ข้อจำกัดทางกฎหมายเกี่ยวกับการกำกับดูแลประกันภัยไซเบอร์[1]

กฤติน ปานแจ่ม[2]

ในยุคเศรษฐกิจดิจิทัล ภัยคุกคามทางไซเบอร์ได้กลายเป็นความเสี่ยงเชิงระบบที่ทุกองค์กรต้องเผชิญ ทั้งการโจมตีเครือข่าย การล้วงข้อมูลส่วนบุคคล การเรียกค่าไถ่ระบบ หรือการทำให้ระบบไม่สามารถใช้งานได้ ความเสียหายจึงมิได้จำกัดเพียงมูลค่าทรัพย์สินที่สูญหาย แต่ลุกลามไปสู่ชื่อเสียง ความเชื่อมั่นของลูกค้า[3] และความรับผิดตามกฎหมายเฉพาะหลายฉบับ เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคล กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ เพื่อตอบสนองต่อความเสี่ยงเหล่านี้ ภาคธุรกิจได้พัฒนาผลิตภัณฑ์ประกันภัยไซเบอร์ขึ้นเพื่อถ่ายโอนความเสี่ยง ทั้งในมิติของค่าใช้จ่ายในการฟื้นฟูระบบ ตรวจสอบทางนิติวิทยาศาสตร์ การดำเนินคดี และความรับผิดต่อบุคคลภายนอก[4] อย่างไรก็ดี เมื่อพิจารณาภายใต้กรอบกฎหมายไทยที่มีอยู่กลับพบข้อจำกัดหลายประการที่ทำให้กลไกประกันภัยไซเบอร์ยังไม่สามารถทำหน้าที่รองรับความเสี่ยงยุคดิจิทัลได้อย่างมีประสิทธิภาพ

ประการแรก เรื่องหน้าที่เปิดเผยข้อความจริง กฎหมายไทยยังยึดหลัก “สุจริตอย่างยิ่ง” ตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 865 ซึ่งให้ผู้เอาประกันภัยต้องเปิดเผยข้อเท็จจริงอันเป็นสาระสำคัญทั้งหมด หากฝ่าฝืนแม้โดยไม่เจตนาก็อาจทำให้สัญญาตกเป็นโมฆียะและเปิดช่องให้ผู้รับประกันภัยบอกล้างสัญญาและปฏิเสธค่าสินไหมได้ หลักการดังกล่าวไม่สอดคล้องกับลักษณะภัยไซเบอร์ซึ่งมีความซับซ้อนทางเทคนิคสูง และผู้เอาประกันภัยจำนวนมากไม่มีความรู้เพียงพอที่จะจำแนกได้ว่าข้อเท็จจริงด้านเทคนิคใดเป็นสาระสำคัญที่ต้องเปิดเผย จึงเกิดภาวะที่ผู้เอาประกันภัยถูกบอกล้างสัญญาจากความไม่รู้มากกว่าความไม่สุจริต ตรงกันข้ามกับอังกฤษซึ่งได้ปรับฐานคิดมาใช้หลักหน้าที่ในการนำเสนอความเสี่ยงอย่างเป็นธรรม (Duty of Fair Presentation

---

[1] บทความนี้เรียบเรียงจากการค้นคว้าอิสระ เรื่อง ข้อจำกัดทางกฎหมายเกี่ยวกับการกำกับดูแลประกันภัยไซเบอร์ โดยมีอาจารย์ที่ปรึกษา คือ อาจารย์ ดร.พีรพงศ์ จงไพศาลสกุล และคณะกรรมการสอบ คือ รองศาสตราจารย์สุเมธ จานประดับ และผู้ช่วยศาสตราจารย์ ดร.สลิล สิรพิทูร

[2] นักศึกษาปริญญาโท หลักสูตรนิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยรามคำแหง

[3] European Union Agency for Cybersecurity (ENISA). **ENISA Threat Landscape 2021: Main Incidents and Threats.** [Online]. Available URL://https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021, 2025 (July, 19).

[4] Organisation for Economic Co-operation and Development (OECD). **Encouraging Clarity in Cyber Insurance Coverage**. [Online]. Available URL://https://web-archive.oecd.org/2020-08-18/546620-Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf, 2025 (July, 19).

of the Risk) โดยจำกัดภาระผู้เอาประกันภัยให้อยู่ในขอบเขตสิ่งที่ตนรู้หรือควรรู้อย่างสมเหตุสมผล และกำหนดหน้าที่สอบถามเพิ่มเติมไว้ที่ผู้รับประกันภัย[5] ขณะที่สิงคโปร์ แม้ยังคงหลักสุจริตอย่างยิ่ง แต่ Monetary Authority of Singapore (MAS)[6] และ Cyber Security Agency (CSA)[7] ได้พัฒนาแบบฟอร์มประเมินความเสี่ยงไซเบอร์และแนวทางปฏิบัติที่ช่วยลดภาระทางข้อมูลของผู้เอาประกันภัยและลดข้อพิพาทภายหลัง

ประการที่สอง เรื่องขอบเขตความคุ้มครองภัยไซเบอร์ ในกฎหมายไทยยังปราศจากมาตรฐานกลาง ทั้งในระดับกฎหมายหลักและกฎเกณฑ์ของสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) ทำให้บริษัทประกันสามารถกำหนดเงื่อนไขและข้อยกเว้นตามดุลพินิจของตนเอง ส่งผลให้เนื้อหากรมธรรม์ขาดเอกภาพและยากต่อความเข้าใจของผู้บริโภค ปัญหายิ่งทวีความซับซ้อนในกรณีความเสี่ยงไซเบอร์ที่แฝงอยู่ในกรมธรรม์ประกันภัยทั่วไปโดยไม่มีการระบุชัดเจน (Silent Cyber) ทำให้เกิดข้อพิพาทว่ากรมธรรม์ครอบคลุมเหตุการณ์โจมตีไซเบอร์หรือไม่[8] ในขณะที่อังกฤษพบว่าหน่วยงานด้านประกันภัย เช่น Lloyd's of London[9] และสมาคมผู้ประกอบธุรกิจประกันภัยของอังกฤษ (Association of British Insurers: ABI)[10] ได้กำหนดรายการความคุ้มครองขั้นต่ำไว้อย่างชัดเจน และสิงคโปร์ใช้แบบฟอร์มมาตรฐานและแนวทางการเปิดเผยเงื่อนไขความคุ้มครองอย่างโปร่งใส กลไกเชิงโครงสร้างเหล่านี้ช่วยลดความคลุมเครือและเสริมความเป็นธรรมในความสัมพันธ์ทางสัญญา

---

[5] Government of the United Kingdom. **Insurance Act 2015 (c. 4), Part 2: Duty of Fair Presentation**. [Online]. Available URL://https://www.legislation.gov.uk/ukpga/2015/4/part/2, 2025 (July, 19).

[6]Monetary Authority of Singapore. **Guidelines on Technology Risk Management (TRM).** [Online]. Available URL://https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines, 2025 (July, 19).

[7]Cyber Security Agency of Singapore. **Guide to Conducting Cybersecurity Risk Assessment for Critical Information Infrastructure**. [Online]. Available URL://https://www.csa.gov.sg/legislation/supplementary-references, 2025 (July, 19).

[8] Guy Carpenter. **Grappling With the Silent Cyber.** [Online]. Available URL://https://www.actuaries.org.sg/sites/default/files/2020-12/20112709ermSilentCyber.pdf, 2025 (July, 19).

[9]Lloyd's Market Association. **LMA20-031-PD: Cyber Risks Endorsements**. [Online]. Available URL://https://www.lmalloyds.com/LMA/LMA_Bulletins/LMA20-031-PD.aspx, 2025 (July, 19).

[10]Association of British Insurers. **Cyber Insurance Guide**. [Online]. Available URL://https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/cyber-insurance, 2025 (July, 19).

ประการที่สาม เรื่องการประเมินมูลค่าความเสียหายจากภัยไซเบอร์ ที่ยังขาดกรอบกฎหมายและมาตรฐานเฉพาะในประเทศไทย ทั้งที่ความเสียหายจากภัยไซเบอร์ส่วนใหญ่เป็นความเสียหายที่จับต้องไม่ได้ เช่น การสูญเสียข้อมูลสำคัญ ความเสียหายต่อชื่อเสียงทางธุรกิจ หรือความเชื่อมั่นของลูกค้า ซึ่งประเมินด้วยกรอบคิดเดิมที่เน้นทรัพย์สินที่มีมูลค่าชัดเจนได้ยาก ระบบปัจจุบันปล่อยให้การประเมินมูลค่าอยู่ภายใต้ดุลพินิจของผู้รับประกันภัยโดยไม่มีข้อกำหนดเรื่องผู้เชี่ยวชาญเฉพาะด้านหรือกรอบวิธีวิทยาเปรียบเทียบ ต่างจากอังกฤษที่จัดตั้งผู้ประเมินภัยไซเบอร์เฉพาะทางและใช้มาตรฐานข้อมูลร่วมเกี่ยวกับความเสี่ยงทางไซเบอร์มาใช้ (Cyber Exposure Data Schema) รวมถึงแนวทางจากหน่วยงานกำกับดูแลทางการเงินของอังกฤษอย่าง Financial Conduct Authority (FCA) ในการใช้แบบประเมินผลกระทบทางไซเบอร์มาตรฐาน[11] และสิงคโปร์ที่พัฒนาแนวทางการบริหารจัดการความเสี่ยงไซเบอร์และแบบจำลองต้นทุนเหตุการณ์ไซเบอร์เป็นเครื่องมือสนับสนุน[12]

เมื่อมองเชื่อมโยงทั้งสามประเด็นดังกล่าว จะเห็นได้ว่าข้อจำกัดของกฎหมายไทยยังไม่รองรับลักษณะเฉพาะของความเสี่ยงไซเบอร์ ทั้งในด้านภาระการเปิดเผยข้อมูล มาตรฐานขอบเขตความคุ้มครอง และกลไกการประเมินมูลค่าความเสียหาย การแก้ไขปัญหาจึงจำเป็นต้องเริ่มจากระดับสัญญารายฉบับไปสู่การออกแบบกรอบมาตรฐานกลาง แนวทางปฏิบัติ และกลไกกำกับดูแลที่ทำให้ตลาดประกันภัยไซเบอร์ของไทยสามารถทำหน้าที่เป็นเครื่องมือจัดการความเสี่ยงยุคดิจิทัลได้อย่างแท้จริงและเป็นธรรมต่อคู่สัญญาทั้งสองฝ่าย

1. ความหมายและลักษณะสำคัญของภัยไซเบอร์

ภัยไซเบอร์ (Cyber Threats) หมายถึง การกระทำที่ก่อให้เกิดอันตรายต่อระบบคอมพิวเตอร์ ข้อมูล หรือโครงสร้างพื้นฐานด้านสารสนเทศ โดยอาศัยการโจมตีผ่านเครือข่ายอินเทอร์เน็ตหรือเทคโนโลยีดิจิทัลอื่น ๆ กฎหมายไทยนิยามคำว่า “ภัยคุกคามทางไซเบอร์” ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ว่าเป็นการกระทำโดยมิชอบผ่านระบบคอมพิวเตอร์ที่มีลักษณะเป็นภยันตรายใกล้จะถึงและอาจส่งผลกระทบต่อการทำงานของระบบ[13] ส่วนในระดับสากลสถาบันมาตรฐานและเทคโนโลยีแห่งชาติของสหรัฐอเมริกา (National Institute of Standards and Technology: NIST) ให้ความหมายว่าเป็นเหตุการณ์ที่กระทบ

---

[11] Financial Conduct Authority. **Financial Services Cyber Incident Response Framework**. [Online]. Available URL://https://www.fca.org.uk/firms/cyber-resilience, 2025 (July, 19).

[12] Monetary Authority of Singapore. **Technology Risk Management Guidelines.** [Online]. Available URL://https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf, 2025 (July, 19).

[13] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, มาตรา 3.

ต่อความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลหรือระบบ ซึ่งเป็นกรอบแนวคิดพื้นฐานที่ใช้ประเมินความเสี่ยงทั่วโลก[14]

ลักษณะสำคัญของภัยไซเบอร์มีหลายประการ ได้แก่ (1) ความไม่แน่นอนสูง เนื่องจากรูปแบบการโจมตี เช่น แรนซัมแวร์ มีการพัฒนาอย่างต่อเนื่องและคาดการณ์ได้ยาก[15] (2) การข้ามพรมแดนและไร้เขตแดน เพราะความเชื่อมโยงของโครงข่ายอินเทอร์เน็ตทำให้เหตุการณ์ที่เกิดขึ้นในประเทศหนึ่งสามารถสร้างผลกระทบเป็นวงกว้างทั่วโลก ดังเช่นกรณี WannaCry และ NotPetya ในปี 2017[16] (3) ความยากในการสืบหาต้นตอ เนื่องจากผู้โจมตีใช้เครื่องมือปกปิดตัวตน เช่น Proxy, VPN และ Dark Web ทำให้การติดตามย้อนกลับเป็นไปโดยยาก (4) ผลกระทบที่กว้างและต่อเนื่อง ไม่เพียงก่อให้เกิดความสูญหายของข้อมูล แต่รวมถึงความเสียหายทางเศรษฐกิจ การหยุดชะงักของบริการสำคัญ และผลกระทบต่อสิทธิขั้นพื้นฐาน เช่น การถูกละเมิดข้อมูลส่วนบุคคล[17] และ (5) ความมีพลวัตสูง โดยภัยไซเบอร์พัฒนาไปสู่รูปแบบที่ซับซ้อนยิ่งขึ้น เช่น การโจมตีผ่านอีเมลธุรกิจ (Business Email Compromise: BEC) และการโจมตีห่วงโซ่อุปทาน (Supply Chain Attack) ซึ่งสร้างผลกระทบเป็นลูกโซ่ต่อองค์กรจำนวนมาก ดังเช่นกรณี SolarWinds ในปี 2020[18]

ด้วยคุณลักษณะเฉพาะเหล่านี้ ภัยไซเบอร์จึงเป็นความเสี่ยงที่แตกต่างจากความเสี่ยงแบบดั้งเดิมอย่างมีนัยสำคัญ การทำความเข้าใจความหมายและคุณลักษณะของภัยไซเบอร์จึงเป็นฐานสำคัญในการออกแบบกลไกกฎหมายและมาตรการจัดการความเสี่ยงที่มีประสิทธิภาพ โดยเฉพาะเครื่องมือประกันภัยไซเบอร์ ซึ่งทำหน้าที่เป็นกลไกถ่ายโอนความเสี่ยงในบริบทที่ภัยมีความไม่แน่นอนสูง ข้ามพรมแดน และมีศักยภาพในการก่อให้เกิดความเสียหายในวงกว้าง ทั้งต่อตลาด เศรษฐกิจ และโครงสร้างพื้นฐานสำคัญของรัฐ

---

[14] National Institute of Standards and Technology (NIST), **Computer Security Incident Handling Guide**, (Gaithersburg, MD: U.S. Department of Commerce, 2012), p.5.

