Coding Scheme) ตลอดจนกระบวนการตรวจสอบความเหมาะสมของเครื่องมือ เพื่อให้กระบวนการวิเคราะห์เอกสารมีความเป็นระบบและสามารถตรวจสอบความน่าเชื่อถือของผลการวิจัยได้

ผู้วิจัยได้พัฒนาเครื่องมือเพื่อใช้ในการเก็บรวบรวมและบันทึกข้อมูล ดังนี้

1) แบบประเมินคุณภาพงานวิจัย เพื่อใช้ตรวจสอบความเหมาะสมและคุณภาพของเอกสารที่นำมาศึกษา

2) แบบบันทึกข้อมูลงานวิจัย ซึ่งใช้ในการบันทึกรายละเอียดสำคัญของเอกสาร เช่น ชื่อเรื่อง ผู้วิจัย ปีที่เผยแพร่ วัตถุประสงค์ วิธีดำเนินการวิจัย ผลการศึกษา และแนวคิดสำคัญ

การพัฒนาและตรวจสอบคุณภาพของแบบประเมินคุณภาพงานวิจัยอ้างอิงหลักเกณฑ์การประเมินคุณภาพงานวิจัยของ Joanna Briggs Institute (JBI, 2023) โดยพิจารณาความเหมาะสมของวัตถุประสงค์การวิจัย ความน่าเชื่อถือของแหล่งข้อมูล ความเหมาะสมของระเบียบวิธีวิจัย วิธีการเก็บรวบรวมข้อมูล การวิเคราะห์ข้อมูล และความสมเหตุสมผลของผลการวิจัย เพื่อให้การคัดเลือกและสังเคราะห์เอกสารเป็นไปอย่างมีคุณภาพและสามารถตรวจสอบได้

4. การเก็บรวบรวมข้อมูล

ผู้วิจัยดำเนินการเก็บรวบรวมข้อมูลด้วยตนเองผ่านฐานข้อมูลออนไลน์ โดยมีขั้นตอนดังนี้

1) คัดเลือกและดาวน์โหลดเอกสารฉบับสมบูรณ์ (Full Text) ที่เกี่ยวข้อง

2) ตรวจสอบความถูกต้องและความน่าเชื่อถือของเอกสารตามหลักเกณฑ์ของ Scott (1990) ได้แก่ ความถูกต้อง (Authenticity) ความน่าเชื่อถือ (Credibility) ความเป็นตัวแทน (Representativeness) และความหมายชัดเจน (Meaning)

3) ศึกษาเนื้อหาโดยละเอียดและและบันทึกข้อมูลที่เกี่ยวข้องลงในแบบบันทึกข้อมูลงานวิจัยตามประเด็นที่กำหนด เพื่อนำไปใช้ในการสังเคราะห์และวิเคราะห์ข้อมูลในลำดับต่อไป

5. การวิเคราะห์เอกสาร

การวิจัยครั้งนี้เป็นการวิจัยเชิงเอกสาร (Documentary Research) โดยใช้ การวิเคราะห์เอกสาร (Document Analysis) ร่วมกับ การสังเคราะห์เนื้อหา (Content Synthesis) เพื่อรวบรวม วิเคราะห์ และสังเคราะห์องค์ความรู้จากหนังสือ บทความวิชาการ งานวิจัย และมาตรฐานสากลที่เกี่ยวข้องกับการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ ได้แก่ NIST Cybersecurity Framework, ISO/IEC 27005, ISO 31000, COBIT 2019 และเอกสารทางวิชาการอื่น ๆ จากนั้นนำข้อมูลมาวิเคราะห์เชิงเปรียบเทียบ (Comparative Analysis) และสังเคราะห์องค์ประกอบ รวมทั้งอธิบายความสัมพันธ์ของแนวคิดเพื่อพัฒนาเป็นกรอบแนวคิดการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ในยุค Digital Disruption

ผลการวิจัย

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อ (1) สังเคราะห์องค์ประกอบของแนวคิดการจัดการความเสี่ยงไซเบอร์ (2) ศึกษาความเชื่อมโยงของแนวคิดการจัดการความเสี่ยงไซเบอร์ในยุค Digital Disruption โดยใช้วิธีวิจัยเชิงเอกสารจากวรรณกรรมวิชาการ มาตรฐานสากล และรายงานเชิงนโยบายที่เกี่ยวข้อง โดยผลการวิจัยมีประเด็นสำคัญดังนี้

1. ผลการสังเคราะห์องค์ประกอบของแนวคิดการจัดการความเสี่ยงไซเบอร์

จากการสังเคราะห์เอกสารทางวิชาการ มาตรฐานสากล (ISO/IEC 27001, NIST CSF, COBIT) และรายงานความเสี่ยงระดับโลกกว่า 40 รายการ พบว่า องค์ประกอบสำคัญของการจัดการความเสี่ยงไซเบอร์ในยุค Digital Disruption โดยเฉพาะในบริบทภาครัฐ ประกอบด้วย 7 ด้านหลัก ดังนี้

1) การกำกับดูแลและนโยบาย (Cyber Governance & Policy) ความมั่นคงไซเบอร์ไม่ใช่เพียงเรื่องเทคนิคของฝ่าย IT แต่เป็น “ภารกิจเชิงยุทธศาสตร์ของรัฐ” ผู้บริหารระดับสูงต้องมีบทบาท นำในการกำหนดนโยบาย อนุมัติงบประมาณ และสร้างโครงสร้างความปลอดภัยที่ชัดเจน

