

การวางมาตรการทางกฎหมายเพื่อป้องกันการละเมิดข้อมูลและการโจมตีทางไซเบอร์ในมหาวิทยาลัย

Legal Measures to Prevent Data Breaches and Cyber Attacks in Universities

ชาตรี จำลองกุล¹, ยัตติพิชัย กลิ่นเจริญ^{1*}, พิสิฐพล พานรัตน์¹ และปราโมทย์ สิทธิจักร²

Chatree Jamlongkul¹, Yatpichai Klincharoen^{1*}, Pisitphon Panurat¹, and Pramote Sittijuk²

Received: 16 January 2025 Revised: 20 March 2025 Accepted: 15 August 2025

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อ (1) ศึกษาสภาพปัญหาและผลกระทบของการละเมิดข้อมูลและการโจมตีทางไซเบอร์ในมหาวิทยาลัย และ (2) พัฒนาแผนป้องกันภัยและกฎระเบียบบนฐานของมาตรการทางกฎหมายเพื่อป้องกันภัยคุกคามดังกล่าว ผู้ให้ข้อมูลสำคัญประกอบด้วย อธิการบดี รองอธิการบดีฝ่ายแผนและพัฒนา เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ และนักวิชาการด้านกฎหมาย รวมทั้ง 11 คน เครื่องมือที่ใช้ในการวิจัยประกอบด้วย 2 ส่วน ได้แก่ (1) แบบสัมภาษณ์เพื่อศึกษาสภาพปัญหาและผลกระทบของการละเมิดข้อมูลและการโจมตีทางไซเบอร์ และ (2) แบบรวบรวมข้อมูลสำหรับการระดมสมองในรูปแบบการสนทนากลุ่มเพื่อพัฒนาแผนป้องกันภัยและกฎระเบียบที่สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) พ.ศ. 2562 เครื่องมือวิจัยได้รับการตรวจสอบโดยผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์และกฎหมาย 3 ท่าน ซึ่งดัชนีความตรงเชิงเนื้อหา มีค่ามากกว่า 0.70 แสดงให้เห็นถึงความตรงตามวัตถุประสงค์ของการวิจัย

ผลการวิจัยพบว่า สภาพปัญหาและผลกระทบของการละเมิดข้อมูลและการโจมตีทางไซเบอร์ในมหาวิทยาลัย ได้แก่ (1) การเผยแพร่ข้อมูลส่วนบุคคลบนเว็บไซต์มหาวิทยาลัย (2) การโจมตีด้วยไวรัสเรียกค่าไถ่ต่อเซิร์ฟเวอร์ฐานข้อมูลวิจัย และ (3) การโจมตีเว็บไซต์ที่พัฒนาด้วย WordPress ซึ่งส่งผลกระทบต่อความปลอดภัยของข้อมูลและภาพลักษณ์ขององค์กร แนวทางแก้ไขที่เสนอ ได้แก่ การอัปเดตระบบและซอฟต์แวร์ การใช้เทคโนโลยีป้องกัน เช่น การเข้ารหัสและการยืนยันตัวตนหลายปัจจัย การฝึกอบรมบุคลากรด้าน PDPA และกฎหมายที่เกี่ยวข้อง อีกทั้งควรปรับปรุงเนื้อหาของกฎหมายเพื่อให้มีความชัดเจนและครอบคลุมทุกกรณีของการละเมิด พร้อมทั้งส่งเสริมมาตรการป้องกันในระดับองค์กรและบุคคล และการจัดสรรทรัพยากรเพื่อสร้างระบบความปลอดภัยที่ยั่งยืนและครบวงจร

คำสำคัญ: มาตรการทางกฎหมาย, การป้องกันการละเมิดข้อมูลและการโจมตีทางไซเบอร์

¹ อาจารย์ สาขาวิชานิติศาสตร์ คณะนิติศาสตร์ มหาวิทยาลัยพิษณุโลก

² อาจารย์ สาขาวิชาเทคโนโลยีสารสนเทศ คณะบริหารธุรกิจและการบัญชี มหาวิทยาลัยพิษณุโลก

¹ Lecturer, Major of Law, Faculty of Law, Phitsanulok University

² Lecturer, Major of Information Technology, Faculty of Business and Accounting, Phitsanulok University

* Corresponding author: Yatpichai Klincharoen, e-mail: yatpichaik@plu.ac.th

Abstract

This research aimed to (1) study the problems and impacts of data breaches and cyberattacks in universities and (2) develop a protection plan and regulations based on legal measures to prevent such threats. The key informants included the university rector, vice-rector for planning and development, IT staff, and legal academics, totaling 11 individuals. The research tools consisted of two parts: (1) an interview form to examine the problems and impacts of data breaches and cyberattacks and (2) a data collection process that utilized brainstorming in a group discussion format to develop a protection plan and regulations in accordance with the Personal Data Protection Act (PDPA) of 2019. The research tools were validated by three experts in cybersecurity and law, achieving a content validity index of over 0.70, indicating alignment with the research objectives.

The research findings revealed that the problems and impacts of data breaches and cyberattacks in universities included (1) the publication of personal data on the university website, (2) ransomware attacks on research database servers, and (3) cyberattacks on WordPress-based websites, all of which negatively affected data security and the institution's reputation. Proposed solutions included system and software updates, the implementation of preventive technologies such as encryption and multi-factor authentication, and personnel training on the PDPA and related laws. Additionally, improvements to legal provisions were suggested to ensure clarity and comprehensive coverage of breach scenarios. Promoting preventive measures at both organizational and individual levels and allocating resources to establish a sustainable and robust security system were also recommended.