[15] European Union Agency for Cybersecurity (ENISA), **ENISA Threat Landscape** [Online]. Available URL://https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf, 2025 (July, 19).

[16] อัศว์ณุต แสงทองดี และ ญาณพล ยั่งยืน, “แนวทางการรับมือและการรับแจ้งเหตุของตำรวจต่อกรณีมัลแวร์เรียกค่าไถ่,” **วารสารสหศาสตร์** 21, 1 (เมษายน 2564): 28.

[17] Ponemon Institute. **2014 Global Report on the Cost of Cyber Crime** [Online]. Available URL://https://www.ponemon.org/news-updates/blog/security/2014-global-report-on-the-cost-of-cyber-crime.html, 2025 (Sep, 27).

[18] Aggeliki Tsohou, Vasiliki Diamantopoulou, Stefanos Gritzalis, and Costas Lambrinoudakis. “Cyber Insurance: State of the Art, Trends and Future Directions,” **International Journal of Information Security** 22, 4 (2023):739.

2. ความเป็นมาของการประกันภัยไซเบอร์

การประกันภัยไซเบอร์ถือกำเนิดขึ้นช่วงปลายทศวรรษ 1990 ในฐานะคำตอบต่อความเสี่ยงรูปแบบใหม่ที่กรมธรรม์ประกันภัยทรัพย์สินและความรับผิดต่อบุคคลภายนอกในรูปแบบดั้งเดิมไม่อาจรองรับได้ โดยเฉพาะความเสียหายจากการรั่วไหลของข้อมูลและการโจมตีระบบสารสนเทศ ผลิตภัณฑ์กลุ่มแรกในสหรัฐอเมริกามักเริ่มจากความรับผิดต่อบุคคลภายนอกจากการละเมิดข้อมูล (Data breach liability)[19] และค่อย ๆ พัฒนาไปสู่กรมธรรม์ที่ครอบคลุมทั้งค่าใช้จ่ายในการฟื้นฟูระบบ ค่าเสียหายจากการหยุดชะงักทางธุรกิจ และค่าใช้จ่ายด้านการจัดการวิกฤติและการประชาสัมพันธ์

ในช่วงต้นทศวรรษ 2000 ภัยไซเบอร์มีพัฒนาการจากไวรัสและการบุกรุกระบบขั้นพื้นฐาน ไปสู่การโจมตีที่ซับซ้อนและเชื่อมโยงกับโครงสร้างพื้นฐานดิจิทัลของระบบเศรษฐกิจโดยรวม กรมธรรม์ประกันภัยไซเบอร์จึงขยายตัวจากเพียงเครื่องมือถ่ายโอนความเสี่ยงมาเป็นตัวกำกับมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศโดยปริยาย เนื่องจากผู้เอาประกันภัยที่ต้องการความคุ้มครองจำเป็นต้องปรับปรุงมาตรการป้องกันตามเงื่อนไขที่บริษัทประกันกำหนด เหตุการณ์โจมตีครั้งใหญ่ในปี ค.ศ. 2017 เช่น WannaCry และ NotPetya ยิ่งตอกย้ำให้เห็นว่า ภัยไซเบอร์สามารถสร้างความเสียหายเชิงระบบในวงกว้าง ทำให้ประกันภัยไซเบอร์ถูกยอมรับมากขึ้นในฐานะกลไกสำคัญเคียงคู่กับมาตรการป้องกันทางเทคนิค[20]

สำหรับประเทศไทย ตลาดประกันภัยไซเบอร์อยู่ในช่วงเติบโตตามการขยายตัวของของธุรกิจพาณิชย์อิเล็กทรอนิกส์ (E-commerce) และเทคโนโลยีทางการเงิน (Fintech) รวมทั้งการใช้อินเทอร์เน็ตและระบบคลาวด์ที่เพิ่มสูงขึ้น รายงานคาดการณ์แนวโน้มตลาดชี้ว่าประเทศไทยมีศักยภาพเติบโตในช่วงปี 2025–2033 อย่างไรก็ตาม โครงสร้างตลาดยังเผชิญข้อจำกัดหลายประการ[21] ทั้งความเสี่ยงจากเหตุการณ์ไซเบอร์เฮอริเคน (cyber hurricane) หรือการโจมตีขนาดใหญ่ที่กระทบหลายองค์กรพร้อมกัน การขาดข้อมูลสถิติสำหรับการคำนวณเบี้ย

---

[19] Information Security Alliance (ISA). **Cyber-Insurance Metrics and Impact on Cyber-Security** [Online]. Available URL://https://obamawhitehouse.archives.gov/files/documents/cyber/ISA%20-%20Cyber-Insurance%20Metrics%20and%20Impact%20on%20Cyber-Security.pdf, 2025 (Sep, 27).

[20] Aggeliki Tsohou, Vasiliki Diamantopoulou, Stefanos Gritzalis, and Costas Lambrinoudakis. “Cyber Insurance: State of the Art, Trends and Future Directions,” **International Journal of Information Security** 22, 4 (2023):737.

[21] IMARC Group. **Thailand Cyber Insurance Market Size, Share and Trends 2025–2033** [Online]. Available URL://https://www.imarcgroup.com/thailand-cyber-insurance-market, 2025 (Sep, 27).

ประกันภัย[22] และปัญหา Silent Cyber ในกรมธรรม์ประกันภัยทั่วไปที่มิได้กำหนดเงื่อนไขเกี่ยวกับภัยไซเบอร์อย่างชัดเจน เนื่องจากภัยไซเบอร์เป็นความเสี่ยงที่ยังใหม่และมีความไม่แน่นอนสูง ส่งผลให้เกิดปัญหาข้อมูลข่าวสารที่ไม่ถูกต้องและได้สัดส่วนระหว่างผู้เอาประกันภัยกับบริษัทประกัน[23]

ในทางกฎหมาย ประกันภัยไซเบอร์สามารถจัดวางอยู่ในกลุ่มการประกันภัยเกี่ยวกับทรัพย์ โดยครอบคลุมวัตถุที่มีรูปร่างและไม่มีรูปร่าง หากทรัพย์หรือสิทธิทางดิจิทัลถูกทำลาย สูญหาย หรือก่อให้เกิดความรับผิดในทางแพ่ง ย่อมถือเป็นความสูญเสียทางการเงินที่อาจเอาประกันภัยได้[24] แต่ความเสี่ยงดิจิทัลในปัจจุบันเผยให้เห็นช่องโหว่เชิงโครงสร้างของตลาดและกฎหมายที่ยังไม่มีฐานข้อมูลและกลไกกำกับดูแลร่วมกันอย่างเพียงพอ พัฒนาการของประกันภัยไซเบอร์จึงมิใช่เพียงปรากฏการณ์ทางธุรกิจ หากยังสะท้อนการเปลี่ยนผ่านของกฎหมายสู่การรองรับความเสี่ยงเชิงระบบในโลกดิจิทัล

3. ประเภทของการประกันภัยไซเบอร์และขอบเขตความคุ้มครอง

ความคุ้มครองตามกรมธรรม์ประกันภัยไซเบอร์แบ่งได้ออกเป็น 3 ประเภท คือ (1) ความคุ้มครองต่อความเสียหายโดยตรง (first-party) (2) ความคุ้มครองต่อความรับผิดต่อบุคคลภายนอก (third-party) และ (3) การคุ้มครองแบบระบุชัดกับการคุ้มครองแบบแฝง (explicit and silent cyber)

3.1 ความคุ้มครองต่อความเสียหายโดยตรง

ความคุ้มครองต่อความเสียหายโดยตรงเป็นแกนหลักของประกันภัยไซเบอร์ เนื่องจากมุ่งเยียวยาความเสียหายที่เกิดขึ้นกับผู้เอาประกันภัยโดยตรง ไม่ว่าจะเป็นการสูญหายหรือถูกเข้ารหัสข้อมูล การถูกมัลแวร์หรือแรนซัมแวร์โจมตี การหยุดชะงักของระบบงาน หรือค่าใช้จ่ายในการฟื้นฟูระบบให้กลับมาใช้งานได้ตามปกติ โดยทั่วไป ความคุ้มครองลักษณะนี้ครอบคลุมค่าใช้จ่ายด้านการสืบสวนเหตุการณ์ทางเทคนิค (forensic) การกู้

[22] Information Security Alliance (ISA). **Cyber-Insurance Metrics and Impact on Cyber-Security** [Online]. Available URL://https://obamawhitehouse.archives.gov/files/documents/cyber/ISA%20-%20Cyber-Insurance%20Metrics%20and%20Impact%20on%20Cyber-Security.pdf, 2025 (Sep, 27).

[23] ศศิธร จิตรประเสริฐ, “โอกาสในการซื้อประกันภัยไซเบอร์ส่วนบุคคล:กรณีศึกษาของประกันภัยไซเบอร์ส่วนบุคคล” (วิทยานิพนธ์เศรษฐศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์, 2566), หน้า 2–5.

[24] สิทธิโชค ศรีเจริญ, **หลักกฎหมายประกันภัย.** (กรุงเทพฯ: สำนักพิมพ์วิญญูชน, 2561), 55.

คืนข้อมูล การสูญเสียรายได้จากการหยุดชะงักทางธุรกิจ และในหลายกรณียังรวมถึงค่าไถ่จากการโจมตีแรนซัมแวร์ด้วย[25]

อย่างไรก็ดี ความคุ้มครองต่อความเสียหายโดยตรงยังเผชิญข้อจำกัดด้านการตีความหลายประการ เช่น ขอบเขตของความเสียหายว่าจะครอบคลุมข้อมูลเชิงพาณิชย์หรือความลับทางธุรกิจเพียงใด ปัญหาความเสียหายที่สืบเนื่องยาวนานซึ่งยากต่อการระบุจุดเริ่มต้นของเหตุการณ์ รวมทั้งประเด็นวิธีพิสูจน์และประเมินมูลค่าความเสียหายที่ไม่มีตัวตนอย่างแน่นอน หากไม่มีเงื่อนไขกรมธรรม์ที่ชัดเจนและกลไกพิสูจน์ความเสียหายที่น่าเชื่อถือ ความคุ้มครองประเภทนี้อาจไม่สามารถตอบสนองความต้องการของผู้เอาประกันภัยได้อย่างเต็มที่

3.2 ความคุ้มครองต่อความรับผิดต่อบุคคลภายนอก

นอกเหนือจากการเยียวยาความเสียหายของผู้เอาประกันภัยเอง การประกันภัยไซเบอร์ยังครอบคลุมความรับผิดต่อบุคคลภายนอกซึ่งเกิดจากเหตุการณ์ไซเบอร์ที่มีต้นทางจากระบบของผู้เอาประกันภัย เช่น การรั่วไหลของข้อมูลส่วนบุคคลของลูกค้า การละเมิดความเป็นส่วนตัว การทำให้ระบบของคู่ค้าเสียหาย หรือการฝ่าฝืนกฎหมายเกี่ยวกับข้อมูลส่วนบุคคลและความมั่นคงปลอดภัยไซเบอร์

ความคุ้มครองลักษณะนี้มักครอบคลุมค่าใช้จ่ายทางกฎหมาย ค่าเสียหายตามคำพิพากษาหรือข้อตกลงยุติข้อพิพาท ตลอดจนค่าใช้จ่ายในการแจ้งเหตุแก่เจ้าของข้อมูลตามบทบัญญัติกฎหมาย เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศต่าง ๆ การที่องค์กรต้องเผชิญความเสี่ยงจากการถูกฟ้องร้องหรือเรียกร้องค่าสินไหมจำนวนมาก ทำให้ความคุ้มครองต่อบุคคลภายนอกเป็นองค์ประกอบที่ขาดไม่ได้ของประกันภัยไซเบอร์ในบริบทที่กฎหมายด้านข้อมูลส่วนบุคคลและความมั่นคงปลอดภัยมีแนวโน้มเข้มงวดขึ้นอย่างต่อเนื่อง

อย่างไรก็ดี ความคุ้มครองต่อความรับผิดต่อบุคคลภายนอกก็มีข้อจำกัดที่ต้องพิจารณา เช่น การยกเว้นกรณีการละเมิดทรัพย์สินทางปัญญา การเผยแพร่เนื้อหาที่ผิดกฎหมาย หรือการกระทำโดยเจตนาทุจริตของผู้บริหารหรือพนักงาน รวมทั้งความท้าทายในการประเมินความเสียหายที่ไม่เป็นตัวเงิน[26] เช่น ความเสียหายต่อชื่อเสียงหรือความไว้วางใจของสาธารณชน การลดความไม่แน่นอนดังกล่าวจำเป็นต้องอาศัยทั้งการกำหนด

---

[25] Information Security Alliance (ISA). **Cyber-Insurance Metrics and Impact on Cyber-Security** [Online]. Available URL://https://obamawhitehouse.archives.gov/files/documents/cyber/ISA%20-%20Cyber-Insurance%20Metrics%20and%20Impact%20on%20Cyber-Security.pdf, 2025 (Sep, 27).