2) การระบุและประเมินความเสี่ยง (Risk Identification and Assessment) เป็นรากฐานสำคัญในการเข้าใจภัยคุกคาม (Threat Landscape) และช่องโหว่ (Vulnerability) โดยต้องประเมินผลกระทบครอบคลุมทั้งมิติเทคโนโลยี เศรษฐกิจ และสังคม

3) มาตรการป้องกัน (Preventive and Control Measures) มุ่งลดโอกาสการเกิดเหตุผ่านการควบคุมสิทธิ์เข้าถึง (Access Control) การเข้ารหัสข้อมูล (Encryption) และการจัดการทรัพยากรสารสนเทศ

4) ระบบตรวจจับและเฝ้าระวัง (Monitoring and Detection) การใช้เทคโนโลยี AI และ Machine Learning เพื่อตรวจจับพฤติกรรมผิดปกติแบบ Real-time เพื่อป้องกันความเสียหายก่อนลุกลามสู่ระดับประเทศ

5) การตอบสนองเหตุการณ์และฟื้นฟู (Incident Response & Recovery) ความสามารถในการควบคุมความเสียหายและทำให้บริการสาธารณะกลับสู่สภาวะปกติได้เร็วที่สุด ซึ่งถือเป็นภารกิจด้านความมั่นคงสาธารณะ

6) มนุษย์และวัฒนธรรมองค์กรไซเบอร์ (Human Cyber Awareness) มนุษย์คือช่องโหว่ที่สำคัญที่สุด โดยพบว่ากว่า 90% ของเหตุการณ์ข้อมูลรั่วไหลเกิดจาก Human Error การสร้างวัฒนธรรมความปลอดภัยจึงมีประสิทธิภาพสูงกว่าการลงทุนด้านเทคโนโลยีเพียงอย่างเดียว

7) ความยืดหยุ่นทางดิจิทัล (Cyber Resilience) การปรับมุมมองจากการป้องกันเพียงอย่างเดียวไปสู่ความสามารถในการดำเนินงานต่อไปได้แม้จะถูกโจมตี

ตารางสรุปเปรียบเทียบและประเด็นสำคัญจากการศึกษา

เพื่อให้เห็นภาพความแตกต่างระหว่างแนวคิดความปลอดภัยแบบดั้งเดิมและความยืดหยุ่นในบริบทภาครัฐ ผลการวิจัยได้นำเสนอดังนี้

ตารางที่ 1 ความแตกต่างระหว่าง Cybersecurity และ Cyber Resilience ในภาครัฐ

มิติ	Cybersecurity	Cyber Resilience
เป้าหมาย	ป้องกันการโจมตี	ดำเนินงานต่อได้แม้ถูกโจมตี
มุมมอง	เชิงเทคนิค	เชิงนโยบาย องค์กร สังคม
โฟกัส	Firewall, access control, patching	Continuity, recovery, adaptability
ตัวชี้วัด	อัตราป้องกันสำเร็จ	ระยะเวลาฟื้นตัว (MTTR) ความต่อเนื่องบริการ

งานวิจัยยังได้สรุปข้อค้นพบจากการวิเคราะห์งานวิจัยสำคัญที่เกี่ยวข้อง เพื่อเป็นแนวทางในการต่อยอดองค์ความรู้ ดังนี้

ตารางที่ 2 ข้อค้นพบเชิงสังเคราะห์จากแหล่งข้อมูลมาตรฐานและงานวิจัย

ลำดับ	ผู้วิจัย/ปี	ผลการวิจัยสำคัญ	ประเด็นต่อยอด
1	ISO (2022)	โครงสร้างนโยบายและการกำกับดูแลเป็นฐานของ Cyber Risk	ต้องเสริมสร้างวัฒนธรรมองค์กร
2	NIST (2018)	ระบุ 5 ฟังก์ชัน: Identify, Protect, Detect, Respond, Recover	เหมาะสำหรับโครงสร้างพื้นฐานสำคัญ
3	IBM Security (2023)	90% ของเหตุการณ์เกิดจาก Human Error	เน้นความเสี่ยงเชิงพฤติกรรมมนุษย์
4	WEF (2024)	Cyber Risk เป็นความเสี่ยงติดอันดับ Top 5 ของโลก	ความร่วมมือข้ามประเทศมีความจำเป็น
5	McKinsey (2024)	องค์กรที่มี Resilience จะฟื้นตัวเร็วกว่าปกติ 40%	ต้องผสานเทคโนโลยี คน และกระบวนการ

นอกจากนี้ การสังเคราะห์งานวิจัยที่เกี่ยวข้องยังพบ “แกนกลางของแนวคิดร่วม” ระหว่างงานวิชาการ และมาตรฐานสากล ดังตารางที่ 2 ซึ่งยืนยันว่า การกำกับดูแลระดับนโยบาย การบูรณาการกลยุทธ์องค์กร และ ปัจจัยด้านมนุษย์ เป็นหัวใจของการจัดการความเสี่ยงไซเบอร์ (IBM Security, 2023; ISACA, 2019)

2. ความเชื่อมโยงของแนวคิดการจัดการความเสี่ยงไซเบอร์ในยุค Digital Disruption

การเปลี่ยนผ่านสู่ยุค Digital Disruption ได้เปลี่ยนภูมิทัศน์ความเสี่ยงไซเบอร์ของภาครัฐอย่างมีนัยสำคัญ ทั้งในเชิงขอบเขต ความซับซ้อน ความเร็ว และผลกระทบ โดยความเสี่ยงดังกล่าวมิได้จำกัดอยู่เพียงระดับเทคนิคของระบบสารสนเทศ แต่ได้ขยายไปสู่ระดับเชิงยุทธศาสตร์ นโยบาย ความมั่นคงของรัฐ และความเชื่อมั่นของประชาชน ซึ่งสอดคล้องกับวัตถุประสงค์การวิจัยที่มุ่งวิเคราะห์ความสัมพันธ์ระหว่าง Digital Disruption กับแนวคิดการจัดการความเสี่ยงไซเบอร์ภาครัฐในมิติร่วมสมัย