Keywords: Legal Measures, Preventing Data Breaches and Cyberattacks

บทนำ

ปัจจุบันได้เข้าสู่ยุคดิจิทัลเต็มรูปแบบ ที่องค์กรทุกแห่งมักเผยแพร่ข้อมูลส่วนบุคคลและภาพรวมของฝ่ายและแผนกต่าง ๆ ผ่านสื่อแบบเอกสารและสื่อออนไลน์ในรูปแบบเว็บไซต์ อย่างไรก็ตาม หากข้อมูลเหล่านี้ ถูกจัดเก็บในระบบฐานข้อมูลที่ไม่มีความปลอดภัย และไม่มีมาตรการทางกฎหมายที่เข้มงวดเพื่อป้องกันภัย อาจเพิ่มความเสี่ยงต่อถูกละเมิดข้อมูลหรือการโจมตีทางไซเบอร์หลายด้านจากภายนอก ส่งผลให้สูญเสียข้อมูลสำคัญและเกิดการรั่วไหลของข้อมูลส่วนบุคคล ทำให้ความน่าเชื่อถือของมหาวิทยาลัยลดลงและ

สร้างความกังวลจากผู้เกี่ยวข้องทั้งภายในและภายนอกมหาวิทยาลัย ทั้งนี้ปัญหายุคคอมพิวเตอร์ทางไซเบอร์ในประเทศไทยมีจำนวนเพิ่มขึ้นและมีความรุนแรงมากขึ้น เนื่องจากประชาชนสามารถเชื่อมต่อทุกสิ่งเข้าสู่โลกอินเทอร์เน็ตทำให้สามารถเข้าถึงข้อมูลในองค์กรต่าง ๆ และสามารถควบคุมการใช้งานอุปกรณ์ต่าง ๆ ผ่านเครือข่ายได้อย่างง่ายดายและเป็นอิสระ จึงเป็นสาเหตุสำคัญให้องค์กรในยุคดิจิทัลส่วนใหญ่ตกอยู่ในความเสี่ยง (กฤษฎิ์ เหล่ากอ และสมบูรณ์สุข สำราญ, 2567)

รูปแบบการถูกละเมิดข้อมูลและโจมตีทางไซเบอร์ในมหาวิทยาลัยมักปรากฏในหลายรูปแบบ

เช่น การเข้าถึงโดยไม่ได้รับอนุญาตจากอาชญากรไซเบอร์ที่พยายามจะเข้าสู่ฐานข้อมูลผ่านวิธีต่างๆ เช่น การลอบแฉีกระบบหรือช่องโหว่ของซอฟต์แวร์เพื่อขโมยข้อมูลส่วนบุคคล ข้อมูลนักศึกษา ข้อมูลการเงิน หรือเอกสารสำคัญอื่นๆ การโจมตีทางโซเชียล และการหลอกลวงทางอินเทอร์เน็ต (Ting et al., 2024) รวมทั้งมัลแวร์และแรนซัมแวร์ถูกติดตั้งในเครือข่ายมหาวิทยาลัยเพื่อเข้ารหัสข้อมูลและเรียก ransomware เพื่อปลดล็อกข้อมูล การโจมตีบริการปฏิเสธการให้บริการ (DDoS) ซึ่งส่งผลทำให้เซิร์ฟเวอร์ เว็บไซต์ และแพลตฟอร์มการให้บริการทางการศึกษาออนไลน์ต่างๆ ของมหาวิทยาลัยล่มหรือไม่สามารถให้บริการได้ในชั่วขณะ หรือระยะเวลานาน

การวางมาตรการทางกฎหมายเพื่อป้องกันการละเมิดข้อมูลและการโจมตีทางไซเบอร์ในมหาวิทยาลัย สามารถดำเนินการให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งเป็นกฎหมายที่สร้างขึ้นเพื่อคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย โดยกำหนดกรอบการเก็บรวบรวม ใช้ และเผยแพร่ข้อมูลอย่างเหมาะสม เจ้าของข้อมูลมีสิทธิในการเข้าถึง แก้ไข และเพิกถอนความยินยอมในการใช้ข้อมูลได้ กฎหมายนี้ยังระบุถึงมาตรการความปลอดภัยที่ต้องมีเพื่อป้องกันการละเมิดข้อมูล รวมทั้งกำหนดบทลงโทษสำหรับการละเมิดกฎหมาย เพื่อสร้างมาตรฐานในการปกป้องข้อมูลส่วนบุคคลและเพิ่มความเชื่อมั่นในการจัดการข้อมูล (สำนักงานราชบัณฑิตยสภา, 2562) รวมทั้งการพัฒนาแผนป้องกันภัยไซเบอร์และกฎระเบียบในการรักษาความปลอดภัยข้อมูลที่เหมาะสมและมีประสิทธิภาพสำหรับทุกหน่วยงานในมหาวิทยาลัย เช่น การเข้ารหัสข้อมูล การจัดเก็บข้อมูลที่ปลอดภัย การติดตามการเข้าถึงข้อมูล และการทดสอบความปลอดภัยเป็นระยะ (Melchior and Soler, 2024) โดยการกำหนดมาตรการดังกล่าว จะดำเนินการ

ร่วมกับการสร้างแนวทางการเผยแพร่ความรู้เกี่ยวกับมาตรการทางกฎหมายไปยังบุคลากรในองค์กรอย่างครอบคลุม เพื่อให้ทุกคนเข้าใจบทบาทและหน้าที่ของตนในการป้องกันการละเมิดข้อมูลและการโจมตีไซเบอร์ และการตอบสนองต่อเหตุการณ์การโจมตีไซเบอร์ที่มีประสิทธิภาพและสอดคล้องกับข้อกำหนดทางกฎหมาย

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาสภาพปัญหาและผลกระทบของการละเมิดข้อมูลและการโจมตีทางไซเบอร์ในมหาวิทยาลัย
2. เพื่อพัฒนาแผนป้องกันภัย และกฎระเบียบบนฐานของมาตรการทางกฎหมายเพื่อป้องกันการละเมิดข้อมูลและการโจมตีทางไซเบอร์ในมหาวิทยาลัย

ทบทวนวรรณกรรม และงานวิจัยเกี่ยวข้อง

1. แนวคิดเกี่ยวกับการวางมาตรการทางกฎหมาย

การบังคับใช้มาตรการกับองค์กรนั้นมีความซับซ้อน เนื่องจากองค์กรมีโครงสร้างที่ซับซ้อนและพลวัตในการดำเนินงานที่แตกต่างจากบุคคลธรรมดา การตอบสนองขององค์กรต่อมาตรการภาครัฐจึงต้องคำนึงถึงกระบวนการรับรู้ข้อมูลและการตัดสินใจในหลายขั้นตอนทั้งจากระดับล่างขึ้นไปสู่ระดับบนและจากระดับบนลงไปสู่ระดับล่าง ซึ่งทำให้การสื่อสารมาตรการไปยังผู้มีอำนาจตัดสินใจหรือผู้ที่ปฏิบัติจริงในเรื่องนั้นเป็นสิ่งสำคัญที่จะทำให้การปฏิบัติตามมาตรการเป็นไปอย่างมีประสิทธิภาพ นอกจากนี้แต่ละองค์กรจะมีวัตถุประสงค์ในการจัดตั้งที่แตกต่างกัน เช่น บริษัทจำกัดและบริษัทมหาชนจำกัดตั้งขึ้นเพื่อกำไรให้แก่ผู้ถือหุ้น สมาคมจัดตั้งเพื่อกระทำการที่ไม่ใช่การหากำไร วิชาชีพชุมชนและวิชาชีพเพื่อ