[26] Aggeliki Tsohou, Vasiliki Diamantopoulou, Stefanos Gritzalis, and Costas Lambrinoudakis. “Cyber Insurance: State of the Art, Trends and Future Directions,” **International Journal of Information Security** 22, 4 (2023):740.

เงื่อนไขกรมธรรม์ที่รัดกุม และการพัฒนาบรรทัดฐานเชิงคำพิพากษาที่ชัดเจนเกี่ยวกับขอบเขตของความรับผิดต่อบุคคลภายนอกจากเหตุการณ์ไซเบอร์

3.3 การคุ้มครองแบบระบุชัด และการคุ้มครองแบบแฝง

การคุ้มครองแบบระบุชัด หมายถึง กรมธรรม์ที่กำหนดเงื่อนไขเกี่ยวกับภัยไซเบอร์ไว้อย่างชัดแจ้ง เช่น การคุ้มครองค่าใช้จ่ายในการแจ้งเหตุกรณีข้อมูลรั่วไหล การฟื้นฟูระบบไอที หรือการชำระค่าไถ่จากการโจมตีแรนซัมแวร์ ลักษณะนี้ช่วยให้ผู้เอาประกันภัยสามารถคาดหมายขอบเขตความคุ้มครองได้อย่างโปร่งใส ลดโอกาสเกิดข้อพิพาทเรื่องการตีความ และสอดคล้องกับแนวโน้มของหลายประเทศที่ผลักดันให้บริษัทประกันระบุความคุ้มครองหรือข้อยกเว้นภัยไซเบอร์ให้ชัดเจนในกรมธรรม์

ในทางกลับกัน การคุ้มครองแบบแฝง หรือที่เรียกว่า silent cyber หมายถึงกรณีที่ภัยไซเบอร์อาจถูกตีความว่าอยู่ภายใต้กรมธรรม์ประกันภัยประเภทอื่นที่มิได้ระบุไว้อย่างชัดเจนว่าจะคุ้มครองหรือยกเว้นภัยไซเบอร์ เช่น ประกันภัยทรัพย์สินหรือประกันภัยความรับผิดต่อบุคคลภายนอกทั่วไป ความไม่ชัดเจนเช่นนี้ทำให้เมื่อเกิดเหตุการณ์ไซเบอร์[27] ผู้เอาประกันภัยอาจอ้างสิทธิในความคุ้มครอง ขณะที่ผู้รับประกันภัยอาจโต้แย้งว่ากรมธรรม์ไม่ได้ถูกออกแบบมาเพื่อครอบคลุมความเสี่ยงดังกล่าวโดยเฉพาะ อันนำไปสู่ข้อพิพาทในการตีความสัญญาและเพิ่มความไม่แน่นอนในการจ่ายค่าสินไหม

สรุปได้ว่าประเภทของความคุ้มครองและลักษณะของการระบุภัยไซเบอร์ในกรมธรรม์สะท้อนให้เห็นว่า ประกันภัยไซเบอร์มิใช่เพียงผลิตภัณฑ์ใหม่ในตลาดประกันภัยเท่านั้น หากยังเป็นกลไกที่เชื่อมโยงโดยตรงกับการออกแบบโครงสร้างกฎหมายสัญญาประกันภัยและการกำกับดูแล เพื่อให้สามารถรองรับความเสี่ยงไซเบอร์ที่มีพลวัตและข้ามพรมแดนได้อย่างมีเสถียรภาพในระยะยาว

4. กฎหมายเกี่ยวกับการกำกับดูแลประกันภัยไซเบอร์ของประเทศไทย

กฎหมายไทยที่ใช้บังคับกับการประกันภัยไซเบอร์ในปัจจุบันยังไม่มีบทบัญญัติเฉพาะ จึงต้องพิจารณาจากกฎหมายที่มีอยู่ คือ ประมวลกฎหมายแพ่งและพาณิชย์ (ลักษณะประกันภัย) พระราชบัญญัติประกันวินาศภัย พ.ศ. 2535 และพระราชบัญญัติสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย พ.ศ. 2550 โดยมีสำนักงาน คปภ. เป็นกลไกหลักในการออกแบบแบบกรมธรรม์ มาตรฐานการกำกับ และการควบคุมดูแลตลาดประกันภัยโดยรวม ซึ่งกฎหมายเหล่านี้ออกแบบมาสำหรับประกันวินาศภัยแบบเดิมเป็นหลัก

[27] Information Security Alliance (ISA). **Cyber-Insurance Metrics and Impact on Cyber-Security** [Online]. Available URL://https://obamawhitehouse.archives.gov/files/documents/cyber/ISA%20-%20Cyber-Insurance%20Metrics%20and%20Impact%20on%20Cyber-Security.pdf, 2025 (Sep, 27).

เช่น ไฟไหม้ น้ำท่วม อุบัติเหตุทรัพย์สิน มากกว่าจะรองรับความเสี่ยงเชิงดิจิทัลที่มีลักษณะไร้รูปร่าง ซับซ้อนทางเทคนิค และมีพลวัตสูงอย่างภัยไซเบอร์

4.1 หลักเกณฑ์ว่าด้วยการเปิดเผยข้อความจริง

กฎหมายแพ่งและพาณิชย์วางสัญญาประกันภัยไว้บนหลัก “สุจริตอย่างยิ่ง” (utmost good faith) ในมาตรา 865 โดยกำหนดให้ผู้เอาประกันภัยมีหน้าที่เปิดเผยข้อเท็จจริงอันเป็นสาระสำคัญทั้งหมดที่ตนรู้หรือควรรู้ต่อผู้รับประกันภัย หากจงใจไม่เปิดเผย หรือแถลงข้อความเท็จ สัญญาย่อมตกเป็นโมฆียะ และผู้รับประกันภัยมีสิทธิบอกล้างสัญญาและปฏิเสธการจ่ายค่าสินไหมทดแทนได้[28] โดยโครงสร้างของมาตรา 865 ทำให้หน้าที่ที่สำคัญอยู่ที่ฝ่ายผู้เอาประกันภัย โดยถือว่าผู้เอาประกันภัยเป็นผู้รู้ข้อเท็จจริงเกี่ยวกับทรัพย์สินหรือความเสี่ยงที่จะเอาประกันภัยดีที่สุด ข้อเท็จจริงที่ต้องเปิดเผยต้องมีลักษณะเป็นข้อเท็จจริงอันเป็นสาระสำคัญ คือข้อเท็จจริงที่หากผู้รับประกันภัยทราบย่อมมีผลต่อการตัดสินใจว่าจะรับประกันภัยหรือไม่ หรือจะเรียกเบี้ยในอัตราใด

จากหลักดังกล่าว จำแนกหน้าที่ของผู้เอาประกันภัยออกเป็น (1) การเปิดเผยข้อความจริง (disclosure) ที่ต้องแจ้งข้อเท็จจริงสำคัญ แม้ผู้รับประกันภัยจะมิได้ถาม (2) การแถลงข้อความเท็จ (misrepresentation) ทั้งในกรณีตอบแบบฟอร์มและการให้ถ้อยคำทั่วไป และ (3) การปฏิบัติตาม คำรับรอง (warranties) ซึ่งเป็นข้อกำหนดที่ผู้เอาประกันภัยรับประกันว่าจะทำหรือไม่ทำอย่างใดอย่างหนึ่ง ทั้งก่อนและระหว่างอายุกรมธรรม์[29]

แม้หลักสุจริตอย่างยิ่งจะวางน้ำหนักภาระไว้ที่ฝ่ายผู้เอาประกันภัย แต่กฎหมายก็มิได้ให้อำนาจฝ่ายผู้รับประกันภัยโดยไม่จำกัด ในมาตรา 866 ได้กำหนดข้อยกเว้นของหน้าที่เปิดเผยข้อเท็จจริงไว้ เช่น กรณีที่ผู้รับประกันภัยรู้อยู่แล้วหรือควรจะรู้หากใช้ความระมัดระวังตามสมควร กรณีที่บริษัทมีโอกาสถามแต่ละเว้นไม่ถาม หรือข้อเท็จจริงที่ไม่ใช่สาระสำคัญหรือเป็นเรื่องที่รู้กันอยู่ทั่วไป ในกรณีเหล่านี้ การไม่เปิดเผยของผู้เอาประกันภัยไม่ส่งผลให้สัญญาตกเป็นโมฆียะ อย่างไรก็ดี เมื่อผู้เอาประกันภัยไม่ปฏิบัติตามหน้าที่ในการเปิดเผยข้อเท็จจริงอันเป็นสาระสำคัญตามที่บัญญัติไว้ในประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 865 ย่อมก่อให้เกิดผลทางกฎหมายต่อสัญญาประกันภัยโดยตรง โดยกฎหมายได้วางหลักเกณฑ์ไว้อย่างชัดเจนว่าการละเลยดังกล่าวไม่ว่าผู้เอาประกันภัยจะมีเจตนาหรือไม่ก็ตาม ถ้าได้มีการปกปิดหรือแถลงข้อความเท็จ เป็นเหตุให้สัญญา

---

[28] สิทธิโชค ศรีเจริญ, **หลักกฎหมายประกันภัย.** (กรุงเทพฯ: สำนักพิมพ์วิญญูชน, 2561), 23-24.

[29] ธีรยุทธ ปักษา, “ข้อยกเว้นความรับผิดของผู้รับประกันภัยในสัญญาประกันชีวิต,” **วารสารปาริชาต มหาวิทยาลัยทักษิณ** 6, 1 (2560): 124.

ประกันภัยตกเป็นโมฆียะ[30] โดยให้ผู้รับประกันภัยใช้สิทธิบอกล้างได้ภายในกำหนดเวลา และเมื่อบอกล้างแล้ว ผู้รับประกันภัยไม่ต้องรับผิดชดใช้ค่าสินไหมทดแทน

4.2 แนวทางการกำหนดความคุ้มครองและการตีราคาความเสียหาย

ความคุ้มครองตามสัญญาประกันภัยตั้งอยู่บนบทบัญญัติที่สำคัญ 3 มาตรา คือ

มาตรา 861 ให้นิยามสัญญาประกันภัยว่าเป็นสัญญาที่ผู้รับประกันภัยตกลงจะใช้เงินเมื่อเกิดเหตุไม่แน่นอนในอนาคต โดยผู้เอาประกันภัยชำระเบี้ยตอบแทน ทำให้เห็นองค์ประกอบร่วมคือ การโอนความเสี่ยงภาวะเหตุไม่แน่นอน และลักษณะการชดใช้ในฐานะค่าสินไหมทดแทน

มาตรา 867 กำหนดให้สัญญาประกันภัยต้องมีพยานหลักฐานเป็นหนังสือ และให้ระบุ รายการจำเป็นในกรมธรรม์ เช่น วัตถุที่เอาประกันภัย ภัยที่รับเสี่ยง จำนวนเงินเอาประกันภัย ระยะเวลาความคุ้มครอง และวิธีส่งเบี้ย เพื่อให้ขอบเขตคุ้มครองมีความแน่นอนและบังคับใช้ได้

มาตรา 869 ให้นิยามวินาศภัยว่าเป็นความเสียหายใด ๆ ที่อาจประมาณเป็นเงินได้ ซึ่งเป็นฐานสำคัญของการกำหนดประเภทความเสียหายที่อยู่ในขอบเขตความคุ้มครอง

ในส่วนของการชดใช้ค่าสินไหมทดแทน มาตรา 877 กำหนดให้ผู้รับประกันภัยรับผิดชดใช้เท่ากับจำนวนวินาศภัยจริง รวมถึงความบุบสลายจากการป้องปัดภัยและค่าใช้จ่ายสมควรในการรักษาทรัพย์ไม่ให้วินาศโดยให้ใช้ สถานที่และเวลาเกิดเหตุเป็นเกณฑ์การตีราคา และห้ามชดใช้เกินกว่า จำนวนเงินเอาประกันภัยที่ตกลงไว้ ขณะเดียวกัน มาตรา 878 กำหนดให้ภาระค่าใช้จ่ายในการตีราคาความเสียหายเป็นหน้าที่ของผู้รับประกันภัย และมาตรา 880 วางหลักการรับช่วงสิทธิ เมื่อผู้รับประกันภัยได้ชดใช้แทนแล้ว

โครงสร้างดังกล่าวสะท้อนรูปแบบของประกันวินาศภัยแบบเดิมที่ผูกความเสียหายเข้ากับทรัพย์สินที่มีมูลค่าเป็นเงินชัดเจน แต่เมื่อถูกนำมาใช้กับภัยไซเบอร์ ซึ่งความเสียหายจำนวนมากเป็นทรัพย์สินไม่มีรูปร่าง ข้อมูล ความลับทางการค้า หรือชื่อเสียงทางธุรกิจ ดังนั้น วิธีตีราคาความเสียหายไม่เป็นตัวเงินภายใต้กรอบมาตรา 869 และ 877 ที่ยังคิดด้วยฐานของวัตถุที่จับต้องได้เป็นหลัก

4.3 บทบาทของสำนักงาน คปภ. ในการกำกับดูแล

ในระดับกฎหมายเฉพาะ พระราชบัญญัติประกันวินาศภัย พ.ศ. 2535 ให้นายทะเบียน (คปภ.) มีบทบาทสำคัญในการกลั่นกรองแบบกรมธรรม์และอัตราเบี้ย โดยมาตรา 29 กำหนดให้แบบและข้อความในกรมธรรม์

---

[30] จิตติ ติงศภัทิย์ ปรับปรุงเพิ่มเติมโดยสิทธิโชค ศรีเจริญ, **กฎหมายแพ่งและพาณิชย์ว่าด้วยประกันภัย**, พิมพ์ครั้งที่ 18 (กรุงเทพฯ :สำนักพิมพ์วิญญชน, 2568), หน้า 62.ใ