1) การขยายพื้นที่เสี่ยงไซเบอร์จากการใช้เทคโนโลยีดิจิทัลขั้นสูง

ผลการวิจัยชี้ว่า การนำเทคโนโลยีใหม่ เช่น Cloud Computing, Internet of Things (IoT), Artificial Intelligence (AI), Big Data และ Blockchain มาใช้ในภาครัฐ แม้เพิ่มประสิทธิภาพ ความรวดเร็ว และความโปร่งใสของการให้บริการสาธารณะ แต่ในขณะเดียวกันกลับได้ขยาย “พื้นที่เสี่ยงไซเบอร์” (attack surface) ของรัฐอย่างมาก (World Economic Forum, 2024) ระบบราชการซึ่งเดิมทำงานแบบแยกส่วน ถูกเชื่อมโยงเป็นเครือข่ายดิจิทัลเดียวกัน ทำให้ช่องโหว่เพียงจุดเดียวอาจลุกลามเป็นเหตุการณ์ไซเบอร์ระดับชาติได้

นอกจากนี้ เทคโนโลยีดิจิทัลยุคใหม่ยังเปิดโอกาสให้ผู้โจมตีใช้วิธีการขั้นสูง เช่น AI-driven phishing, automated ransomware และการโจมตีผ่านห่วงโซ่อุปทานดิจิทัล ซึ่งเกินขีดความสามารถของการป้องกันแบบดั้งเดิม ส่งผลให้ความเสี่ยงไซเบอร์ของภาครัฐมีลักษณะ ซับซ้อน รวดเร็ว และยากต่อการคาดการณ์มากขึ้น (IBM Security, 2023)

2) การเปลี่ยนสถานะของความเสี่ยงไซเบอร์สู่ “ความเสี่ยงเชิงยุทธศาสตร์ของรัฐ”

ผลการศึกษาพบว่า ในบริบทภาครัฐ ข้อมูลดิจิทัล ได้กลายเป็นสินทรัพย์เชิงยุทธศาสตร์ของประเทศ ทั้งข้อมูลทะเบียนราษฎร ระบบภาษี สาธารณสุข สวัสดิการสังคม และความมั่นคงภายในส่งผลให้ความเสี่ยงไซเบอร์ไม่ได้เป็นเพียงความเสี่ยงด้าน IT แต่พัฒนาเป็นความเสี่ยงเชิงกลยุทธ์ (Strategic Risk) ที่กระทบต่อความมั่นคง สิทธิประชาชน และเสถียรภาพทางการเมือง (ISO, 2022)

ความเสียหายจากเหตุไซเบอร์ของภาครัฐจึงไม่ได้จำกัดอยู่ที่การกู้คืนระบบหรือค่าใช้จ่ายทางเทคนิค แต่รวมถึงผลกระทบเชิงนโยบายและสังคม เช่น การหยุดชะงักของบริการรัฐ การละเมิดข้อมูลส่วนบุคคล ความตื่นตระหนกของประชาชน และการเสื่อมศรัทธาต่อรัฐบาล ซึ่งสะท้อนว่าการบริหารความเสี่ยงไซเบอร์จำเป็นต้องอยู่ในความรับผิดชอบของผู้บริหารระดับสูง ไม่ใช่หน้าที่ของฝ่ายเทคนิคเพียงอย่างเดียว

3) ความเสี่ยงไซเบอร์ในฐานะ “Shared Risk” และการบริหารเชิงระบบนิเวศ (Ecosystem)

ผลการวิจัยสอดคล้องกับแนวคิดของ ISACA (2019) ที่ระบุว่า ความเสี่ยงไซเบอร์ในยุคดิจิทัลเป็นความเสี่ยงร่วม (Shared Risk) ที่เกิดจากความเชื่อมโยงเชิงโครงข่ายระหว่างหน่วยงานรัฐ ภาคเอกชน ผู้รับจ้าง ผู้ให้บริการคลาวด์ และองค์กรท้องถิ่น การบริหารความเสี่ยงแบบองค์กรเดี่ยวจึงไม่เพียงพออีกต่อไป

ในภาครัฐระบบจำนวนมากพึ่งพาซึ่งกันและกัน เช่น ระบบทะเบียนราษฎรเชื่อมกับ การสาธารณสุข การคลัง และสวัสดิการ ทำให้ช่องโหว่ในห่วงโซ่อุปทานดิจิทัลเพียงจุดเดียวสามารถ สร้างผลกระทบ เป็นลูกโซ่ (Cascading Cyber Risk) ต่อทั้งระบบราชการได้ ผลการวิจัยจึงชี้ให้เห็นความจำเป็นของการบริหาร ความเสี่ยงไซเบอร์ในมิติ Ecosystem Governance ผ่านมาตรฐานกลาง การกำกับดูแล Vendor และการ แลกเปลี่ยน Threat Intelligence ระหว่างหน่วยงาน

4) การเปลี่ยนแนวคิดจาก Reactive สู่ Proactive และ Predictive Cyber Risk Management

ผลการศึกษาพบการเปลี่ยนกระบวนทัศน์ด้านการจัดการความเสี่ยงไซเบอร์อย่างชัดเจน จาก การตอบสนองหลังเกิดเหตุ (Reactive) ไปสู่การป้องกันเชิงรุก (Proactive) และการคาดการณ์ล่วงหน้า (Predictive) โดยใช้ข้อมูลเชิงลึกและ AI วิเคราะห์แนวโน้มภัยไซเบอร์ล่วงหน้า (IBM Security, 2023)