สังคมจัดตั้งเพื่อสร้างรายได้และส่งเสริมการพึ่งพาตนเองของชุมชน มูลนิธิจัดตั้งเพื่อการกุศล แต่ในบางกรณีอาจมีการจัดตั้งองค์กรเพื่อจุดประสงค์ที่ไม่ถูกต้อง เช่น การหลบเลี่ยงภาษี หรือการฟอกเงิน ทำให้หน่วยงานที่กำกับดูแลต้องมีการตรวจสอบอย่างรอบคอบระหว่างการส่งเสริมการจัดตั้งและการลงทะเบียนองค์กรที่ฝ่าฝืนกฎหมาย ในการกำหนดความรับผิดชอบเมื่อมีการฝ่าฝืนมาตรการหน่วยงานที่เกี่ยวข้องต้องพิจารณาอย่างละเอียดว่าควรให้ใครเป็นผู้รับผิดชอบและวิธีการกำหนดความรับผิดชอบนั้นต้องมีผลในการป้องกันการกระทำผิดได้อย่างแท้จริง และในการกำหนดโทษต่อองค์กรเมื่อมีการฝ่าฝืนมาตรการ เช่น โทษปรับ การพักหรือยกเลิกใบอนุญาต ควรกำหนดอัตราโทษที่เหมาะสมเพื่อป้องกันการกระทำผิดในอนาคตและกระตุ้นให้มีระบบตรวจสอบภายในที่มีประสิทธิภาพ การออกมาตรการและการบังคับใช้อย่างเหมาะสมจะช่วยให้องค์กรสามารถดำเนินกิจการได้ตามกฎหมายและเป็นไปในทางที่ส่งเสริมสังคมอย่างยั่งยืน (อภิชน จันทรเสน, 2562)

2. หลักเกณฑ์ทางกฎหมายในการละเมิดข้อมูล

ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 ที่เผยแพร่เมื่อวันที่ 15 ธันวาคม 2565 ได้กำหนดแนวทางชัดเจนสำหรับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ซึ่งเป็นการให้ความสำคัญกับการปฏิบัติตามขั้นตอนที่โปร่งใสและรับผิดชอบต่อกรณีที่เกิดเหตุละเมิดข้อมูลส่วนบุคคล โดยเหตุละเมิดข้อมูลอาจเกิดจากหลายสาเหตุ เช่น การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ความผิดพลาดทางระบบคอมพิวเตอร์ การโจมตีทางไซเบอร์ หรืออุบัติเหตุที่ทำให้ข้อมูลส่วนบุคคลถูกเปิดเผยโดยไม่ตั้งใจ

ประกาศนี้มีความสำคัญ เนื่องจากหากการละเมิดข้อมูลส่วนบุคคลมีความเสี่ยงสูงที่อาจส่งผลกระทบต่อสิทธิและเสรีภาพของบุคคลเจ้าของข้อมูลจะต้องได้รับการแจ้งเตือนโดยเร็วที่สุด เพื่อให้พวกเขาสามารถดำเนินการแก้ไขสถานการณ์และลดความเสียหายที่อาจเกิดขึ้นได้ โดยการแจ้งต้องมีข้อมูลสำคัญ เช่น ลักษณะของการละเมิด ช่องทางการติดต่อบุคคลที่รับผิดชอบ (เช่น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือ DPO) และผลกระทบที่อาจเกิดขึ้น นอกจากนี้ยังต้องมีการชี้แจงมาตรการในการแก้ไขและแนวทางที่เจ้าของข้อมูลสามารถดำเนินการเพื่อป้องกันและลดผลกระทบจากเหตุละเมิดนี้ (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2565)

การแจ้งเหตุละเมิดข้อมูลที่มีความรวดเร็ว เป็นสิ่งสำคัญ เนื่องจากช่วยให้เจ้าของข้อมูลสามารถดำเนินการที่จำเป็น เช่น การเปลี่ยนรหัสผ่าน การติดตามการใช้งานข้อมูลส่วนบุคคล หรือการติดต่อหน่วยงานที่เกี่ยวข้อง เช่น ธนาคาร หรือบริการออนไลน์ เพื่อป้องกันการใช้ข้อมูลที่ถูกละเมิด การปฏิบัติตามแนวทางนี้จะช่วยเสริมสร้างระบบการปกป้องข้อมูลส่วนบุคคลและลดความเสี่ยงจากเหตุละเมิดในอนาคต

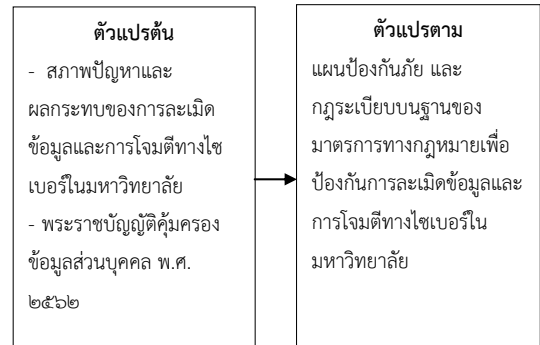
3. งานวิจัยที่เกี่ยวข้อง

เกียรตินิยม รัชงาม และสังเวียน เทพผา (2567) ศึกษาเปรียบเทียบมาตรการกฎหมายคุ้มครองข้อมูลส่วนบุคคลระหว่างต่างประเทศและประเทศไทย พบว่ากฎหมาย GDPR ของสหภาพยุโรปและ CCPA ของสหรัฐอเมริกา มีมาตรการคุ้มครองที่ครอบคลุมและบทลงโทษที่เข้มงวดกว่าเมื่อเทียบกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศไทย ซึ่งเน้นป้องกันอาชญากรรมไซเบอร์ แต่ยังขาดรายละเอียดในการคุ้มครองข้อมูลส่วนบุคคล รวมถึงทรัพยากรและกลไกการบังคับใช้ที่มีประสิทธิภาพ ในขณะที่ต่างประเทศให้ความสำคัญ