ประกันวินาศภัย รวมทั้งเอกสารแนบท้าย ต้องได้รับความเห็นชอบจากนายทะเบียนก่อนนำมาใช้ และหากบริษัทใช้แบบหรือข้อความที่ไม่ตรงตามที่ได้รับความเห็นชอบ ผู้เอาประกันภัยหรือผู้รับประโยชน์มีสิทธิเลือกบังคับตาม (ก) ข้อความตามกรมธรรม์ที่ออกจริง (ข) ข้อความที่นายทะเบียนเคยอนุมัติ หรือ (ค) บอกเลิกสัญญาและเรียกคืนเบี้ยทั้งหมด ทั้งนี้ไม่กระทบต่อความผิดทางอาญาตามพระราชบัญญัติ

มาตรา 30 ในทำนองเดียวกัน บัญญัติให้อัตราเบี้ยที่บริษัทกำหนดต้องผ่านการให้ความเห็นชอบจากนายทะเบียน และเปิดโอกาสให้นายทะเบียนสั่งเปลี่ยนอัตราได้ โดยการเปลี่ยนแปลงดังกล่าวมีผลเฉพาะในอนาคต ไม่กระทบกรมธรรม์เดิม

ส่วนโครงสร้างของคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยและสำนักงาน คปภ. นั้นกำหนดไว้ในพระราชบัญญัติสำนักงาน คปภ. พ.ศ. 2550 มาตรา 6–8 และมาตรา 12 โดยที่มาตรา 6–8 วางโครงสร้างองค์คณะของคณะกรรมการ ประกอบด้วยกรรมการโดยตำแหน่งจากหน่วยงานเศรษฐกิจหลัก เช่น กระทรวงการคลัง ธปท. สคบ. ก.ล.ต. และกรรมการผู้ทรงคุณวุฒิจากสาขากฎหมาย การเงิน ประกันภัย ฯลฯ พร้อมทั้งกำหนดคุณสมบัติ ลักษณะต้องห้าม และวาระการดำรงตำแหน่ง เพื่อคุ้มครองความเป็นอิสระและความน่าเชื่อถือขององค์คณะกำกับ และมาตรา 12 มอบอำนาจให้คณะกรรมการกำหนดหลักเกณฑ์ วิธีการ เงื่อนไข และแนวปฏิบัติในการประกอบธุรกิจประกันภัยให้สอดคล้องมาตรฐานสากล กำกับ ส่งเสริม และพัฒนาธุรกิจประกันภัย ให้ความเห็นต่อรัฐมนตรีและคณะรัฐมนตรีในการออกกฎกระทรวง/ประกาศตามกฎหมายประกันภัย รวมทั้งกำกับดูแลสำนักงานในเชิงบริหาร กล่าวคือ กลไกกฎหมายประกันวินาศภัยและพระราชบัญญัติสำนักงานคปภ. กำหนดให้หน่วยงานกำกับดูแลของรัฐมีหน้าที่ในการกำหนดแบบกรมธรรม์ มาตรฐานอัตราเบี้ย และกติกาตลาด รวมทั้งมอบอำนาจกว้างในการออกประกาศและแนวนโยบาย

สำหรับประกันภัยไซเบอร์ หลักการที่รัฐเป็นผู้กำกับดูแลนี้จึงมีศักยภาพที่จะใช้เป็นฐานในการกำหนดมาตรฐานกลางว่าด้วยขอบเขตความคุ้มครอง เงื่อนไข Silent Cyber วิธีการประเมินความเสียหาย และแบบฟอร์มประเมินความเสี่ยงเฉพาะด้านไซเบอร์ได้ แต่ในทางปฏิบัติ ยังไม่มีประกาศหรือแนวทางเฉพาะที่ใช้รองรับความเสี่ยงไซเบอร์อย่างจริงจัง ทำให้บริษัทประกันกำหนดขอบเขตความคุ้มครองและมูลค่าความเสียหายได้ตามดุลพินิจภายใต้กรอบกฎหมายทั่วไป มากกว่าจะมีกลไกเชิงมาตรฐานที่ตอบรับลักษณะเฉพาะของภัยไซเบอร์โดยตรง

5. กฎหมายเกี่ยวกับการกำกับดูแลประกันภัยไซเบอร์ของประเทศอังกฤษ

กฎหมายของประเทศอังกฤษเกี่ยวกับการประกันภัยไซเบอร์สามารถมองได้ว่าเป็นต้นแบบของการปฏิรูปโครงสร้างกฎหมายประกันภัยเพื่อรองรับความเสี่ยงยุคดิจิทัล โดยเฉพาะผ่านพระราชบัญญัติประกันภัย พ.ศ. 2558 (Insurance Act 2015) และกลไกกำกับดูแลของ Financial Conduct Authority (FCA) และ Prudential

Regulation Authority (PRA) ซึ่งร่วมกันสร้างดุลยภาพระหว่างการคุ้มครองผู้เอาประกันภัย การบริหารความเสี่ยงของผู้รับประกันภัย และเสถียรภาพของตลาดประกันภัยไซเบอร์โดยรวม จากพัฒนาการสำคัญที่เริ่มจากกฎหมายเดิมภายใต้พระราชบัญญัติประกันภัยทางทะเล ค.ศ. 1906 (Marine Insurance Act 1906) ซึ่งวางหลัก “สุจริตอย่างยิ่ง” (utmost good faith) เป็นแกนกลางของสัญญาประกันภัย โดยกำหนดให้ผู้เอาประกันภัยต้องเปิดเผยข้อเท็จจริงอันเป็นสาระสำคัญทุกประการ มิฉะนั้นผู้รับประกันภัยมีสิทธิเลิกสัญญาได้ทั้งฉบับ ผลของหลักการนี้ทำให้ภาระก่อนทำสัญญาเอนเอียงไปอยู่ที่ฝ่ายผู้เอาประกันภัยอย่างเข้มข้น เมื่อบริบทของความเสี่ยงเปลี่ยนเป็นความเสี่ยงไซเบอร์ที่ซับซ้อนเชิงเทคนิคและเปลี่ยนแปลงเร็ว การกำหนดว่าอะไรคือข้อเท็จจริงสำคัญที่ต้องเปิดเผยจึงกลายเป็นภาระที่ไม่สมเหตุสมผล และอาจนำไปสู่ผลทางสัญญาที่รุนแรงเกินควร

ต่อมาพระราชบัญญัติประกันภัย พ.ศ. 2558 จึงเข้ามาปรับโครงสร้างใหม่ โดยตัดอำนาจเลิกสัญญาโดยอัตโนมัติเนื่องจากขาดความสุจริตอย่างยิ่ง[31] และวางหน้าที่การนำเสนอความเสี่ยงอย่างเป็นธรรม” (duty of fair presentation of the risk) เป็นหลักเกณฑ์กลางสำหรับสัญญาที่ไม่ใช่สัญญาผู้บริโภค หลักนี้กำหนดทั้ง (1) เนื้อหาที่ต้องเปิดเผย คือ ข้อเท็จจริงอันเป็นสาระสำคัญที่ผู้เอาประกันภัยรู้หรือควรรู้โดยสมเหตุสมผล และ (2) วิธีการนำเสนอที่ต้องชัดเจน เป็นระบบ ไม่คลุมเครือ และไม่ชวนให้เข้าใจผิด พร้อมทั้งยกเว้นข้อเท็จจริงบางประเภทที่ไม่จำเป็นต้องเปิดเผย เช่น เรื่องที่ลดความเสี่ยง หรือเรื่องที่ผู้รับประกันภัยรู้อยู่แล้ว[32] โดยกฎหมายยังวางกรอบอย่างละเอียดว่าผู้เอาประกันภัยรู้อะไรหรือพึงรู้อะไรซึ่งแยกเกณฑ์สำหรับบุคคลธรรมดาและนิติบุคคล และกำหนดให้ต้องสืบค้นข้อมูลภายในองค์กรและผู้ที่เกี่ยวข้องในระดับที่สมเหตุสมผล[33] ขณะเดียวกันก็จำกัดขอบเขตความรู้ของผู้รับประกันภัยเฉพาะบุคคลที่มีอำนาจตัดสินใจรับเสี่ยง และข้อมูลที่ควรถูกถ่ายทอดจนถึงมือผู้ตัดสินใจหรือเข้าถึงได้โดยง่าย หลักเหล่านี้ทำให้ขอบเขตหน้าที่เปิดเผยและหน้าที่สืบสวนของแต่ละฝ่ายสมดุล”มากกว่าระบบที่ใช้หลักสุจริตอย่างยิ่งแบบเดิม

ผลทางกฎหมายเมื่อมีการฝ่าฝืนหน้าที่ดังกล่าวก็ถูกปรับให้ได้สัดส่วน หากฝ่าฝืนโดยจงใจหรือประมาทเลินเล่ออย่างร้ายแรง ผู้รับประกันภัยสามารถเลิกสัญญา ปฏิเสธค่าสินไหม และยึดเบี้ยได้ แต่หากเป็นการฝ่าฝืนโดยไม่จงใจหรือไม่ร้ายแรง การเยียวยาจะขึ้นกับสิ่งที่ผู้รับประกันภัยจะทำ หากได้รับการนำเสนอความเสี่ยงอย่างถูกต้อง เช่น หากจะไม่รับประกันเลย ก็เพิกถอนสัญญาแต่คืนเบี้ยทั้งหมด หากจะรับแต่เปลี่ยนเงื่อนไข ก็ให้ถือว่าสัญญามีผลตามเงื่อนไขที่ควรเป็นแต่ต้น หรือหากจะเรียกเบี้ยสูงกว่า ก็ให้ลดค่าสินไหมตามสัดส่วนเบี้ยที่

[31] Insurance Act 2015 (UK), s.14.

[32] Insurance Act 2015 (UK), s.-7. (duty of fair presentation)

[33] Insurance Act 2015 (UK), s.44.

จ่ายจริงต่อเบี้ยที่ควรเรียก[34] กลไกนี้สะท้อนแนวคิดที่เน้นการปรับสิทธิหน้าที่ให้สอดคล้องกับระดับความเสียหายของการฝ่าฝืน มากกว่าการใช้มาตรการเลิกสัญญาแบบได้ทั้งหมดหรือไม่ได้เลย

ในด้านขอบเขตความคุ้มครองของประกันภัยไซเบอร์ให้ความสำคัญอย่างยิ่งกับการลดปัญหา Silent Cyber หรือการที่ความเสี่ยงไซเบอร์แฝงอยู่ในกรมธรรม์ประกันภัยทั่วไปโดยไม่ระบุชัดว่าให้ความคุ้มครองหรือไม่ ตลาดประกันผ่าน Lloyd's of London และสมาคมผู้ประกอบธุรกิจประกันภัย (Association of British Insurers: ABI) ได้ผลักดันให้มีการจัดทำกรมธรรม์ไซเบอร์เฉพาะ (standalone cyber policies)[35] และออกแนวปฏิบัติให้กรมธรรม์ทุกประเภทต้องระบุอย่างชัดแจ้งว่าครอบคลุมหรือยกเว้นความเสี่ยงไซเบอร์ ผลคือโครงสร้างของความคุ้มครองไซเบอร์ในอังกฤษมีแนวโน้มประกอบด้วย (1) ความคุ้มครองต่อความเสียหายโดยตรง เช่น การกู้คืนระบบ การสืบสวนทางเทคนิค และการหยุดชะงักของธุรกิจ (2) ความคุ้มครองต่อความรับผิดต่อบุคคลภายนอก และ (3) การกำหนดเงื่อนไข/ข้อยกเว้นเฉพาะ เช่น ข้อยกเว้นภัยสงครามไซเบอร์[36] ส่งผลให้โครงสร้างของสัญญามีความโปร่งใสกว่าการปล่อยให้ตีความจากกรมธรรม์ทั่วไป

ในด้านการประเมินมูลค่าความเสียหายจากภัยไซเบอร์ แม้พระราชบัญญัติประกันภัย พ.ศ. 2558 ไม่ได้บัญญัติเกณฑ์เฉพาะ แต่ตลาดอังกฤษได้พัฒนากลไกเสริม เช่น การใช้ผู้ประเมินภัยเฉพาะด้านไซเบอร์ (cyber loss adjusters)[37] การจัดทำมาตรฐานข้อมูลความเสี่ยงไซเบอร์ (Cyber Exposure Data Schema)[38] และการกำหนดให้กรมธรรม์ไซเบอร์ครอบคลุมค่าใช้จ่ายหลัก ได้แก่ ค่าใช้จ่ายทางเทคนิค ความเสียหายจากการหยุดชะงักของธุรกิจ และความรับผิดต่อบุคคลภายนอก อย่างไรก็ดี การตีราคาความเสียหายเชิงนามธรรม เช่น ชื่อเสียงหรือความเชื่อมั่นของลูกค้า และความเสี่ยงเชิงระบบที่กระทบหลายองค์กรพร้อมกัน ยังเป็นข้อจำกัดเชิงโครงสร้างที่ต้องอาศัยการพัฒนามาตรฐานและข้อมูลเพิ่มเติมอย่างต่อเนื่อง จะเห็นได้ว่ากฎหมายอังกฤษเกี่ยวกับการประกันภัยไซเบอร์มีลักษณะเป็นกรอบกำกับดูแลที่ปรับหลักสุจริตอย่างยิ่งให้เหมาะกับความเสี่ยงดิจิทัล วาง

---

[34] Insurance Act 2015 (UK), s.8(1)–(2) and Schedule 1, paras. 1–3

[35] Organisation for Economic Co-operation and Development (OECD). **Enhancing the Role of Insurance in Cyber Risk Management** (Paris: OECD Publishing, 2017), pp. 18–20.

[36] Organisation for Economic Co-operation and Development (OECD). **Enhancing the Role of Insurance in Cyber Risk Management** (Paris: OECD Publishing, 2017), pp. 20–23.