สำหรับภาครัฐ แนวคิด Predictive มีความสำคัญอย่างยิ่ง เนื่องจากบริการสาธารณะจำนวนมาก ไม่สามารถหยุดชะงักได้ เช่น ระบบโรงพยาบาล ภาษี และโครงสร้างพื้นฐานสำคัญ ผลการวิจัยระบุว่า การ พัฒนาระบบเฝ้าระวังแบบ Real-time ศูนย์ SOC ระดับชาติ และการบริหารข้อมูล log อย่างเป็นระบบ เป็น หัวใจของความสามารถในการ “รู้ก่อน-เตือนก่อน-รับมือก่อน” ผู้โจมตี

5) ปัจจัยมนุษย์และวัฒนธรรมความปลอดภัยไซเบอร์ของภาครัฐ

แม้เทคโนโลยีจะพัฒนาอย่างรวดเร็ว ผลการวิจัยยืนยันตรงกันว่า ปัจจัยมนุษย์ยังเป็นความเสี่ยง สำคัญที่สุด โดยรายงานระบุว่ากว่า 90% ของเหตุการณ์ไซเบอร์มีสาเหตุจากความผิดพลาดของผู้ใช้ (IBM Security, 2023) โดยเฉพาะในภาครัฐที่มีบุคลากรจำนวนมากและหลากหลายระดับทักษะ

ดังนั้น การบริหารความเสี่ยงไซเบอร์ที่มีประสิทธิภาพจึงต้องให้ความสำคัญกับการสร้าง วัฒนธรรมความปลอดภัยไซเบอร์ ผ่านการฝึกอบรม การสื่อสารเชิงนโยบาย การจำลองสถานการณ์ และการ ปลุกฝังความรับผิดชอบร่วม ซึ่งสอดคล้องกับข้อเสนอของ World Economic Forum (2024) ที่มองว่า “มนุษย์” ไม่ได้เป็นเพียงจุดอ่อน แต่เป็นด่านป้องกันแรกของความมั่นคงไซเบอร์

3. ช่องว่างองค์ความรู้ (Research Gap)

จากการทบทวนวรรณกรรมพบว่า แม้การศึกษาด้านความมั่นคงไซเบอร์และการจัดการความเสี่ยง ไซเบอร์จะได้รับความสนใจเพิ่มขึ้นอย่างต่อเนื่องในยุค Digital Disruption แต่ยังปรากฏช่องว่างองค์ความรู้สำคัญ หลายประการที่ยังไม่ได้รับการศึกษาอย่างครอบคลุม โดยเฉพาะในบริบทภาครัฐ ซึ่งสะท้อนข้อจำกัดของงานวิจัย กระแสหลักที่เน้นมุมมองเชิงเทคนิคมากกว่ามิติทางมนุษย์ องค์กร และสังคม

ประการแรก งานวิจัยส่วนใหญ่ยังมุ่งเน้นการจัดการความเสี่ยงไซเบอร์ในเชิงเทคนิค เช่น การพัฒนา โครงสร้างพื้นฐานด้านความปลอดภัย ระบบตรวจจับภัยไซเบอร์ อัลกอริทึมการวิเคราะห์ข้อมูล หรือการนำกรอบ มาตรฐานด้านเทคโนโลยีสารสนเทศมาใช้ในองค์กร ขณะที่การศึกษาเกี่ยวกับพฤติกรรมมนุษย์ ปัจจัยด้านจิตวิทยา องค์กร ความเชื่อ ความเข้าใจ และแรงจูงใจของผู้ใช้ ซึ่งเป็นสาเหตุหลักของเหตุการณ์ไซเบอร์ กลับได้รับความ สนใจในเชิงวิชาการค่อนข้างจำกัด ทั้งที่รายงานของ IBM Security (2023) ระบุว่า มากกว่าร้อยละ 90 ของ เหตุการณ์ข้อมูลรั่วไหลมีสาเหตุจากความผิดพลาดของมนุษย์ ช่องว่างดังกล่าวชี้ให้เห็นความจำเป็นในการพัฒนา

องค์ความรู้ที่บูรณาการแนวคิดด้านจิตวิทยาองค์กร พฤติกรรมผู้ใช้ และวัฒนธรรมดิจิทัล เข้ากับการจัดการความเสี่ยงไซเบอร์อย่างเป็นระบบ

ประการที่สอง ยังขาดกรอบแนวคิดและงานวิจัยที่อธิบายความเสี่ยงไซเบอร์ในฐานะ “ความเสี่ยงมหภาค” (Macro Risk) ที่ส่งผลข้ามมิติ ทั้งด้านเศรษฐกิจ ความมั่นคงของรัฐ คุณภาพบริการสาธารณะ และความเชื่อมั่นของประชาชน แม้ World Economic Forum (2024) จะเน้นย้ำว่า ภัยไซเบอร์ได้พัฒนาเกินกว่าประเด็นด้านไอทีไปสู่ความเสี่ยงเชิงโครงสร้างของระบบเศรษฐกิจและสังคมโลก แต่งานวิจัยจำนวนมากยังวิเคราะห์ในระดับองค์กรหรือหน่วยงานเดียว และไม่ครอบคลุมผลกระทบเชิงระบบนิเวศดิจิทัลของประเทศ เช่น ความเหลื่อมล้ำทางดิจิทัล สิทธิข้อมูลส่วนบุคคล หรือความเปราะบางของบริการภาครัฐที่มีความสำคัญต่อชีวิตประชาชน ช่องว่างดังกล่าวสะท้อนความจำเป็นในการพัฒนารอบทฤษฎีที่เชื่อมโยงรัฐศาสตร์ เศรษฐศาสตร์ สังคมวิทยา และ Cybersecurity เข้าด้วยกัน