สำคัญกับการปรับปรุงกฎหมายตามเทคโนโลยี และมีการสร้างความร่วมมือระหว่างประเทศและหน่วยงานเฉพาะทาง ในงานวิจัยนี้ได้เสนอแนะ การพัฒนากฎหมายที่ต้องคำนึงถึงหน้าที่ของผู้ควบคุมข้อมูล การพัฒนาโครงสร้างพื้นฐาน สร้างความร่วมมือระหว่างประเทศ และการมีกฎหมายที่เข้มงวด ที่สนับสนุนด้วยระบบที่มีประสิทธิภาพ ซึ่งจะสามารถช่วยลดอัตราอาชญากรรมไซเบอร์ได้

ในงานวิจัยของ Amo-Filva et al. (2024) พบว่า สถาบันการศึกษาหลายแห่งที่ใช้ งานซอฟต์แวร์จากผู้ให้บริการบนคลาวด์ นำมาซึ่ง ความทำลายและข้อกังวลเฉพาะเกี่ยวกับความ เป็นส่วนตัวและความปลอดภัยของข้อมูลนักเรียน ดังนั้นสถาบันการศึกษาควรมีแผนที่มุ่งเน้นการ ส่งเสริมการใช้งานเครื่องมือดิจิทัลอย่างมีความรับผิดชอบ และการพัฒนาความปลอดภัยของข้อมูลใน การจัดการข้อมูลด้านการศึกษาและข้อมูลเชิง วิชาการต่างๆ รวมทั้งการเพิ่มความตระหนักรู้และ เสริมสร้างการป้องกันข้อมูลในสถาบันการศึกษา บนฐานของการใช้ทรัพยากรที่มีอยู่ในให้เกิด ประสิทธิภาพสูงสุด ทั้งนี้ในงานวิจัยของชรินทร์ทิพย์ ปันสุวรรณ และสมนทิพย์ จิตสว่าง (2565) ได้แนะนำเกี่ยวกับมาตรการกำกับดูแลและการ บังคับใช้นโยบายด้านความมั่นคงปลอดภัย ไซเบอร์ในองค์กร โดยที่องค์กรควรดำเนินการจัด ทำนโยบายและแนวทางปฏิบัติในการจัดการความ เสี่ยง รวมถึงการประเมินความเสี่ยงให้อยู่ในระดับ ที่ยอมรับได้ และต้องปรับปรุงกฎหมายไซเบอร์ให้ มีความชัดเจนและมีบทลงโทษที่เหมาะสม เพื่อ เสริมสร้างความตระหนักรู้และการป้องกันภัย คุกคามไซเบอร์ รวมทั้งหน่วยงานควรสร้าง มาตรการในการจัดการภัยคุกคามไซเบอร์ที่รองรับ สถานการณ์ที่จะเกิดขึ้นในอนาคต

กรอบแนวคิดงานวิจัย



ภาพที่ 1 กรอบแนวคิดงานวิจัย

ขอบเขตการวิจัย

การวิจัยนี้มุ่งศึกษาสภาพปัญหาและผล กระทบของการโจมตีทางไซเบอร์ในมหาวิทยาลัย พิษณุโลก พร้อมพัฒนาแผนป้องกันภัยและกฎ ระเบียบบนฐานมาตรการทางกฎหมาย เพื่อ ป้องกันการละเมิดข้อมูลและภัยคุกคามไซเบอร์ โดยนำเสนอแนวทางป้องกันและพัฒนาแผน ป้องกันที่สามารถเป็นต้นแบบให้มหาวิทยาลัย เอกชนและรัฐบาลอื่นๆ ได้

วิธีการวิจัย

1. ประชากรที่เป็นผู้ให้ข้อมูลสำคัญ ได้แก่ 1) อธิการบดี และรองอธิการบดีฝ่ายแผน และพัฒนา 2) หัวหน้างาน และเจ้าหน้าที่ฝ่าย เทคโนโลยีสารสนเทศ จำนวน 4 คน และ 3) นัก วิชาการด้านกฎหมายของมหาวิทยาลัยพิษณุโลก จำนวน 5 คน รวมจำนวนทั้งหมด 11 คน
2. การสร้างและตรวจสอบคุณภาพ เครื่องมือการวิจัย

2.1 การสร้างเครื่องมือการวิจัย

ประกอบด้วยเครื่องมือการวิจัย

2 ประเภท ดังนี้

2.1.1 การสร้างแบบสัมภาษณ์ เพื่อศึกษาสภาพปัญหาและผลกระทบของการละเมิดข้อมูลและการโจมตีทางไซเบอร์ในมหาวิทยาลัย สำหรับหัวหน้างาน และเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศและเครือข่ายการสื่อสารข้อมูล เพื่อสอบถามและทบทวนเอกสารที่เกี่ยวข้องกับสภาพปัญหา ผลกระทบ และรายงานข้อมูลทางสถิติในการถูกละเมิดข้อมูลและการโจมตีทางไซเบอร์ที่ผ่านมา 5 ปีย้อนหลังของมหาวิทยาลัย

2.1.2 การสร้างแบบรวบรวมข้อมูลเพื่อระดมสมองในรูปแบบการสนทนากลุ่ม เพื่อพัฒนาแผนป้องกันภัย และกฎระเบียบการป้องกันการละเมิดข้อมูลและการโจมตีทางไซเบอร์สำหรับอธิการบดี รองอธิการบดีฝ่ายแผนและพัฒนา และหัวหน้างานเทคโนโลยีสารสนเทศและเครือข่ายการสื่อสารข้อมูล เพื่อรวบรวมข้อมูลเกี่ยวกับรูปแบบของแผนป้องกันภัย และกฎระเบียบป้องกันการละเมิดข้อมูลและการโจมตีทางไซเบอร์ในมหาวิทยาลัย ที่สอดคล้องกับมาตรการทางกฎหมายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยได้กำหนดกรอบคำถามที่ครอบคลุมประเด็นสำคัญ ได้แก่ รูปแบบของแผนป้องกันภัยคุกคามไซเบอร์ที่ควรนำมาใช้ กฎระเบียบในการจัดการข้อมูลส่วนบุคคลที่สอดคล้องกับมาตรการทางกฎหมาย แนวทางในการจัดสรรทรัพยากรและงบประมาณที่เพียงพอ และข้อเสนอแนะในการปรับปรุงแผนพัฒนามหาวิทยาลัยให้รองรับภัยคุกคามไซเบอร์ในอนาคต