[37] Samantha Ward and Eleanor Matthews. **On the (Cyber) Attack: How Are the FCA and PRA Regulating Cyber Risk?** [Online]. Available URL://https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2023/11/on-the-cyber-attack.pdf, 2025 (Sep, 27).

[38] University of Cambridge Centre for Risk Studies. **Cyber Insurance Exposure Data Schema v1.0** [Online]. Available URL://https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-cyber-data-schema-v1.0.pdf, 2025 (Sep, 27).

หน้าที่การนำเสนอความเสี่ยงอย่างเป็นธรรมพร้อมมาตรการเยียวยาแบบสมส่วน กำหนดทิศทางให้ตลาดเพิ่มความโปร่งใสด้านความคุ้มครองไซเบอร์ และใช้กลไกกำกับดูแลทางการเงินเพื่อรองรับความเสี่ยงในตลาดประกันภัยไซเบอร์

6. กฎหมายเกี่ยวกับการกำกับดูแลประกันภัยไซเบอร์ของประเทศสิงคโปร์

กฎหมายประกันภัยไซเบอร์ของประเทศสิงคโปร์ยังไม่มีกฎหมายเฉพาะแบบเดียวกับกฎหมายประกันภัยไซเบอร์ แต่ใช้การผสมผสานระหว่าง (1) หลักกฎหมายประกันภัยดั้งเดิมที่ยึดหลักสุจริตอย่างยิ่ง และ (2) กลไกกำกับดูแลของ Monetary Authority of Singapore (MAS) และ Cyber Security Agency of Singapore (CSA) ผ่านแนวปฏิบัติ (guidelines) และกรอบกำกับดูแล (frameworks) ที่มีลักษณะเป็น soft law เพื่อให้ตลาดประกันภัยไซเบอร์พัฒนาไปในทิศทางที่สอดคล้องกับความเสี่ยงไซเบอร์ยุคใหม่

6.1 หลักสุจริตอย่างยิ่งและแนวทางการเปิดเผยความเสี่ยง

กฎหมายประกันภัยของสิงคโปร์ยังคงใช้หลักสุจริตอย่างยิ่งตามมาตรา 17 แห่งพระราชบัญญัติประกันภัยทางทะเล ค.ศ. 1906 ฉบับปรับปรุงแก้ไข ปี ค.ศ. 2020 (Marine Insurance Act 1906, Rev. Ed. 2020) ซึ่งกำหนดให้สัญญาประกันภัยเป็นสัญญาที่ตั้งอยู่บนความสุจริตใจอย่างยิ่ง หากฝ่ายใดละเมิด หลักการอีกฝ่ายย่อมมีสิทธิเพิกถอนสัญญาได้[39] หลักนี้เชื่อมโยงกับหน้าที่เปิดเผยข้อเท็จจริงอันเป็นสาระสำคัญตามมาตรา 18 ที่วางภาระให้ผู้เอาประกันภัยต้องเปิดเผยข้อมูลเกี่ยวกับความเสี่ยงทุกประการที่อาจมีผลต่อการตัดสินใจรับประกันภัย มิฉะนั้นผู้รับประกันภัยสามารถอ้างสิทธิเลิกสัญญาได้ทั้งหมด[40]

อย่างไรก็ดี เมื่อหลักดังกล่าวถูกนำมาใช้กับประกันภัยไซเบอร์ ซึ่งมีความเสี่ยงเชิงเทคนิคที่ซับซ้อนและเปลี่ยนแปลงเร็ว โดยเฉพาะในกลุ่มธุรกิจขนาดกลางและขนาดย่อม (SMEs) กลับก่อให้เกิดปัญหาว่าผู้เอาประกันภัยไม่รู้จริงว่าข้อเท็จจริงใดเป็นสาระสำคัญที่ต้องเปิดเผย เช่น การใช้บริการคลาวด์ มาตรการสำรองข้อมูล หรือการเข้ารหัสข้อมูล ข้อบกพร่องจึงมิได้เกิดจากการทุจริต หากแต่เกิดจากข้อจำกัดด้านความรู้ทางเทคนิค หากตีความหลักสุจริตอย่างยิ่งอย่างเคร่งครัด บริษัทประกันอาจมีฐานทางกฎหมายเพียงพอที่จะปฏิเสธความคุ้มครองบ่อยครั้ง อันกระทบต่อความเชื่อมั่นในตลาดประกันภัยไซเบอร์โดยรวม เพื่อลดความไม่สมดุลดังกล่าว MAS และ CSA จึงเข้ามาช่วยหลักสุจริตอย่างยิ่งผ่านเครื่องมือกำกับดูแล ได้แก่ แบบฟอร์มประเมิน

[39] Marine Insurance Act 1906, Rev. Ed. 2020 (Singapore), s.17.

[40] Marine Insurance Act 1906, Rev. Ed. 2020 (Singapore), s.18.

ความเสี่ยงไซเบอร์ (cyber risk assessment forms)[41] แบบสอบถามด้าน IT governance และ cybersecurity controls ตลอดจน checklist ด้าน incident response readiness รวมทั้งโครงการรับรองมาตรฐานความมั่นคงไซเบอร์ Cyber Essentials และ Cyber Trust Mark ของ CSA[42] เครื่องมือเหล่านี้ช่วยให้ผู้เอาประกันภัยสามารถระบุและเปิดเผยความเสี่ยงได้อย่างเป็นระบบ ลดปัญหาการไม่เปิดเผยโดยไม่เจตนา และทำให้หน้าที่ตามหลักสุจริตปฏิบัติได้จริงมากขึ้นในบริบทภัยไซเบอร์

6.2 แนวทางการกำหนดความคุ้มครองของประกันภัยไซเบอร์

แม้สิงคโปร์จะยังไม่มีกฎหมายเฉพาะว่าด้วยประกันภัยไซเบอร์ แต่ MAS และ CSA ได้ใช้แนวปฏิบัติและกรอบกำกับดูแลเพื่อกำหนดมาตรฐานกให้ตลาด โดย MAS เน้นให้ผู้รับประกันภัยกำหนดขอบเขตความคุ้มครอง (coverage wording) และข้อยกเว้น (exclusions) อย่างโปร่งใส เข้าใจง่าย พร้อมกำหนดให้มีการประเมินความเสี่ยงไซเบอร์ล่วงหน้าก่อนทำสัญญา ขณะที่ CSA สนับสนุนการใช้มาตรฐานด้านความมั่นคงไซเบอร์ขององค์กร ซึ่งสามารถใช้เป็นข้อมูลประกอบการประเมินความเสี่ยงของบริษัทประกัน กรมธรรม์ไซเบอร์จะประกอบด้วย (1) ความคุ้มครองภายใน (first-party coverage) เช่น ค่าใช้จ่ายในการกู้คืนระบบ ตรวจสอบทางนิติวิทยาศาสตร์ แจ้งเหตุข้อมูลรั่วไหล และความเสียหายจากการหยุดชะงักของธุรกิจ (2) ความคุ้มครองต่อความรับผิดต่อบุคคลภายนอก (third-party liability) เช่น การถูกฟ้องร้องจากการรั่วไหลของข้อมูลส่วนบุคคล หรือค่าปรับจากหน่วยงานกำกับ (3) ความคุ้มครองเสริม เช่น ค่าไถ่จาก ransomware ค่าที่ปรึกษาประชาสัมพันธ์ และค่าใช้จ่ายในการต่อสู้คดี

6.3 การประเมินมูลค่าความเสียหายจากภัยไซเบอร์

สิงคโปร์ยังไม่มีกฎหมายที่กำหนดวิธีประเมินมูลค่าความเสียหายจากภัยไซเบอร์โดยตรง แต่ใช้กรอบกำกับดูแลและแนวปฏิบัติของ MAS และ CSA เป็นฐานสำคัญ MAS ได้พัฒนา risk models และ incident reporting framework เพื่อให้บริษัทประกันและสถาบันการเงินใช้เป็นข้อมูลอ้างอิงในการประเมินความเสี่ยงและมูลค่าความเสียหาย ขณะที่ CSA สนับสนุนให้จัดทำ incident response plans และ cyber risk impact assessment ซึ่งสามารถแปลงเป็นตัวแปรสำคัญในการคำนวณค่าสินไหม ที่สำคัญ สิงคโปร์ได้จัดทำ Cyber Risk Management Project (CyRiM) ภายใต้ความร่วมมือระหว่าง MAS, CSA และสถาบันการศึกษา เพื่อสร้าง

---

[41] Monetary Authority of Singapore (MAS). **Cyber Security Regulations** [Online]. Available URL://https://www.mas.gov.sg/regulation/cyber-security, 2025 (Sep, 27).

[42] Cyber Security Agency of Singapore (CSA). **Certification for the Cyber Trust Mark** [Online]. Available URL://https://www.csa.gov.sg/our-programmes/support-for-enterprises/sg-cyber-safe-programme/cybersecurity-certification-for-organisations/cyber-trust/certification-for-the-cyber-trust-mark, 2025 (Sep, 27).

แบบจำลองความเสี่ยงเชิงสถานการณ์ (scenario-based models) เช่น การโจมตีโครงสร้างพื้นฐานการเงินหรือระบบคลาวด์ที่กระทบหลายองค์กรพร้อมกัน[43] ผลของโครงการนี้ถูกใช้เป็นฐานข้อมูลกลาง ในการกำหนดเบี้ยประกันและวงเงินคุ้มครองที่สะท้อนต้นทุนความเสี่ยงเชิงระบบได้ดีขึ้น แม้จะมีเครื่องมือดังกล่าว แต่การตีราคาความเสียหายไซเบอร์ยังเผชิญข้อจำกัด ได้แก่ การขาดข้อมูลเชิงสถิติระยะยาว (actuarial data) ความยากในการตีราคาความเสียหายที่เป็นนามธรรม เช่น ชื่อเสียงและความไว้วางใจของลูกค้า และความเสี่ยงเชิงระบบจากเหตุการณ์ขนาดใหญ่ ซึ่งล้วนทำให้การประเมินมูลค่าความเสียหายยังมีความไม่แน่นอนสูง

6.4 บทบาทของ MAS และ CSA ในการยกระดับมาตรฐานตลาด

การกำกับดูแลประกันภัยไซเบอร์ของสิงคโปร์อาศัยการบูรณาการหน่วยงานกำกับเป็นสำคัญ โดย MAS ทำหน้าที่กำกับสถาบันการเงินและผู้รับประกันภัยตาม Insurance Act (Cap. 142) และแนวปฏิบัติสำคัญ เช่น Technology Risk Management Guidelines (TRM Guidelines) ซึ่งกำหนดให้ผู้รับประกันภัยต้องมีมาตรการบริหารความเสี่ยงไซเบอร์ที่รัดกุม มีเงินกองทุนรองรับความเสี่ยงไซเบอร์เชิงระบบ และต้องเปิดเผยเงื่อนไขความคุ้มครองและข้อยกเว้นอย่างชัดเจน

ด้าน CSA ทำหน้าที่เป็นหน่วยงานกลางด้านความมั่นคงไซเบอร์ สนับสนุนการยกระดับมาตรฐานผ่านโครงการ Cyber Essentials และ Cyber Trust Mark ซึ่งทำหน้าที่เป็นดัชนีความพร้อมด้านไซเบอร์ขององค์กรผู้เอาประกันภัยที่ได้รับการรับรองสามารถใช้ใบรับรองดังกล่าวเป็นหลักฐานประกอบการเปิดเผยความเสี่ยงและเจรจาความคุ้มครองกับบริษัทประกัน นอกจากนี้ CSA ยังสนับสนุนการแบ่งปันข้อมูลภัยคุกคาม (threat intelligence sharing) จัดทำ playbooks และ incident response frameworks[44] และเชื่อมโยงมาตรการกับมาตรฐานสากล เช่น ISO/IEC 27001 และ NIST Cybersecurity Framework

7. วิเคราะห์ปัญหาเกี่ยวกับการกำกับดูแลประกันภัยไซเบอร์

กฎหมายไทยที่เกี่ยวข้องกับประกันภัยไซเบอร์ยังอยู่บนฐานของกฎหมายประกันภัยแบบเดิมเป็นหลัก โดยเฉพาะประมวลกฎหมายแพ่งและพาณิชย์ บรรพ 3 ลักษณะประกันภัย ประกอบกับพระราชบัญญัติประกันวินาศภัย พ.ศ. 2535 และโครงสร้างการกำกับดูแลตามพระราชบัญญัติสำนักงาน คปภ. พ.ศ. 2550 แม้กฎหมาย

---

[43] Insurance Risk and Finance Research Centre (IRFRC). **Cyber Risk Management Project Brief (CyRiM)** [Online]. Available URL://https://www.ntu.edu.sg/irfrc/research/cyrim/project-brief, 2025 (Sep, 27).

[44] Cyber Security Agency of Singapore (CSA). **The Singapore Cybersecurity Strategy 2021** [Online]. Available URL://https://www.csa.gov.sg/resources/publications/the-singapore-cybersecurity-strategy-2021/, 2025 (Sep, 27).