ประการที่สาม ความสัมพันธ์เชิงเหตุและผลระหว่าง Digital Disruption ซึ่งครอบคลุมเทคโนโลยีเกิดใหม่ เช่น AI, Big Data Analytics, IoT, Cloud Computing และ Blockchain with ระดับ Cyber Resilience ขององค์กร โดยเฉพาะในภาครัฐ ยังได้รับการศึกษาอย่างจำกัด งานวิจัยส่วนใหญ่มีลักษณะเชิงพรรณนา (Descriptive Studies) หรือกรณีศึกษาเชิงอธิบาย มากกว่างานเชิงทฤษฎีหรือเชิงประจักษ์ที่สามารถทดสอบความสัมพันธ์เชิงสาเหตุ บทบาทของปัจจัยตัวกลาง และผลลัพธ์ เชิงนโยบายอย่างเป็นระบบ ทั้งที่ Digital Transformation ถูกมองว่าเป็นทั้งกลไกขับเคลื่อนนวัตกรรมและแหล่งสร้างความเสี่ยงใหม่ หากขาดการบริหารจัดการที่เหมาะสมอาจบั่นทอนเสถียรภาพของรัฐ ในระยะยาว (World Economic Forum, 2024) ช่องว่างนี้จึงเปิดโอกาสในการพัฒนางานวิจัยเชิงทดลอง การศึกษาเชิงระยะยาว (Longitudinal Studies) และแบบจำลองเชิงพยากรณ์เพื่ออธิบายพลวัตของความเสี่ยงไซเบอร์ในยุคดิจิทัล

ประการที่สี่ บริบทภาครัฐยังเป็นพื้นที่ที่ได้รับการศึกษาอย่างจำกัดเมื่อเทียบกับภาคเอกชน ทั้งที่ภาครัฐมีลักษณะเฉพาะแตกต่างอย่างชัดเจน ไม่ว่าจะเป็นพันธกิจด้านสาธารณะ โครงสร้างราชการแบบลำดับชั้น ข้อจำกัดด้านงบประมาณ ความรับผิดชอบต่อประชาชน และกรอบกฎหมายที่ซับซ้อน งานวิจัยด้านความมั่นคงไซเบอร์จำนวนมากยังอาศัยข้อมูลจากองค์กรเอกชนหรืออุตสาหกรรมเทคโนโลยี ซึ่งไม่สามารถสะท้อนความท้าทายด้านธรรมาภิบาลดิจิทัล นโยบายสาธารณะ และความไว้วางใจของประชาชนที่ภาครัฐต้องเผชิญได้อย่างครบถ้วน

ประการสุดท้าย ยังขาดงานวิจัยเชิงเปรียบเทียบนโยบายไซเบอร์ระดับประเทศ (comparative cyber governance) ที่สามารถอธิบายเหตุปัจจัยเชิงสถาบัน วัฒนธรรมการบริหาร ความโปร่งใส และทุนมนุษย์ที่ทำให้บางประเทศสามารถสร้าง Cyber Resilience ได้ดีกว่าประเทศอื่น แม้จะมีระดับเทคโนโลยีใกล้เคียงกัน ช่องว่างนี้เป็นข้อจำกัดสำคัญต่อการออกแบบนโยบายสาธารณะด้านความมั่นคงไซเบอร์ในบริบทประเทศกำลังพัฒนา

โดยสรุป ช่องว่างองค์ความรู้ที่สำคัญสะท้อนว่า งานวิจัยด้านความเสี่ยงไซเบอร์ยังต้องขยายกรอบการวิเคราะห์จากมิติเทคโนโลยีไปสู่มิติทางมนุษย์ องค์กร นโยบาย และสังคมอย่างบูรณาการ งานวิจัยในอนาคตจึงควรมุ่งพัฒนาโมเดลการจัดการความเสี่ยงเชิงคาดการณ์ (Predictive Risk Management) กรอบการกำกับดูแลเชิงระบบนิเวศ (Ecosystem-based Governance) การศึกษาเชิงสาเหตุในระยะยาว และองค์ความรู้ด้าน

พฤติกรรม ซึ่งจะมีบทบาทสำคัญในการเสริมสร้าง Cyber Resilience ของภาครัฐในยุค Digital Disruption อย่างยั่งยืน

สรุป อภิปรายผลการวิจัย และข้อเสนอแนะ

การอภิปรายผลการวิจัยโดยสรุป วิเคราะห์ และตีความผลลัพธ์เชิงวิชาการ พร้อมเชื่อมโยงกับวรรณกรรมที่เกี่ยวข้อง แนวคิดเชิงทฤษฎี และบริบทการบริหารความมั่นคงไซเบอร์ในภาครัฐภายใต้สภาวะ Digital Disruption ผลการอภิปรายชี้ให้เห็นถึงความสำคัญขององค์ประกอบการจัดการความเสี่ยงไซเบอร์ที่มีต่อการเสริมสร้างระดับความยืดหยุ่นทางดิจิทัลขององค์กรภาครัฐ

นอกจากนี้ ยังเสนอข้อเสนอแนะเชิงนโยบายและแนวทางเชิงปฏิบัติสำหรับการพัฒนาระบบบริหารความมั่นคงไซเบอร์ของภาครัฐให้มีประสิทธิภาพยิ่งขึ้น รวมถึงระบุข้อจำกัดของการวิจัยและแนวทางการศึกษาในอนาคตเพื่อขยายองค์ความรู้ในประเด็นดังกล่าว