2.2 การตรวจสอบคุณภาพเครื่องมือการวิจัย แบบสัมภาษณ์ และแบบรวบรวมข้อมูล ในข้อ 2.1.1 และ 2.1.2 จะผ่านการตรวจสอบโดยผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ และผู้เชี่ยวชาญด้านกฎหมายจำนวนทั้งหมด 3 คน เพื่อให้มั่นใจว่าข้อคำถามในเครื่องมือมีความตรงกับวัตถุประสงค์ของการวิจัย ซึ่งผลการประเมินพบว่า ค่า Index of Content Validity (IOC) ของ

ทั้งสัมภาษณ์ และแบบรวบรวมข้อมูลมีค่ามากกว่า 0.70 ซึ่งแสดงให้เห็นว่ามีความตรงตามวัตถุประสงค์ของการวิจัยเป็นอย่างดี ไม่มีคำถามใดที่ถูกตัดออกหรือมีความคลาดเคลื่อนจากวัตถุประสงค์หลักของการวิจัย มีเพียงบางคำถามได้รับการปรับปรุงเพื่อสื่อความหมายไปในทิศทางเดียวและมีความชัดเจนยิ่งขึ้น และการปรับปรุงการใช้ภาษาในการตั้งคำถามที่เข้าใจง่ายยิ่งขึ้น

3. การรวบรวมข้อมูล

ใช้วิธีบันทึกเสียงด้วยสมาร์ตโฟนโดยได้ไฟล์เสียงในรูปแบบ .MP3 จากนั้นใช้โปรแกรมทางปัญญาประดิษฐ์ (AI for Speech-to-Text) ที่ให้บริการออนไลน์ เพื่อแปลงเสียงเป็นข้อความ และใช้โปรแกรม ChatGPT ในการตรวจสอบและสรุปเนื้อหาที่รวบรวมได้จากผู้ให้ข้อมูลสำคัญ

4. การวิเคราะห์ข้อมูล

แบบสัมภาษณ์ และแบบรวบรวมข้อมูล ใช้การวิเคราะห์เชิงเนื้อหาเพื่อสรุปและจำแนกสภาพปัญหา ผลกระทบ แนวทางการสร้างแผนและกฎระเบียบบนฐานของมาตรการทางกฎหมาย เพื่อป้องกันการละเมิดข้อมูลและการโจมตีทางไซเบอร์ในมหาวิทยาลัย

ผลการวิจัย

ผลการศึกษาสภาพปัญหาและผลกระทบของการละเมิดข้อมูลและการโจมตีทางไซเบอร์ในมหาวิทยาลัย รอบ 5 ปีที่ผ่านมา สรุปได้ดังนี้

1.1 การเผยแพร่ข้อมูลส่วนบุคคลบนเว็บไซต์และความเสี่ยงต่อความเป็นส่วนตัวและความปลอดภัยของข้อมูล

ผู้ให้ข้อมูลกล่าวว่า “บุคลากรของมหาวิทยาลัยบางส่วน ได้รับการรบกวนจากการโทรสแปมหรือข้อความขยะที่ทำให้ความเป็นส่วนตัวของพวกเขาถูกรบกวน ทั้งนี้อาจเนื่องมาจากการเผยแพร่ข้อมูลส่วนตัว เช่น หมายเลข

โทรศัพท์และอีเมลของบุคลากรบนเว็บไซต์อาจเพิ่มความเสี่ยงต่อความเป็นส่วนตัวและความปลอดภัยของข้อมูล ความเสี่ยงนี้อาจส่งผลกระทบต่อภาพลักษณ์ของมหาวิทยาลัย เนื่องจากการเผยแพร่ข้อมูลส่วนตัวอาจทำให้ความเชื่อมั่นในความปลอดภัยและการดูแลข้อมูลของมหาวิทยาลัยลดลง”

“ในการแก้ไขปัญหาดังกล่าว ควรมีการทบทวนและปรับปรุงนโยบายการจัดการข้อมูลเพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต รวมถึงการใช้มาตรการรักษาความปลอดภัย เช่น การเข้ารหัส การจำกัดการเข้าถึง และการใช้ระบบการยืนยันตัวตนหลายขั้นตอน ฝึกอบรมบุคลากรเกี่ยวกับวิธีการรักษาความปลอดภัยข้อมูลและการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และควรตรวจสอบและบำรุงรักษาระบบเว็บไซต์อย่างสม่ำเสมอ เพื่อลดช่องโหว่ที่อาจถูกใช้ในการแอบดูข้อมูลส่วนบุคคลและอีเมลที่เผยแพร่บนเว็บไซต์”

1.2 การถูกโจมตีทางไซเบอร์ด้วยไวรัสเรียกค่าไถ่ต่อเซิร์ฟเวอร์ฐานข้อมูลวิจัยของมหาวิทยาลัย

ผู้ให้ข้อมูลกล่าวว่า “มหาวิทยาลัยได้ประสบปัญหาที่สำคัญจากการโจมตีทางไซเบอร์ด้วยไวรัสเรียกค่าไถ่ที่เป้าหมายคือเซิร์ฟเวอร์ฐานข้อมูลวิจัย ซึ่งใช้จัดเก็บข้อมูลการวิจัยสำคัญและข้อมูลส่วนบุคคลของนักวิจัย การโจมตีนี้ทำให้ข้อมูลที่มีค่าหลายประเภทสูญหาย เช่น ข้อมูลการทดลอง ข้อมูลทางสถิติ และข้อมูลการศึกษา การเข้าถึงข้อมูลไม่ได้เป็นระยะเวลาหนึ่ง และชุดคำสั่งของโปรแกรมได้เสียหาย จนทำให้นักพัฒนาต้องใช้เวลาในการติดตั้งโปรแกรมใหม่เพื่อให้บริการเว็บกลับมาได้ตามปกติ ผลกระทบจากการโจมตีนี้ทำให้เกิดการสูญเสียข้อมูลสำคัญ และส่งผลกระทบต่อการทำงานและการเรียนการสอน มหาวิทยาลัยต้องใช้ทรัพยากรเพื่อกู้คืนข้อมูลที

สูญหาย และอาจต้องใช้เงินทุนเพิ่มเติมในการฟื้นฟูระบบและการบำรุงรักษาความปลอดภัย การโจมตีทำให้การทำงานวิจัยของนักวิจัยไม่สามารถดำเนินการได้ตามปกติ เนื่องจากข้อมูลที่จำเป็นสูญหายหรือไม่สามารถเข้าถึงได้ ซึ่งส่งผลกระทบต่อการจัดการเรียนการสอนเช่นกัน”