เหล่านี้ยังไม่ได้ออกแบบมาเพื่อภัยไซเบอร์โดยเฉพาะ แต่เป็นฐานสำคัญที่ใช้ตีความเงื่อนไข ความคุ้มครอง และการประเมินความเสียหายภายใต้กรมธรรม์ประกันภัยไซเบอร์ในปัจจุบัน โดยแบ่งเป็น 3 ประเด็น ดังนี้

7.1 ปัญหาเกี่ยวกับหน้าที่เปิดเผยข้อความจริง

หลักสุจริตอย่างยิ่งตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 865 วางหน้าที่ให้ผู้เอาประกันภัยต้องเปิดเผยข้อเท็จจริงอันเป็นสาระสำคัญทั้งหมด แม้ผู้รับประกันภัยจะไม่ได้สอบถามก็ตาม หลักการนี้เหมาะสมกับสัญญาประกันภัยแบบเดิม เช่น ประกันอัคคีภัยหรือประกันชีวิต ที่ความเสี่ยงเป็นรูปธรรมและผู้เอาประกันภัยสามารถทราบได้ว่าข้อเท็จจริงใดสำคัญต่อการประเมินความเสี่ยง อย่างไรก็ดี เมื่อถูกนำมาใช้กับสัญญาประกันภัยไซเบอร์ กลับปรากฏปัญหาหลายประการ เนื่องจากภัยไซเบอร์มีลักษณะซับซ้อน เปลี่ยนแปลงตลอดเวลา และต้องอาศัยความรู้เฉพาะด้านความมั่นคงปลอดภัยสารสนเทศในการประเมินความเสี่ยง ผู้เอาประกันภัยจำนวนมากไม่สามารถทราบได้ว่าข้อเท็จจริงใดเข้าข่ายสาระสำคัญตามมาตรา 865 ทั้งที่ข้อเท็จจริงด้านมาตรการรักษาความปลอดภัย การสำรองข้อมูล การใช้บริการคลาวด์ หรือการบริหารจัดการข้อมูลภายในองค์กร ล้วนส่งผลต่อความเสี่ยงโดยตรง การไม่เข้าใจความสำคัญของข้อมูลเหล่านี้อาจนำไปสู่การไม่เปิดเผยโดยสุจริต แต่ยังถูกตีความว่าเป็นการปกปิดซึ่งเปิดโอกาสให้ผู้รับประกันภัยบอกล้างสัญญาหรือปฏิเสธความคุ้มครองได้ง่ายเกินสมควร ความไม่สมดุลนี้สะท้อนถึงความเหลื่อมล้ำทางความรู้ระหว่างคู่สัญญา เนื่องจากผู้รับประกันภัยมีผู้เชี่ยวชาญช่วยประเมินความเสี่ยง ขณะที่ผู้เอาประกันภั โดยเฉพาะธุรกิจขนาดกลางและขนาดย่อมมักไม่เข้าใจประเด็นทางเทคนิคอย่างเพียงพอ

ประเด็นปัญหาสำคัญอีกประการคือ มาตรา 865 ครอบคลุมเฉพาะก่อนการทำสัญญา ขณะที่ลักษณะภัยไซเบอร์มีการเปลี่ยนแปลงอย่างต่อเนื่อง เช่น ช่องโหว่ใหม่ การอัปเดตระบบ หรือการเปลี่ยนแปลงโครงสร้างสารสนเทศภายในองค์กร ซึ่งล้วนเป็นข้อเท็จจริงที่มีผลต่อความเสี่ยง แต่ไม่ได้อยู่ในกรอบหน้าที่ตามกฎหมาย นอกจากนี้ บทบัญญัติยังไม่ได้กำหนดความเชื่อมโยงเหตุอย่างชัดเจนว่าข้อเท็จจริงที่ไม่เปิดเผยจะต้องมีผลกระทบต่อการยอมรับประกันภัยหรือการเกิดความเสียหาย จึงเกิดปัญหาเมื่อความเสียหายไม่ได้เกี่ยวข้องกับข้อเท็จจริงที่ตกหล่น แต่ผู้รับประกันภัยยังสามารถบอกล้างสัญญาได้ตามตัวบท

ในทางเปรียบเทียบ ประเทศอังกฤษได้ปรับปรุงระบบโดยบัญญัติหน้าที่ การนำเสนอความเสี่ยงอย่างเป็นธรรม (Duty of Fair Presentation) ที่กำหนดให้ผู้เอาประกันภัยต้องเปิดเผยเท่าที่ตนรู้หรือควรรู้อย่างสมเหตุสมผล และกำหนดหน้าที่เชิงรุกให้ผู้รับประกันภัยต้องสอบถามเพิ่มเติมหากข้อมูลยังไม่ครบถ้วน ขณะเดียวกัน การเยียวยาในกรณีผิดหน้าที่ก็มีความยืดหยุ่นและเป็นสัดส่วน เช่น การปรับเบี้ยประกัน หรือปฏิเสธเฉพาะส่วนที่เกี่ยวข้อง ไม่ใช่การบอกล้างสัญญาทั้งฉบับดังเช่นกฎหมายไทย ส่วนประเทศสิงคโปร์ แม้ยังยึดหลักสุจริตอย่างยิ่ง แต่มีการออกแบบฟอร์มมาตรฐานและแนวทางการเปิดเผยข้อมูล เพื่อช่วยลดการตีความ

คลุมเครือและแก้ภาวะอสมดุลด้านความรู้ จากการวิเคราะห์ พบว่ามาตรา 865 ไม่สามารถรองรับลักษณะความเสี่ยงแบบหลายมิติของภัยไซเบอร์ได้อย่างเหมาะสม ทั้งในด้านความซับซ้อนเชิงเทคนิค ความไม่แน่นอนของข้อเท็จจริงที่ถือเป็นสาระสำคัญ การไม่มีเกณฑ์ชี้วัดที่ชัดเจน การเชื่อมโยงความเสี่ยงระหว่างหลายกรมธรรม์ และกลไกเยียวยาที่ขาดความสมดุล นอกจากนี้ ความไม่ชัดเจนของกฎหมายยังส่งผลกระทบต่อการพัฒนาตลาดประกันภัยไซเบอร์ เนื่องจากผู้ประกอบการอาจกังวลว่าจะไม่ได้รับความคุ้มครองจริงเมื่อเกิดเหตุ ทำให้ตลาดไม่สามารถเติบโตได้เต็มศักยภาพ

โดยสรุป แม้หลักสุจริตอย่างยิ่งมีความสำคัญในระบบสัญญาประกันภัย แต่เมื่อนำมาใช้กับสัญญาประกันภัยไซเบอร์กลับก่อให้เกิดข้อจำกัดเชิงกฎหมายและภาระที่ไม่สมส่วนต่อผู้เอาประกันภัย ประเทศไทยจึงควรพิจารณาปรับปรุงกฎหมายให้สอดคล้องกับความเสี่ยงเชิงเทคโนโลยีและแนวปฏิบัติสากล เพื่อให้สัญญาประกันภัยไซเบอร์มีความเป็นธรรม โปร่งใส และสามารถคุ้มครองผู้เอาประกันภัยได้จริง

7.2 ปัญหาเกี่ยวกับขอบเขตความคุ้มครองภัยไซเบอร์

การกำหนดขอบเขตความคุ้มครองในสัญญาประกันภัยไซเบอร์เป็นสิ่งที่สำคัญ เพราะเป็นตัวกำหนดว่าผู้เอาประกันภัยจะได้รับการคุ้มครองต่อความเสียหายประเภทใดและในระดับใด อย่างไรก็ตาม กฎหมายไทยยังไม่มีพระราชบัญญัติประกันภัยไซเบอร์โดยเฉพาะ และต้องอาศัยหลักทั่วไปในประมวลกฎหมายแพ่งและพาณิชย์ควบคู่กับพระราชบัญญัติประกันวินาศภัย พ.ศ. 2535 ซึ่งถูกออกแบบมาภายใต้ความเสี่ยงทางกายภาพ เช่น ไฟไหม้ รถยนต์ หรือภัยธรรมชาติ เมื่อนำมาใช้กับภัยไซเบอร์ซึ่งมีลักษณะไม่เป็นรูปธรรม ต่อเนื่อง และเชื่อมโยงกัน จึงก่อให้เกิดปัญหาเชิงนิยาม ขอบเขตความคุ้มครอง และการตีความสัญญาอย่างมีนัยสำคัญ

มาตรา 861 ซึ่งนิยามสัญญาประกันภัยว่าต้องมีเหตุในอนาคตอันไม่แน่นอน ประสบปัญหาเมื่อใช้กับภัยไซเบอร์ที่มักไม่ใช่เหตุการณ์เฉียบพลัน แต่เป็นเหตุที่แฝงอยู่ในระบบเป็นเวลานาน หรือมีลักษณะสืบเนื่องต่อเนื่อง ส่งผลให้กำหนด เหตุที่เอาประกันภัยได้ยาก ทั้งในแง่เวลาและจำนวนเหตุ นอกจากนี้ ความเสียหายจากภัยไซเบอร์จำนวนมากเกี่ยวข้องกับข้อมูล ชื่อเสียง หรือความเชื่อมั่น ซึ่งไม่ได้มีลักษณะเป็นทรัพย์สินตามความเข้าใจดั้งเดิม ทำให้การนำมาตรา 869 ว่าด้วยวินาศภัยมาใช้มีความคลุมเครือว่าความเสียหายทางดิจิทัลเหล่านี้อยู่ในขอบเขตที่อาจประมาณเป็นเงินได้หรือไม่ สำหรับมาตรา 867 ที่กำหนดให้กรมธรรม์ระบุวัตถุที่เอาประกัน ภัยที่รับเสี่ยง และระยะเวลาคุ้มครอง ปัญหาสำคัญในบริบทไซเบอร์คือ กฎหมายไม่ได้กำหนดมาตรฐานกลางในการระบุภัยที่รับเสี่ยงและคำจำกัดความที่เกี่ยวข้อง เช่น เหตุการณ์ทางไซเบอร์ การรั่วไหลของข้อมูล หรือ ความล้มเหลวของระบบเครือข่าย ส่งผลให้แต่ละบริษัทใช้ถ้อยคำและเงื่อนไขแตกต่างกันอย่างมาก เกิดความเสี่ยงของการคุ้มครองแบบแฝง (Silent Cyber) และเปิดช่องให้ผู้รับประกันภัยใช้ข้อยกเว้นหรือความไม่ชัดเจนในการปฏิเสธความคุ้มครอง แม้ผู้เอาประกันภัยจะเข้าใจโดยสุจริตว่าตนได้รับความคุ้มครองก็ตาม ถึงแม้

พระราชบัญญัติประกันวินาศภัย พ.ศ. 2535 มาตรา 29–30 จะกำหนดให้แบบกรมธรรม์และอัตราเบี้ยต้องได้รับความเห็นชอบจากนายทะเบียนเพื่อคุ้มครองผู้เอาประกันภัย แต่ยังไม่มีหลักเกณฑ์เฉพาะสำหรับกรมธรรม์ไซเบอร์ ทำให้ผู้รับประกันภัยมีอิสระสูงในการออกแบบขอบเขตความคุ้มครอง เช่น บางกรมธรรม์คุ้มครองเฉพาะการโจมตีจากภายนอก ไม่ครอบคลุมการรั่วไหลโดยบุคลากรภายใน บางกรมธรรม์คุ้มครองค่าใช้จ่ายกู้ระบบแต่ไม่คุ้มครองค่าไถ่จาก ransomware หรือบางกรมธรรม์จำกัดเฉพาะระบบที่ผู้เอาประกันภัยเป็นเจ้าของ ไม่รวมระบบคลาวด์หรือระบบที่เช่าใช้ ความแตกต่างดังกล่าวทำให้ผู้เอาประกันภัยไม่สามารถเปรียบเทียบกรมธรรม์ได้อย่างโปร่งใส และไม่สามารถคาดหมายสิทธิความคุ้มครองของตนได้แน่นอน อีกทั้ง กฎหมายไทยยังไม่มีนิยามชัดเจนของภัยไซเบอร์ หรือความเสียหายทางไซเบอร์ ทำให้การตีความขึ้นอยู่กับดุลพินิจของผู้รับประกันภัยเป็นหลัก ทั้งในประเด็นเหตุที่ถือเป็นภัยไซเบอร์ และลักษณะของความเสียหายที่อยู่ในขอบเขตคุ้มครอง นำไปสู่ข้อพิพาทและบั่นทอนความเชื่อมั่นในตลาดประกันภัยไซเบอร์โดยรวม

เมื่อเปรียบเทียบกับอังกฤษที่ใช้ Insurance Act 2015 ควบคู่กับมาตรการของหน่วยงานกำกับ เช่น FCA/PRA และบทบาทของ Lloyd’s of London และ ABI ในการกำหนดให้กรมธรรม์ต้องระบุความคุ้มครองและข้อยกเว้นภัยไซเบอร์อย่างชัดเจน เพื่อลดปัญหา Silent Cyber และสร้างมาตรฐานขั้นต่ำของความคุ้มครอง ส่วนสิงคโปร์ใช้แนวทางกำกับแบบ soft law โดย MAS กำหนดแบบประเมินความเสี่ยงไซเบอร์มาตรฐานและ CSA ผลักดันมาตรฐานด้านความปลอดภัยไซเบอร์ที่เชื่อมโยงกับการประเมินความคุ้มครองและเบี้ยประกันภัย ทำให้เนื้อหากรมธรรม์ไซเบอร์มีการระบุขอบเขตความคุ้มครอง แยก first-party และ third-party อย่างเป็นระบบ และลดโอกาสเกิดข้อพิพาท

สำหรับประเทศไทย การขาดทั้งนิยามทางกฎหมาย มาตรฐานกลางของกรมธรรม์ และกลไกกำกับเฉพาะด้านไซเบอร์ ส่งผลให้ขอบเขตความคุ้มครองมีความไม่แน่นอนสูง ผู้เอาประกันภัยเสียเปรียบในการทำสัญญา และตลาดประกันภัยไซเบอร์ไม่สามารถพัฒนาได้เต็มศักยภาพ ทั้งที่ภัยไซเบอร์มีแนวโน้มทวีความรุนแรงและแพร่หลายมากขึ้น จึงมีความจำเป็นเร่งด่วนที่กฎหมายไทยควรพิจารณาจัดทำกรอบนิยาม มาตรฐานขอบเขตความคุ้มครอง และแนวทางกำกับดูแลเฉพาะ เพื่อเสริมสร้างความเป็นธรรม โปร่งใส และความเชื่อมั่นในระบบประกันภัยไซเบอร์โดยรวม