1. สรุปผลการวิจัย

การวิจัยนี้มีวัตถุประสงค์หลักสองประการ ได้แก่ (1) เพื่อสังเคราะห์องค์ประกอบแนวคิดการจัดการความเสี่ยงไซเบอร์ในภาครัฐ และ (2) เพื่อศึกษาความเชื่อมโยงระหว่าง Digital Disruption กับ Cyber Resilience ของภาครัฐโดยใช้ระเบียบวิธีวิจัยเชิงเอกสารจากวรรณกรรมวิชาการสากล มาตรฐานด้านความมั่นคงไซเบอร์ และรายงานเชิงนโยบายระดับนานาชาติ

ผลการวิจัยพบว่า แนวคิดการจัดการความเสี่ยงไซเบอร์ในภาครัฐเป็นกระบวนการเชิงระบบที่ต้องอาศัยการบูรณาการหลายมิติ มิใช่เพียงการใช้มาตรการหรือเครื่องมือทางเทคนิค โดยสามารถสังเคราะห์องค์ประกอบหลักได้ 7 ประการ ได้แก่

- 1) การกำกับดูแลและนโยบายไซเบอร์
- 2) การระบุและประเมินความเสี่ยง
- 3) มาตรการป้องกัน
- 4) ระบบตรวจจับและเฝ้าระวัง
- 5) การตอบสนองเหตุการณ์และการฟื้นฟู
- 6) ปัจจัยมนุษย์และวัฒนธรรมองค์กร
- 7) ความยืดหยุ่นทางดิจิทัล



ภาพที่ 1 องค์ประกอบการจัดการความเสี่ยงไซเบอร์ภาครัฐไทย

ที่มา: ผู้วิจัยสังเคราะห์จาก NIST (2024), ISO 31000:2018, ISO/IEC 27005:2022, COBIT 2019, และ World Economic Forum (2022)

ผลการสังเคราะห์เชิงบริบทชี้ให้เห็นว่า Digital Disruption จากการนำเทคโนโลยี เช่น Cloud Computing, IoT, AI, Big Data และ Blockchain มาใช้ในภาครัฐ ได้เปลี่ยนลักษณะของความเสี่ยงไซเบอร์จากปัญหาทางเทคนิคของฝ่ายเทคโนโลยีสารสนเทศไปสู่ “ความเสี่ยงเชิงยุทธศาสตร์ของรัฐ” ที่ส่งผลกระทบต่อเศรษฐกิจ สังคม ความเชื่อมั่นของประชาชน และความมั่นคงระดับชาติ (World Economic Forum, 2024; ISO/IEC 27001, 2022; ISACA, 2019; IBM Security, 2023)

นอกจากนี้ ผลการวิจัยยังพบว่า ความเสี่ยงไซเบอร์ของภาครัฐมีลักษณะเป็น Shared Risk เนื่องจากระบบราชการดิจิทัลทำงานแบบเชื่อมโยงเป็น Ecosystem ผ่านแพลตฟอร์มข้อมูลกลาง ผู้ให้บริการเทคโนโลยีภายนอก และห่วงโซ่อุปทานดิจิทัล ทำให้ช่องโหว่ในหน่วยงานใดหน่วยงานหนึ่งสามารถส่งผลกระทบแบบลูกโซ่ต่อทั้งระบบรัฐได้ การบริหารความเสี่ยงแบบรายองค์กรจึงไม่เพียงพออีกต่อไป จำเป็นต้องยกระดับสู่การจัดการความมั่นคงไซเบอร์แบบบูรณาการระดับประเทศ

ในมิติของแนวคิดการบริหาร ผลการวิจัยสะท้อนการเปลี่ยนผ่านจากการจัดการความเสี่ยงเชิงรับ (reactive) ไปสู่เชิงรุก (proactive) และเชิงพยากรณ์ (predictive) โดยใช้ข้อมูลและ AI วิเคราะห์แนวโน้มภัยล่วงหน้า ซึ่งมีบทบาทสำคัญต่อการเสริมสร้าง Cyber Resilience ของภาครัฐ ทั้งนี้ ผลการสังเคราะห์ยังยืนยันว่า “ปัจจัยมนุษย์” เป็นตัวแปรชี้ขาดระดับความเสี่ยงไซเบอร์ เนื่องจากพฤติกรรม ความตระหนักรู้ และวัฒนธรรมองค์กรมีผลโดยตรงต่อความปลอดภัยของระบบ แม้จะมีเทคโนโลยีที่ทันสมัยก็ตาม

สำหรับบริบทประเทศไทย ผลการวิจัยพบว่า การขับเคลื่อนรัฐบาลดิจิทัลและการใช้บริการภาครัฐออนไลน์อย่างแพร่หลาย ทำให้ความเสี่ยงไซเบอร์กลายเป็นประเด็นสำคัญด้านความมั่นคงควบคู่กับเศรษฐกิจและคุณภาพชีวิตประชาชน แม้ประเทศไทยจะมีกฎหมายสำคัญ เช่น พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์