“ทั้งนี้เพื่อแก้ไขปัญหาดังกล่าวและป้องกัน

การโจมตีในอนาคต มหาวิทยาลัยควรดำเนินการในการแก้ไขปัญหาด้วยวิธีการต่าง ๆ เช่น อัปเดตซอฟต์แวร์และระบบปฏิบัติการให้เป็นเวอร์ชันล่าสุดเสมอ ใช้ซอฟต์แวร์ป้องกันไวรัสและเครื่องมือการตรวจจับการโจมตี ฝึกอบรมบุคลากรเกี่ยวกับการรักษาความปลอดภัยข้อมูลและวิธีป้องกันตัวเองจากการโจมตี ใช้ระบบสำรองข้อมูลที่เชื่อถือได้และสามารถกู้คืนข้อมูลได้รวดเร็วในกรณีที่เกิดการโจมตี และติดตั้งระบบการเข้ารหัสและ SSL/TLS เพื่อป้องกันการดักข้อมูลและการโจมตีทางไซเบอร์อื่น ๆ การดำเนินการตามแนวทางเหล่านี้จะช่วยลดความเสี่ยงจากการโจมตีด้วยไวรัสเรียกค่าไถ่ และรักษาความปลอดภัยของเซิร์ฟเวอร์ฐานข้อมูลวิจัยและข้อมูลของมหาวิทยาลัยได้อย่างมีประสิทธิภาพ”

1.3 การถูกโจมตีทางไซเบอร์ต่อเว็บไซต์มหาวิทยาลัยที่ใช้โปรแกรม WordPress

ผู้ให้ข้อมูลกล่าวว่า “มหาวิทยาลัยได้ประสบปัญหาการโจมตีทางไซเบอร์ที่มุ่งทำลายเว็บไซต์ของมหาวิทยาลัย ซึ่งพัฒนาโดยใช้โปรแกรม WordPress โดยผลการวิเคราะห์พบว่า เว็บไซต์ที่พัฒนามบนแพลตฟอร์ม WordPress อาจมีช่องโหว่สำคัญที่ต้องทำการตั้งค่าความปลอดภัยบนเครื่องเซิร์ฟเวอร์และอุดช่องโหว่ด้านความปลอดภัยแบบหลายวิธี เช่น SQL Injection หรือ Cross-Site Scripting (XSS) ผู้โจมตีสามารถใช้ช่องโหว่ของระบบหรือปลั๊กอินที่ไม่ได้รับการอัปเดตเพื่อเข้ามาปรับเปลี่ยนเนื้อหาของหน้าเว็บไซต์ได้อย่างง่ายดาย การไม่ดูแลรักษาระบบอย่างเพียงพอ

ทำให้มหาวิทยาลัยตกอยู่ในความเสี่ยงจากการโจมตีทางไซเบอร์ ซึ่งผลกระทบจากการโจมตีนี้มีความหลากหลายและรุนแรง มหาวิทยาลัยต้องเผชิญกับความเสี่ยงด้านภาพลักษณ์จากการที่ข้อมูลส่วนบุคคลของผู้เยี่ยมชมเว็บไซต์อาจถูกบุกรุก ขาดความเชื่อมั่นในความปลอดภัย ส่งผลกระทบต่อภาพลักษณ์ของมหาวิทยาลัย ความเสียหายทางการเงินจากการต้องใช้ทรัพยากรในการแก้ไขปัญหา รวมถึงค่าปรับหากข้อมูลส่วนบุคคลรั่วไหล ความเสี่ยงด้านกฎหมายจากการไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และผลกระทบต่อการเรียนการสอนและบริการออนไลน์ที่มหาวิทยาลัยจัดให้กับนักศึกษา”

“ทั้งนี้ เพื่อแก้ไขปัญหาดังกล่าวและป้องกันการโจมตีในอนาคต มหาวิทยาลัยควรดำเนินการในการแก้ไขปัญหาด้วยวิธีการต่างๆ เช่น อัปเดตระบบ WordPress และปลั๊กอินให้เป็นเวอร์ชันล่าสุด ใช้ปลั๊กอินความปลอดภัยที่สามารถตรวจสอบการโจมตีได้ ใช้เทคนิคการยืนยันตัวตนหลายขั้นตอน (MFA) สำรองข้อมูลและเตรียมแผนฟื้นฟูระบบ ฝึกอบรมบุคลากรเกี่ยวกับความเสี่ยงและวิธีการปฏิบัติที่ปลอดภัย และติดตั้ง SSL/TLS เพื่อป้องกันการดักข้อมูลระหว่างการส่งข้อมูล การดำเนินการตามแนวทางเหล่านี้จะช่วยลดความเสี่ยงจากการโจมตีทางไซเบอร์และรักษาความปลอดภัยของเว็บไซต์และข้อมูลของมหาวิทยาลัยได้อย่างมีประสิทธิภาพ”

ผลการพัฒนาแผนป้องกันภัยและกฎระเบียบบนฐานของมาตรการทางกฎหมายเพื่อป้องกันการละเมิดข้อมูลและการโจมตีทางไซเบอร์ในมหาวิทยาลัย

การพัฒนาแผนป้องกันภัยและกฎระเบียบบนฐานของมาตรการทางกฎหมายเพื่อป้องกัน การละเมิดข้อมูลและการโจมตีทางไซเบอร์ในมหาวิทยาลัย ได้มาจากผลการระดมสมอง เพื่อนำปัญหาที่ค้นพบ 3 ประการ ได้แก่ 1) การเผยแพร่ข้อมูลส่วนบุคคลบนเว็บไซต์และความเสี่ยงต่อความเป็นส่วนตัวและความปลอดภัยของข้อมูล 2) การถูกโจมตีทางไซเบอร์ด้วยไวรัสเรียกค่าไถ่ต่อเซิร์ฟเวอร์ฐานข้อมูลวิจัยของมหาวิทยาลัย และ 3) การถูกโจมตีทางไซเบอร์ต่อเว็บไซต์มหาวิทยาลัยที่ใช้โปรแกรม WordPress มาพัฒนาและเสนอเป็นแผนป้องกันภัย และกฎระเบียบการป้องกันการละเมิดข้อมูลและการโจมตีทางไซเบอร์ที่มีความสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และใช้การจัดสรรทรัพยากรและงบประมาณที่คุ้มค่าสอดคล้องกับแผนกลยุทธ์การพัฒนามหาวิทยาลัยในปี 2567 ทั้งนี้องค์ความรู้ดังกล่าวได้ถูกสร้างและกลั่นกรองมาจากอธิการบดี รองอธิการบดีฝ่ายแผนและพัฒนา และหัวหน้างานเทคโนโลยีสารสนเทศและเครือข่ายการสื่อสารข้อมูล และนักวิชาการด้านกฎหมายของมหาวิทยาลัย สรุปได้ดังนี้