7.3 ปัญหาเกี่ยวกับการประเมินมูลค่าความเสียหายจากภัยไซเบอร์

การประเมินมูลค่าความเสียหายเป็นตัวกำหนดจำนวนค่าสินไหมทดแทนที่ผู้รับประกันภัยต้องชดใช้แก่ผู้เอาประกันภัย หลักการนี้ในกฎหมายไทยปรากฏชัดในบริบทประกันวินาศภัยแบบเดิม เช่น ไฟไหม้หรือโจรกรรม ที่มีทรัพย์สินจับต้องได้และตีราคาเป็นตัวเงินได้โดยตรง ภายใต้หลักมาตรา 877 แห่งประมวลกฎหมายแพ่งและพาณิชย์ซึ่งกำหนดให้ชดใช้เท่ามูลค่าความเสียหายจริง ภายในจำนวนเงินเอาประกันภัย รวมถึงค่าใช้จ่าย

เพื่อป้องกันหรือจำกัดความเสียหาย และถือเอามูลค่า ณ สถานที่และเวลาเกิดเหตุวินาศภัยเป็นเกณฑ์ อย่างไรก็ดี เมื่อหลักการดังกล่าวถูกนำมาใช้กับประกันภัยไซเบอร์กลับพบข้อจำกัดอย่างมีนัยสำคัญ คือ ลักษณะของเหตุภัยไซเบอร์ เช่น การโจมตีระบบหรือการรั่วไหลของข้อมูล มักไม่ใช่เหตุการณ์เฉียบพลัน ณ เวลาและสถานที่ที่แน่นอน แต่อาจดำเนินไปอย่างต่อเนื่องและเพิ่งถูกค้นพบภายหลัง ทำให้การกำหนดเวลาและสถานที่เกิดวินาศภัยตามกรอบมาตรา 877 เป็นไปได้ยาก ส่งผลต่อการตีราคาและจำกัดขอบเขตความเสียหายที่ชดใช้ได้ ประกอบกับความเสียหายจากภัยไซเบอร์จำนวนมากเป็นความเสียหายเชิงนามธรรมหรือเชิงข้อมูล เช่น การสูญเสียข้อมูลสำคัญ การสูญเสียความเชื่อมั่นของลูกค้า หรือความเสียหายต่อชื่อเสียงองค์กร ซึ่งไม่ได้สอดคล้องกับกรอบความเสียหายทางกายภาพที่กฎหมายประกันภัยไทยใช้เป็นฐานคิดหลัก นำไปสู่การตีความว่าอะไรถือเป็นวินาศภัยตามมาตรา 877 และ 869 ได้อย่างจำกัด ความคุ้มครองจึงมักจำกัดอยู่เพียงค่าใช้จ่ายที่พิสูจน์ได้โดยตรง เช่น ค่ากู้คืนระบบ ค่าที่ปรึกษาด้านเทคนิคหรือกฎหมาย และค่าปรับจากหน่วยงานกำกับ ขณะที่ผลกระทบทางเศรษฐกิจในภาพรวมอาจสูงกว่ามาก

แม้มาตรา 878 จะกำหนดให้ค่าใช้จ่ายในการตีราคาความเสียหายเป็นภาระของผู้รับประกันภัย และมาตรา 880 วางหลักการรับช่วงสิทธิเพื่อป้องกันการชดใช้เกินจริง แต่ในทางปฏิบัติการประเมินความเสียหายยังถูกจำกัดด้วยข้อกำหนดในกรมธรรม์ เช่น ค่าเสียหายส่วนแรก หลักสัดส่วนเฉลี่ย หรือการคุ้มครองร่วม ซึ่งแม้ผ่านการเห็นชอบตามพระราชบัญญัติประกันวินาศภัย พ.ศ. 2535 มาตรา 29–30 แล้วก็ยังไม่ได้สร้างมาตรฐานเฉพาะสำหรับการประเมินความเสียหายไซเบอร์ ผลคือ การตีราคายังคงขึ้นอยู่กับดุลพินิจของบริษัทประกันภัยและผู้ประเมินสินไหมแต่ละราย โดยไม่มีเกณฑ์กลางรองรับ โดยความซับซ้อนของความเสียหายทางไซเบอร์ยิ่งทำให้ปัญหาชัดเจนขึ้น เมื่อแยกออกเป็นความเสียหายทางเทคนิค ทางธุรกิจ ความเสียหายต่อสิทธิของบุคคลภายนอก และความเสียหายที่ไม่ใช่ตัวเงิน ผู้เอาประกันภัยจึงต้องเผชิญภาระพิสูจน์มูลค่าความเสียหายในเชิงชื่อเสียงหรือความเชื่อมั่น ซึ่งเป็นเรื่องยากและมักถูกโต้แย้งได้ง่าย อีกทั้งประเทศไทยยังไม่มีองค์กรกลางกำหนดมาตรฐานการประเมินมูลค่าความเสียหายไซเบอร์โดยเฉพาะ ทำให้เกิดความเหลื่อมล้ำระหว่างคู่สัญญาและเพิ่มความเสี่ยงต่อข้อพิพาท

เมื่อเปรียบเทียบกับประเทศอังกฤษและสิงคโปร์จะเห็นทิศทางที่ต่างกัน อังกฤษอาศัยทั้งกรอบกฎหมายและแนวปฏิบัติของตลาด เช่น Lloyd’s และ ABI ในการกำหนดองค์ประกอบของความเสียหายไซเบอร์อย่างครอบคลุม ทั้งค่าใช้จ่ายทางเทคนิค การบริหารจัดการวิกฤต และการฟื้นฟูชื่อเสียง แม้จะเป็นเพียง soft law แต่ถูกใช้เป็นมาตรฐานกลางในตลาด ส่วนสิงคโปร์ใช้มาตรการกำกับเชิงปฏิบัติของ MAS และ CSA ผ่านแบบประเมินความเสี่ยงและแนวทางเก็บข้อมูลที่เกี่ยวข้อง ทำให้คู่สัญญามีความเข้าใจตรงกันมากขึ้น และช่วยให้การประเมินมูลค่าความเสียหายสอดคล้องกับข้อเท็จจริงทางเทคนิค

สรุปได้ว่าการขาดมาตรฐานกลางและกฎหมายเฉพาะในการประเมินมูลค่าความเสียหายจากภัยไซเบอร์ในประเทศไทย ส่งผลกระทบทั้งต่อผู้เอาประกันภัย ผู้รับประกันภัย และระบบกฎหมายโดยรวม ทำให้สิทธิในการได้รับการชดใช้มีความไม่แน่นอน และอาจบั่นทอนความเชื่อมั่นในตลาดประกันภัยไซเบอร์ องค์กรกำกับดูแลจำเป็นต้องเร่งกำหนดเกณฑ์และแนวทางเฉพาะในการประเมินความเสียหายไซเบอร์ตามแนวทางที่โปร่งใส ตรวจสอบได้ และสอดคล้องกับมาตรฐานระหว่างประเทศ

8. ข้อเสนอแนะ

วิเคราะห์ปัญหาพบว่ากฎหมายประกันภัยไทยยังไม่สอดคล้องกับลักษณะเฉพาะของภัยไซเบอร์ซึ่งมีความซับซ้อนทางเทคนิคและเปลี่ยนแปลงอย่างรวดเร็ว โดยเฉพาะใน 3 ประเด็นหลัก ได้แก่ (1) หน้าที่เปิดเผยความจริงตามหลักสุจริตอย่างยิ่ง (2) การกำหนดขอบเขตความคุ้มครองภัยไซเบอร์ และ (3) การประเมินมูลค่าความเสียหายจากภัยไซเบอร์ ซึ่งทั้งสามประเด็นนี้เป็นกลไกหลักของสัญญาประกันภัยไซเบอร์ หากกฎหมายไม่รองรับอย่างเหมาะสม ย่อมกระทบต่อความเป็นธรรมและประสิทธิภาพของระบบประกันภัยไซเบอร์โดยรวม ดังนั้น ผู้เขียนจึงเสนอแนวทางปรับปรุงกฎหมายและกลไกกำกับดูแล โดยมีเป้าหมายให้ (1) หลักการเปิดเผยข้อเท็จจริงมีความสมดุลระหว่างคู่สัญญา (2) ขอบเขตความคุ้มครองมีมาตรฐานกลางที่ชัดเจน และ (3) การประเมินมูลค่าความเสียหายอาศัยเกณฑ์ทางเทคนิคที่ตรวจสอบได้ที่เป็นมาตรฐานกลาง

8.1 ข้อเสนอแนะเกี่ยวกับหน้าที่เปิดเผยความจริง

มาตรา 865 แห่งประมวลกฎหมายแพ่งและพาณิชย์ยังคงวางหลักสุจริตอย่างยิ่ง โดยให้หน้าที่การเปิดเผยข้อเท็จจริงไว้ที่ผู้เอาประกันภัยเป็นสำคัญ ซึ่งไม่สอดคล้องกับลักษณะของภัยไซเบอร์ที่มีมิติทางเทคนิคสูง ผู้เอาประกันภัย โดยเฉพาะธุรกิจขนาดกลางและขนาดย่อมมักไม่สามารถทราบได้อย่างแท้จริงว่าข้อมูลใดเป็นสาระสำคัญต่อการประเมินความเสี่ยง ทำให้เกิดความไม่สมดุลของอำนาจต่อรองในทางปฏิบัติ และเปิดช่องให้ผู้รับประกันภัยอาศัยข้อบกพร่องในการเปิดเผยข้อมูลเป็นเหตุบอกล้างสัญญาหรือปฏิเสธความคุ้มครองได้ แม้ในกรณีที่ผู้เอาประกันภัยมิได้มีเจตนาปกปิดก็ตาม

อย่างไรก็ดี การแก้ไขประมวลกฎหมายแพ่งและพาณิชย์โดยตรงย่อมมีความยุ่งยากและส่งผลกระทบต่อโครงสร้างกฎหมายประกันภัยโดยรวม ผู้เขียนจึงเสนอให้ใช้แนวทางแก้ไขเพิ่มเติมพระราชบัญญัติประกันวินาศภัย พ.ศ. 2535 ซึ่งมีความยืดหยุ่นมากกว่า และสามารถออกแบบกลไกเฉพาะสำหรับประกันภัยไซเบอร์ได้อย่างเหมาะสม โดยเสนอให้นำหลักการ “Duty of Fair Presentation of the Risk” ของอังกฤษมาปรับใช้ในลักษณะที่ว่า “ผู้เอาประกันภัยมีหน้าที่เปิดเผยเฉพาะข้อเท็จจริงอันเป็นสาระสำคัญเท่าที่ตนรู้อยู่หรือควรรู้โดยสมเหตุสมผล ขณะเดียวกัน ผู้รับประกันภัยต้องมีหน้าที่สอบถามเพิ่มเติมเกี่ยวกับความเสี่ยงที่เห็นว่าสำคัญก่อนการรับประกันภัย การไม่เปิดเผยข้อมูลบางประการจะเป็นเหตุให้ใช้สิทธิบอกล้างสัญญาได้ก็แต่เมื่อพิสูจน์ได้ว่า

ผู้เอาประกันภัยจงใจปกปิดหรือประมาทเลินเล่ออย่างร้ายแรงเท่านั้น" หากการละเว้นเกิดจากการไม่รู้ข้อเท็จจริงเชิงเทคนิคโดยสุจริต ควรใช้มาตรการเยียวยาเชิงสัดส่วน เช่น การปรับอัตราเบี้ยประกันภัย หรือเพิ่มหรือลดจำนวนค่าสินไหมทดแทน แทนการบอกล้างสัญญาทั้งฉบับ

แนวทางดังกล่าวจะช่วยเปลี่ยนระบบจากการวางภาระเกือบทั้งหมดไว้ที่ผู้เอาประกันภัย ไปสู่ระบบที่ผู้รับประกันภัยต้องมีบทบาทเชิงรุกมากขึ้นในการสอบถาม ตรวจสอบ และประเมินความเสี่ยง พร้อมทั้งช่วยสร้างดุลยภาพแห่งสิทธิและหน้าที่ระหว่างคู่สัญญาให้สอดคล้องกับบริบทของภัยไซเบอร์ในยุคปัจจุบันมากยิ่งขึ้น

8.2 ข้อเสนอแนะเกี่ยวกับขอบเขตความคุ้มครองภัยไซเบอร์

ข้อเสนอแนะเกี่ยวกับการปรับปรุงขอบเขตความคุ้มครองภัยไซเบอร์ควรมุ่งแก้ไขปัญหาความไม่ชัดเจนและความไม่สม่ำเสมอของกรมธรรม์ โดยจะเห็นได้ว่ากฎหมายไทยยังขาดนิยามทางกฎหมายของ "ภัยไซเบอร์" และ "Silent Cyber" อีกทั้งยังไม่มีมาตรฐานกลางด้านขอบเขตความคุ้มครอง จึงเปิดโอกาสให้ผู้รับประกันภัยกำหนดเงื่อนไขตามดุลพินิจของตนเอง ส่งผลให้กรมธรรม์มีความแตกต่างกันอย่างมาก ผู้เอาประกันภัยไม่สามารถเปรียบเทียบผลิตภัณฑ์ได้อย่างโปร่งใสและไม่อาจคาดหมายสิทธิความคุ้มครองที่แท้จริงได้ เพื่อแก้ไขปัญหานี้ ผู้เขียนเสนอให้ดำเนินการทั้งในการออกประกาศและการแก้ไขเพิ่มเติมกฎหมายหลัก โดยให้สำนักงาน คปภ.ใช้อำนาจตามมาตรา 29 แห่งพระราชบัญญัติประกันวินาศภัย พ.ศ. 2535 และมาตรา 12 แห่งพระราชบัญญัติ คปภ. พ.ศ. 2550 ออก "ประกาศว่าด้วยแบบกรมธรรม์ประกันภัยไซเบอร์มาตรฐานกลาง" ซึ่งควรกำหนดขอบเขตความคุ้มครองขั้นต่ำ เช่น ความเสียหายต่อระบบและข้อมูล ความรับผิดต่อบุคคลภายนอก การหยุดชะงักของธุรกิจ และค่าฟื้นฟูชื่อเสียง ตลอดจนกำหนดให้ผู้รับประกันภัยต้องระบุอย่างชัดเจนว่ากรมธรรม์ครอบคลุมหรือยกเว้น Silent Cyber เพื่อยุติความคลุมเครือ นอกจากนี้ ควรส่งเสริมให้กรมธรรม์ใช้ถ้อยคำที่เข้าใจง่าย และให้ผู้รับประกันภัยรายงานสถิติภัยไซเบอร์และค่าสินไหมต่อ คปภ. เพื่อจัดตั้งฐานข้อมูลกลางสำหรับการวิเคราะห์ความเสี่ยงและกำหนดเบี้ยประกันอย่างเป็นธรรม