พ.ศ. 2562 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แต่เหตุการณ์โจมตีไซเบอร์ที่เกิดขึ้นยังสะท้อนความท้าทายด้านนโยบาย โครงสร้าง บุคลากร และวัฒนธรรมองค์กรรัฐ ตัวอย่างการอภิปราย เช่น ผลการวิจัยที่พบว่า "การกำกับดูแลและนโยบาย" เป็นองค์ประกอบสำคัญที่สุด สอดคล้องกับงานวิจัยของธัญวรัตน์ คงนุ่น (2568) ที่พบว่า การสนับสนุนจากผู้บริหารเป็นปัจจัยสำคัญต่อการพัฒนาวัฒนธรรมความเสี่ยงขององค์กรภาครัฐ และสอดคล้องกับงานของ Al-Nimer et al. (2021) ที่เสนอว่าการกำกับดูแลโดยผู้บริหารระดับสูงมีอิทธิพลต่อประสิทธิภาพของการบริหารความเสี่ยงองค์กร นอกจากนี้ยังสอดคล้องกับ COSO ERM (2017) และ ISO/IEC 27001 (2022) ที่กำหนดให้ภาวะผู้นำและการกำกับดูแลเป็นรากฐานของระบบบริหารความมั่นคงปลอดภัยไซเบอร์

ด้านบุคลากรและวัฒนธรรมองค์กร ผลการวิจัยสอดคล้องกับ IBM Security (2023) ที่พบว่าความผิดพลาดของมนุษย์เป็นสาเหตุสำคัญของเหตุการณ์ไซเบอร์ และสอดคล้องกับงานของ Da Veiga และ Martins (2015) ที่เสนอว่าการสร้างวัฒนธรรมความมั่นคงปลอดภัยสารสนเทศเป็นปัจจัยสำคัญต่อการลดความเสี่ยงไซเบอร์ อย่างไรก็ตาม ผลการวิจัยครั้งนี้ขยายองค์ความรู้เดิมโดยเสนอว่าการพัฒนาวัฒนธรรมความมั่นคงไซเบอร์ของภาครัฐไทยจำเป็นต้องเชื่อมโยงกับระบบธรรมาภิบาล การพัฒนาศักยภาพบุคลากร และการเรียนรู้ขององค์กร จึงจะนำไปสู่การสร้างความยืดหยุ่นทางไซเบอร์ (Cyber Resilience) ได้อย่างยั่งยืน

โดยสรุป งานวิจัยนี้ได้สังเคราะห์แนวคิดและองค์ประกอบของการจัดการความเสี่ยงไซเบอร์ภาครัฐไทยภายใต้แรงกดดันของ Digital Disruption และเสนอกรอบแนวคิดเชิงระบบที่มองความมั่นคงไซเบอร์ในฐานะกลไกการบริหารรัฐกิจและความมั่นคงของประเทศ มิใช่เพียงประเด็นทางเทคนิค

2. อภิปรายผล

ผลการวิจัยสะท้อนให้เห็นว่า การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์มิได้เป็นเพียงประเด็นด้านเทคโนโลยีสารสนเทศ แต่เป็นประเด็นเชิงยุทธศาสตร์ของการกำกับดูแลองค์กร (Cyber Governance) ซึ่งผู้บริหารระดับสูงต้องมีบทบาทในการกำหนดนโยบาย ทิศทาง และการจัดสรรทรัพยากรเพื่อสนับสนุนการบริหารความเสี่ยงไซเบอร์ ผลการศึกษาสอดคล้องกับกรอบ ISO/IEC 27001 (ISO, 2022) ที่กำหนดให้ผู้บริหารสูงสุดแสดงภาวะผู้นำและความมุ่งมั่นต่อระบบบริหารความมั่นคงสารสนเทศ และสอดคล้องกับ COBIT 2019 (ISACA, 2019) ที่มองว่าการกำกับดูแลด้านไซเบอร์เป็นความรับผิดชอบของคณะผู้บริหารและคณะกรรมการองค์กร ไม่ใช่หน้าที่เฉพาะของฝ่ายเทคโนโลยีสารสนเทศ ทั้งยังสอดคล้องกับแนวคิด Enterprise Risk Management ของ COSO (2017) ที่เสนอว่าความเสี่ยงควรถูกบูรณาการเข้ากับการกำหนดกลยุทธ์และการตัดสินใจขององค์กร

ผลการวิจัยยังแสดงให้เห็นว่า Digital Disruption ได้เปลี่ยนลักษณะของความเสี่ยงจากภัยไซเบอร์จากความเสี่ยงเชิงเทคนิค (Technical Risk) ไปสู่ความเสี่ยงเชิงระบบ (Systemic Risk) ที่เชื่อมโยงระหว่างหน่วยงาน เครือข่ายดิจิทัล และโครงสร้างพื้นฐานสำคัญของประเทศ สอดคล้องกับรายงานของ World Economic Forum (2024) ที่จัดให้ภัยไซเบอร์เป็นหนึ่งในความเสี่ยงระดับโลกที่ส่งผลกระทบต่อเศรษฐกิจ ความมั่นคง และความเชื่อมั่นของสังคม อย่างไรก็ตาม ผลการสังเคราะห์ของงานวิจัยนี้ขยายแนวคิดดังกล่าว โดยเสนอว่าบริบทของประเทศไทยมีความท้าทายเฉพาะจากการขับเคลื่อนรัฐบาลดิจิทัล ซึ่งทำให้การจัดการความเสี่ยงไซเบอร์

จำเป็นต้องบูรณาการทั้งด้านนโยบาย กฎหมาย การบริหารจัดการ และความร่วมมือระหว่างหน่วยงาน มากกว่าการพัฒนาแบบรักษาความมั่นคงสารสนเทศในระดับองค์กรเพียงอย่างเดียว

นอกจากนี้ ผลการวิจัยยังสะท้อนข้อจำกัดเชิงโครงสร้างของประเทศไทย ได้แก่ ความแตกต่างด้านงบประมาณ บุคลากร และศักยภาพด้านดิจิทัลระหว่างหน่วยงานส่วนกลางและองค์กรปกครองส่วนท้องถิ่น ซึ่งสอดคล้องกับข้อเสนอของ ISO (2022) และ World Economic Forum (2024) ที่ชี้ว่าความสำเร็จของการบริหารความเสี่ยงไซเบอร์ขึ้นอยู่กับความสามารถของระบบกำกับดูแลและการสนับสนุนเชิงสถาบัน มากกว่าการมีกฎหมายหรือมาตรฐานเพียงอย่างเดียว ผลการศึกษาจึงชี้ให้เห็นว่าการพัฒนาความมั่นคงไซเบอร์ของภาครัฐไทยจำเป็นต้องให้ความสำคัญกับการลดความเหลื่อมล้ำด้านศักยภาพระหว่างหน่วยงาน ควบคู่กับการสร้างกลไกสนับสนุนด้านองค์ความรู้ บุคลากร และงบประมาณอย่างเป็นระบบ

โดยสรุป องค์ความรู้ใหม่ที่ได้จากการวิจัยครั้งนี้ คือ การเสนอว่าการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ในบริบทภาครัฐไทยควรได้รับการพิจารณาในฐานะ "ระบบการกำกับดูแลเชิงบูรณาการ" (Integrated Cyber Risk Governance System) ซึ่งประกอบด้วยองค์ประกอบที่เชื่อมโยงกัน 7 ด้าน ได้แก่ (1) การกำกับดูแลและนโยบาย (2) การประเมินความเสี่ยง (3) มาตรการป้องกัน (4) การเฝ้าระวังและตรวจจับ (5) การตอบสนองและการฟื้นฟู (6) บุคลากรและวัฒนธรรมองค์กร และ (7) ความยืดหยุ่นดิจิทัล (Cyber Resilience) โดยองค์ประกอบเหล่านี้ไม่ได้ทำงานแยกส่วน แต่มีความสัมพันธ์เชิงพลวัตและสนับสนุนซึ่งกันและกัน การขาดองค์ประกอบใดองค์ประกอบหนึ่งย่อมส่งผลกระทบต่อประสิทธิภาพของระบบโดยรวม ดังนั้น การสร้างความมั่นคงไซเบอร์ของประเทศไทยจึงควรเปลี่ยนจากแนวคิดการป้องกันภัยไซเบอร์ (Cybersecurity) ไปสู่การสร้างความสามารถในการปรับตัว พื้นตัว และดำรงภารกิจของรัฐได้อย่างต่อเนื่องภายใต้ความไม่แน่นอนของยุค Digital Disruption หรือ Cyber Resilience ระดับประเทศ

3. ข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป

- 1) ศึกษาความสัมพันธ์เชิงสาเหตุระหว่าง Digital Disruption และ Cyber Resilience โดยใช้การวิจัยเชิงปริมาณ การวิเคราะห์โครงสร้างสมการ หรือการศึกษาแบบ longitudinal
- 2) วิจัยเชิงประจักษ์ด้านพฤติกรรมความเสี่ยงของบุคลากรภาครัฐ เพื่ออธิบายแรงจูงใจและปัจจัยเชิงจิตวิทยา
- 3) พัฒนาโมเดลการประเมินความเสี่ยงไซเบอร์ที่เหมาะสมกับบริบทประเทศไทย
- 4) ศึกษาความเหลื่อมล้ำด้านขีดความสามารถไซเบอร์ระหว่างหน่วยงานรัฐส่วนกลางและท้องถิ่น
- 5) วิเคราะห์ผลกระทบทางเศรษฐกิจและสังคมของเหตุการณ์ไซเบอร์ภาครัฐ
- 6) ศึกษาารูปแบบความร่วมมือรัฐ-เอกชน-พลเมืองด้านความมั่นคงไซเบอร์
- 7) วิจัยเชิงเปรียบเทียบนโยบายไซเบอร์ของประเทศไทยที่ประสบความสำเร็จ
- 8) พัฒนา Cybersecurity Readiness Index สำหรับภาครัฐไทย เพื่อใช้เป็นเครื่องมือกำกับเชิงนโยบายในระดับประเทศ

เอกสารอ้างอิง

- คงนุ่น, ธัญวรัตน์. (2568). ปัจจัยที่ส่งผลต่อความสำเร็จของการพัฒนาวัฒนธรรมความเสี่ยงขององค์กรภาครัฐ: กรณีศึกษาที่ว่าการอำเภอเมือง จังหวัดอุดรธานี. วารสารการจัดการและการพัฒนาท้องถิ่น มหาวิทยาลัยราชภัฏพิบูลสงคราม, 5(1), 17–27.
- นงลักษณ์ วิรัชชัย. (2541). *การวิจัยทางพฤติกรรมศาสตร์*. กรุงเทพมหานคร: จุฬาลงกรณ์มหาวิทยาลัย.
- Al-Nimer, M., Abbadi, S. S., Al-Omush, A., & Ahmad, H. (2021). Risk management practices and firm performance with a mediating role of business model innovation: Observations from Jordan. *Journal of Risk and Financial Management*, 14(3), 113.
- Aromataris, E., & Munn, Z. (Eds.). (2024). *JBİ manual for evidence synthesis*. Joanna Briggs Institute. <https://jbi-global.atlassian.net/wiki/spaces/MANUAL>
- Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management: Integrating with strategy and performance*. COSO.
- IBM Security. (2023). *Cost of a data breach report 2023*. IBM Corporation.
- International Organization for Standardization. (2022). *ISO/IEC 27001: Information security management systems*. ISO.
- ISACA. (2019). *COBIT 2019 framework: Governance and management objectives*. ISACA.
- Scott, J. (1990). *A matter of record: Documentary sources in social research*. Polity Press.
- WEF – World Economic Forum. (2024). *Global risks report 2024*. World Economic Forum