ในส่วนของการปรับปรุงกฎหมายหลัก ผู้เขียนเสนอให้แก้ไขเพิ่มเติมพระราชบัญญัติประกันวินาศภัย พ.ศ. 2535 โดยบัญญัติเพิ่มบทที่ให้อำนาจ คปภ.โดยเฉพาะในการกำหนดนิยามของ "ภัยไซเบอร์" และ "ความเสียหายทางไซเบอร์" พร้อมทั้งกำหนดแบบกรมธรรม์มาตรฐานและขอบเขตความคุ้มครองขั้นต่ำที่ผู้รับประกันภัยทุกแห่งต้องปฏิบัติตาม อันจะทำให้กลไกกำกับดูแลมีความชัดเจน มีเอกภาพ และสามารถลดความแตกต่างของกรมธรรม์ได้อย่างเป็นรูปธรรม การมีทั้งประกาศแนวปฏิบัติและฐานอำนาจตามกฎหมายระดับ

พระราชบัญญัติจะช่วยสร้างความแน่นอนของระบบ เพิ่มความเชื่อมั่นให้แก่ผู้บริโภค และสนับสนุนให้ตลาดประกันภัยไซเบอร์ของประเทศไทยมีความโปร่งใสและพัฒนามาตรฐานได้ทัดเทียมต่างประเทศ

8.3 ข้อเสนอแนะเกี่ยวกับการประเมินมูลค่าความเสียหายจากภัยไซเบอร์

จากการที่กฎหมายไทยยังขาดทั้งมาตรฐานกลางและวิธีการประเมินมูลค่าความเสียหายที่เหมาะสมกับลักษณะเฉพาะของภัยไซเบอร์ และกลไกการรับรองผู้ประเมินที่มีความรู้ทั้งด้านเทคนิค ส่งผลให้กระบวนการประเมินมูลค่าความเสียหายยังขึ้นอยู่กับดุลพินิจของบริษัทประกันภัยเป็นหลัก และมักจำกัดอยู่เพียงค่าใช้จ่ายทางเทคนิคที่สามารถพิสูจน์ได้ ขณะที่ความเสียหายเชิงนามธรรม เช่น ชื่อเสียง ความไว้วางใจของลูกค้า และผลกระทบต่อธุรกิจระยะยาวกลับไม่ได้รับการชดเชยอย่างเป็นธรรม เพื่อแก้ไขข้อจำกัดดังกล่าว ผู้เขียนเห็นควรให้มีการปรับปรุงทั้งในการกำกับดูแลและทางกฎหมายอย่างบูรณาการ โดยเริ่มจากการจัดตั้งกลไกผู้ประเมินภัยไซเบอร์เฉพาะทางตามอำนาจมาตรา 13 แห่งพระราชบัญญัติ คปภ. พ.ศ. 2550 โดยให้สำนักงาน คปภ. แต่งตั้งคณะทำงานหรือคณะผู้ประเมินภัยไซเบอร์ที่มีความเชี่ยวชาญด้านเทคนิคและด้านกฎหมาย ทำหน้าที่กำหนดคุณสมบัติ อบรม ทดสอบ และออกใบรับรองผู้ประเมินสินไหมไซเบอร์ โดยคณะดังกล่าวควรประกอบด้วยผู้แทนจากสำนักงาน คปภ. สมาคมประกันวินาศภัยไทย ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์จาก ThaiCERT หรือสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) และนักวิชาการด้านกฎหมาย เพื่อให้มาตรฐานการประเมินมีความครอบคลุมทุกมิติและเทียบเคียงมาตรฐานสากล

นอกจากนี้ ควรให้ คปภ. ออกกรอบมาตรฐานการประเมินมูลค่าความเสียหายไซเบอร์โดยใช้อำนาจตามมาตรา 12 ของพระราชบัญญัติ คปภ. โดยกำหนดองค์ประกอบการประเมินอย่างเป็นระบบอย่างน้อยสามด้าน ได้แก่ (1) ด้านเทคนิค เช่น ค่าใช้จ่ายในการฟื้นฟูระบบ การกู้คืนข้อมูล และการป้องกันการโจมตีซ้ำ (2) ด้านชื่อเสียงและความเชื่อมั่น เช่น ผลกระทบต่อภาพลักษณ์องค์กร ความไว้วางใจของลูกค้า และความเสียหายทางธุรกิจเชิงคุณภาพ และ (3) ด้านกฎหมายและความรับผิด เช่น ค่าปรับตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ค่าชดเชยความเสียหายแก่บุคคลภายนอก และค่าใช้จ่ายในกระบวนการทางคดี การกำหนดองค์ประกอบเช่นนี้จะทำให้การประเมินมูลค่าความเสียหายสะท้อนความเสียหายจริงขององค์กรได้ครบถ้วนและลดข้อพิพาทระหว่างคู่สัญญา

ในระดับโครงสร้างพื้นฐาน ควรให้ คปภ. ใช้อำนาจตามมาตรา 20 ของพระราชบัญญัติ คปภ. ในการจัดตั้งฐานข้อมูลกลางด้านความเสียหายไซเบอร์ โดยรวบรวมและเชื่อมโยงข้อมูลกับหน่วยงานด้านความมั่นคงไซเบอร์ของประเทศ เช่น ThaiCERT สพธอ. สกมช. และธนาคารแห่งประเทศไทย พร้อมกำหนดให้บริษัทประกันภัยรายงานสถิติการเกิดเหตุและค่าสินไหมไซเบอร์ต่อ คปภ. อย่างสม่ำเสมอ ฐานข้อมูลดังกล่าวจะเป็น

เครื่องมือสำคัญในการกำหนดอัตราเบี้ยประกันภัย การประเมินระดับความเสี่ยงของแต่ละอุตสาหกรรม และการตรวจสอบความเป็นธรรมในการชำระค่าสินไหม

ท้ายที่สุด ผู้เขียนเสนอให้แก้ไขเพิ่มเติมพระราชบัญญัติประกันวินาศภัย พ.ศ. 2535 โดยบัญญัติเพิ่มบทบาทให้สำนักงาน คปภ.มีอำนาจโดยตรงในการกำหนดมาตรฐานการประเมินมูลค่าความเสียหายจากภัยไซเบอร์ รวมถึงการจัดตั้งหรือรับรองหน่วยงานผู้ประเมินภัยไซเบอร์ เพื่อให้กลไกดังกล่าวมีฐานะทางกฎหมายที่ชัดเจนและมีผลผูกพัน การยกระดับทั้งการกำกับดูแลและกฎหมายในลักษณะนี้จะช่วยให้การประเมินความเสียหายมีความโปร่งใส ตรวจสอบได้ และสะท้อนความเสียหายที่แท้จริงมากยิ่งขึ้น ตลอดจนเสริมสร้างความเชื่อมั่นของผู้เอาประกันภัยและประสิทธิภาพของตลาดประกันภัยไซเบอร์ไทยโดยรวม

เอกสารอ้างอิง

จิตติ ติงศภัทิย์ ปรับปรุงเพิ่มเติมโดยสิทธิโชค ศรีเจริญ .**กฎหมายแพ่งและพาณิชย์ว่าด้วยประกันภัย.** พิมพ์ครั้งที่ 18. (กรุงเทพฯ :สำนักพิมพ์วิญญูชน, 2568).

ธีรยุทธ ปักษา. “ข้อยกเว้นความรับผิดของผู้รับประกันภัยในสัญญาประกันชีวิต.” **วารสารปาริชาต มหาวิทยาลัยทักษิณ** 6, 1 (2560): 113-134.

ศศิธร จิตรประเสริฐ. “โอกาสในการซื้อประกันภัยไซเบอร์ส่วนบุคคล: กรณีศึกษาของประกันภัยไซเบอร์ส่วนบุคคล.” (วิทยานิพนธ์เศรษฐศาสตรมหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์, 2566).

สิทธิโชค ศรีเจริญ. **หลักกฎหมายประกันภัย.** (กรุงเทพฯ: สำนักพิมพ์วิญญูชน, 2561).

อัศว์ณุต แสงทองดี และ ญาณพล ยั่งยืน. “แนวทางการรับมือและการรับแจ้งเหตุของตำรวจต่อกรณีมัลแวร์เรียกค่าไถ่.” **วารสารสหศาสตร์** 21, 1 (เมษายน 2564): 26-44.

Aggeliki Tsohou, Vasiliki Diamantopoulou, Stefanos Gritzalis, and Costas Lambrinoudakis. “Cyber Insurance: State of the Art, Trends and Future Directions,” **International Journal of Information Security** 22, 4 (2023):739.

Association of British Insurers. **Cyber Insurance Guide**. [Online]. Available URL://https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/cyber-insurance, 2025 (July, 19).

Cyber Security Agency of Singapore (CSA). **Certification for the Cyber Trust Mark** [Online]. Available URL://https://www.csa.gov.sg/our-programmes/support-for-enterprises/sg-cyber-safe-programme/cybersecurity-certification-for-organisations/cyber-trust/certification-for-the-cyber-trust-mark, 2025 (Sep, 27).

Cyber Security Agency of Singapore. **Guide to Conducting Cybersecurity Risk Assessment for Critical Information Infrastructure**. [Online]. Available URL://https://www.csa.gov.sg/legislation/supplementary-references, 2025 (July, 19).

Cyber Security Agency of Singapore (CSA). **The Singapore Cybersecurity Strategy 2021** [Online]. Available URL://https://www.csa.gov.sg/resources/publications/the-singapore-cybersecurity-strategy-2021/, 2025 (Sep, 27).

European Union Agency for Cybersecurity (ENISA), **ENISA Threat Landscape** [Online]. Available URL://https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf, 2025 (July, 19).

European Union Agency for Cybersecurity (ENISA). **ENISA Threat Landscape 2021: Main Incidents and Threats.** [Online]. Available URL://https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021, 2025 (July, 19).

Financial Conduct Authority. **Financial Services Cyber Incident Response Framework**. [Online]. Available URL://https://www.fca.org.uk/firms/cyber-resilience, 2025 (July, 19).

Government of the United Kingdom. **Insurance Act 2015 (c. 4), Part 2: Duty of Fair Presentation**. [Online]. Available URL://https://www.legislation.gov.uk/ukpga/2015/4/part/2, 2025 (July, 19).

Guy Carpenter. **Grappling With the Silent Cyber.** [Online]. Available URL://https://www.actuaries.org.sg/sites/default/files/2020-12/20112709ermSilentCyber.pdf, 2025 (July, 19).

IMARC Group. **Thailand Cyber Insurance Market Size, Share and Trends 2025–2033** [Online]. Available URL://https://www.imarcgroup.com/thailand-cyber-insurance-market, 2025 (Sep, 27).

Information Security Alliance (ISA). **Cyber-Insurance Metrics and Impact on Cyber-Security** [Online]. Available URL://https://obamawhitehouse.archives.gov/files/documents/cyber/ISA%20-%20Cyber-Insurance%20Metrics%20and%20Impact%20on%20Cyber-Security.pdf, 2025 (Sep, 27).

Insurance Risk and Finance Research Centre (IRFRC). **Cyber Risk Management Project Brief (CyRiM)** [Online]. Available URL://https://www.ntu.edu.sg/irfrc/research/cyrim/project-brief, 2025 (Sep, 27).

Lloyd's Market Association. **LMA20-031-PD: Cyber Risks Endorsements**. [Online]. Available URL://https://www.lmalloyds.com/LMA/LMA_Bulletins/LMA20-031-PD.aspx, 2025 (July, 19).

Monetary Authority of Singapore (MAS). **Cyber Security Regulations** [Online]. Available URL://https://www.mas.gov.sg/regulation/cyber-security, 2025 (Sep, 27).

Monetary Authority of Singapore. **Guidelines on Technology Risk Management (TRM).** [Online]. Available URL://https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines, 2025 (July, 19).

Monetary Authority of Singapore. **Technology Risk Management Guidelines.** [Online]. Available URL://https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf, 2025 (July, 19).

National Institute of Standards and Technology (NIST), **Computer Security Incident Handling Guide**, (Gaithersburg, MD: U.S. Department of Commerce, 2012).

Organisation for Economic Co-operation and Development (OECD). **Encouraging Clarity in Cyber Insurance Coverage**. [Online]. Available URL://https://web-archive.oecd.org/2020-08-18/546620-Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf, 2025 (July, 19).

Organisation for Economic Co-operation and Development (OECD). **Enhancing the Role of Insurance in Cyber Risk Management** (Paris: OECD Publishing, 2017).

Ponemon Institute. **2014 Global Report on the Cost of Cyber Crime** [Online]. Available URL://https://www.ponemon.org/news-updates/blog/security/2014-global-report-on-the-cost-of-cyber-crime.html, 2025 (Sep, 27).

Samantha Ward and Eleanor Matthews. **On the (Cyber) Attack: How Are the FCA and PRA Regulating Cyber Risk?** [Online]. Available URL://https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2023/11/on-the-cyber-attack.pdf, 2025 (Sep, 27).

University of Cambridge Centre for Risk Studies. **Cyber Insurance Exposure Data Schema v1.0** [Online]. Available URL://https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-cyber-data-schema-v1.0.pdf, 2025 (Sep, 27).