ตารางที่ 1 ผลการพัฒนาแผนป้องกันภัยและกฎระเบียบบนฐานของมาตรการทางกฎหมายเพื่อป้องกันการละเมิดข้อมูลและการโจมตีทางไซเบอร์ในมหาวิทยาลัย

หัวข้อปัญหา	แนวทางป้องกัน	มาตรการทางกฎหมาย	ผลลัพธ์ที่คาดหวัง
การเผยแพร่ข้อมูลส่วนบุคคลบนเว็บไซต์	<ul style="list-style-type: none"> - กำหนดนโยบายหลักเกี่ยวกับการเผยแพร่ข้อมูลส่วนตัวโดยไม่จำเป็น - ใช้ระบบยืนยันตัวตนหลายขั้นตอน (MFA) - ใช้มาตรการเข้ารหัสข้อมูล (Data Encryption) - ฝึกอบรมบุคลากรเกี่ยวกับ PDPA และการปฏิบัติที่เหมาะสม 	<ul style="list-style-type: none"> - บังคับใช้กฎหมาย PDPA - กำหนดบทลงโทษสำหรับการละเมิด - แต่งตั้ง DPO เพื่อควบคุมและแนะนำการปฏิบัติตามกฎหมาย 	<ul style="list-style-type: none"> - เพิ่มความปลอดภัยข้อมูลส่วนบุคคล - ลดความเสี่ยงต่อการละเมิดข้อมูล - เสริมสร้างความมั่นใจให้เจ้าของข้อมูลส่วนบุคคล
การโจมตีทางไซเบอร์ด้วยไวรัสเรียกค่าไถ่	<ul style="list-style-type: none"> - อัปเดตระบบปฏิบัติการและซอฟต์แวร์ป้องกันไวรัส - ใช้ระบบ IDPS - ตั้งค่าระบบสำรองข้อมูลแบบ Offline Backup - ฝึกอบรมบุคลากรเกี่ยวกับวิธีการป้องกันการโจมตี 	<ul style="list-style-type: none"> - บังคับใช้กฎหมายอาชญากรรมทางคอมพิวเตอร์ - สร้างความร่วมมือระหว่างมหาวิทยาลัยและหน่วยงานด้านกฎหมาย 	<ul style="list-style-type: none"> - ลดความเสี่ยงจากไวรัสเรียกค่าไถ่ - ป้องกันข้อมูลสำคัญสูญหาย - เพิ่มประสิทธิภาพการกู้คืนข้อมูลในกรณีฉุกเฉิน
การโจมตีทางไซเบอร์ต่อเว็บไซต์ WordPress	<ul style="list-style-type: none"> - อัปเดต WordPress และปลั๊กอิน - ใช้ปลั๊กอินเพิ่มความปลอดภัย เช่น Wordfence Security - ติดตั้ง SSL/TLS Certificates - ตรวจสอบช่องโหว่เว็บไซต์อย่างสม่ำเสมอ - ใช้ระบบ MFA และ Access Control 	<ul style="list-style-type: none"> - ปฏิบัติตามกฎหมาย PDPA - ระบุมบทลงโทษในกรณีละเมิดความปลอดภัย 	<ul style="list-style-type: none"> - เพิ่มความปลอดภัยเว็บไซต์ - ลดโอกาสการถูกโจมตี - เสริมสร้างความน่าเชื่อถือในระบบเว็บไซต์ของมหาวิทยาลัย

จากตารางที่ 1 สรุปได้ว่าแผนป้องกันภัยและกฎระเบียบบนพื้นฐานของมาตรการทางกฎหมาย เพื่อเพิ่มความปลอดภัยของข้อมูลและลดความเสี่ยงจากการโจมตีทางไซเบอร์ในมหาวิทยาลัย โดยครอบคลุม 3 ประเด็นหลัก ได้แก่ การป้องกันการเผยแพร่ข้อมูลส่วนบุคคลบนเว็บไซต์, การรับมือกับการโจมตีด้วยไวรัสเรียกค่าไถ่, และการป้องกันการโจมตีเว็บไซต์ WordPress

มาตรการที่นำเสนอประกอบด้วยแนวทางป้องกัน เช่น การกำหนดนโยบายด้านความปลอดภัย, การใช้เทคโนโลยีป้องกัน เช่น การเข้ารหัสข้อมูล, การใช้ระบบยืนยันตัวตนหลายขั้นตอน, และการอัปเดตซอฟต์แวร์อย่างสม่ำเสมอ นอกจากนี้ ยังเน้นการฝึกอบรมบุคลากรให้มีความรู้เกี่ยวกับกฎหมายที่เกี่ยวข้อง เช่น PDPA และกฎหมายอาชญากรรมทางคอมพิวเตอร์

ผลลัพธ์ที่คาดหวังคือการเพิ่มความปลอดภัยของข้อมูลส่วนบุคคล, ลดความเสี่ยงจากการโจมตี, และเสริมสร้างความน่าเชื่อถือให้กับระบบของมหาวิทยาลัย ทั้งนี้ การบังคับใช้

มาตรการทางกฎหมายควบคู่ไปกับการปฏิบัติตามแนวทางป้องกัน จะช่วยสร้างสภาพแวดล้อมทางไซเบอร์ที่ปลอดภัยและยั่งยืน

ตารางที่ 2 ผลการวิเคราะห์ความครอบคลุมและช่องโหว่ของกฎหมายเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลหรือโจมตีทางไซเบอร์

หัวข้อปัญหา	บทลงโทษทางแพ่ง	บทลงโทษทางอาญา	บทลงโทษทางปกครอง	การวิเคราะห์ความครอบคลุมและช่องโหว่ของกฎหมาย
การเผยแพร่ข้อมูลส่วนบุคคลบนเว็บไซต์	- ชดใช้ค่าสินไหมทดแทนตามความเสียหายจริง - ศาลอาจเพิ่มค่าสินไหมทดแทนได้สูงสุดสองเท่าของค่าสินไหมทดแทนที่แท้จริง	- จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ	- ปรับสูงสุดไม่เกิน 5,000,000 บาท	ความครอบคลุมของกฎหมาย : กฎหมายยังขาดความชัดเจนในการบังคับใช้และตรวจสอบกรณีการละเมิดในทางปฏิบัติ การลงโทษอาจไม่รุนแรงพอในบางกรณี ช่องโหว่ของกฎหมาย : กฎหมายไม่มีมาตรการบังคับองค์กรให้มีการป้องกันที่เข้มงวดก่อนการละเมิดเกิดขึ้น
การโจมตีทางไซเบอร์ด้วยไวรัสเรียกค่าไถ่	- ชดใช้ค่าสินไหมทดแทนสำหรับข้อมูลที่เสียหาย	- เข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต: จำคุกไม่เกิน 2 ปี หรือปรับไม่เกิน 40,000 บาท หรือทั้งจำทั้งปรับ - ทำให้ข้อมูลสูญหาย/เสียหาย: จำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ	- มาตรการทางกฎหมายเพิ่มเติมขึ้นอยู่กับความร้ายแรงของการละเมิด	ความครอบคลุมของกฎหมาย : กฎหมายช่วยสร้างแนวทางการลงโทษที่เหมาะสมตามระดับความร้ายแรงของการโจมตี ช่องโหว่ของกฎหมาย : ขาดมาตรการที่มุ่งเน้นการป้องกันในเชิงเทคโนโลยี เช่น การกำหนดมาตรฐานการสำรองข้อมูล หรือการบังคับใช้ IDPS
การโจมตีทางไซเบอร์ต่อเว็บไซต์ WordPress	- ชดใช้ค่าสินไหมทดแทนหากข้อมูลส่วนบุคคลรั่วไหล	- การแฮกหรือทำลายข้อมูล: จำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ	- ปรับสูงสุดไม่เกิน 5,000,000 บาทในกรณีข้อมูลส่วนบุคคลรั่วไหล	ความครอบคลุมของกฎหมาย : มีบทลงโทษที่ครอบคลุมการละเมิดข้อมูล แต่ยังไม่ชัดเจนในกรณีเว็บไซต์ที่ไม่ได้เก็บข้อมูลส่วนตัว ช่องโหว่ของกฎหมาย : กฎหมายยังไม่ระบุถึงมาตรการป้องกันที่เฉพาะเจาะจง เช่น การอัปเดตซอฟต์แวร์หรือการตรวจสอบช่องโหว่เว็บไซต์

จากตารางที่ 2 พบว่า กฎหมายในปัจจุบันมีบทลงโทษที่ครอบคลุมในระดับหนึ่ง ซึ่งครอบคลุมทั้งบทลงโทษทางแพ่ง อาญา และปกครอง อย่างไรก็ตาม ในทางปฏิบัติการบังคับใช้กฎหมายยังคงมีความล่าช้าและขาดความชัดเจนในหลายกรณี โดยเฉพาะกรณีที่ต้องการการพิจารณาอย่างละเอียดหรือการบังคับใช้มาตรการเชิงเทคนิคที่ซับซ้อน ช่องโหว่หลักของกฎหมายใน

ปัจจุบันคือการขาดมาตรการป้องกันที่มุ่งเน้นด้านเทคโนโลยีและแนวทางเชิงรุก เช่น การกำหนดมาตรฐานการป้องกันข้อมูลส่วนบุคคล การตรวจสอบช่องโหว่ของระบบ การอัปเดตซอฟต์แวร์อย่างต่อเนื่อง หรือการจัดให้มีระบบป้องกันภัยคุกคามทางไซเบอร์ (IDPS) ซึ่งจะช่วยลดความเสี่ยงจากการโจมตีได้ตั้งแต่ต้นทาง

ตารางที่ 3 แผนการจัดสรรทรัพยากรเพื่อป้องกันการละเมิดข้อมูลและการโจมตีทางไซเบอร์ในมหาวิทยาลัย

แผนการจัดสรรทรัพยากร	รายละเอียด	ผลลัพธ์ที่คาดหวัง	ความสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
1. การจัดสรรทรัพยากรบุคคล			
- ทีมงานความปลอดภัยไซเบอร์	แต่งตั้งทีมงานเฉพาะกิจ เฝ้าระวังและตอบสนองต่อภัยคุกคาม	เพิ่มความเร็วและประสิทธิภาพในการตอบสนองต่อภัยคุกคาม	การจัดตั้งทีมที่มีความเชี่ยวชาญในการจัดการข้อมูลและภัยคุกคามไซเบอร์ เพื่อคุ้มครองข้อมูลส่วนบุคคลตามมาตรการที่กำหนดในพระราชบัญญัติ
- การเพิ่มบุคลากร IT Security	จ้างผู้เชี่ยวชาญและอบรมบุคลากรเพื่อพัฒนาทักษะด้านความปลอดภัยข้อมูล	บุคลากรมีความรู้และความเชี่ยวชาญในการจัดการภัยไซเบอร์	การอบรมและการพัฒนาทักษะให้กับบุคลากรในด้านการรักษาความปลอดภัยของข้อมูลส่วนบุคคลตามมาตรฐานที่กำหนด
2. โครงสร้างพื้นฐาน			
- ติดตั้ง Firewall/ IDPS	อัปเดตระบบป้องกันภัยไซเบอร์ เช่น Firewall และ Intrusion Detection Systems	ลดความเสี่ยงจากการโจมตีทางไซเบอร์	การติดตั้งระบบป้องกันภัยไซเบอร์เพื่อปกป้องข้อมูลส่วนบุคคลจากการถูกโจมตีหรือการเข้าถึงโดยไม่ได้รับอนุญาต
- อัปเดตระบบ CMS	ปรับปรุง WordPress และติดตั้งปลั๊กอินเสริมความปลอดภัย	ลดช่องโหว่ของเว็บไซต์	การอัปเดตระบบเพื่อปิดช่องโหว่ที่อาจทำให้ข้อมูลส่วนบุคคลถูกเข้าถึงโดยไม่ได้รับอนุญาต
- การเข้ารหัสข้อมูล	ใช้ซอฟต์แวร์เข้ารหัสข้อมูลทั้งในฐานข้อมูลและการส่งข้อมูล	ป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต	การเข้ารหัสข้อมูลช่วยปกป้องข้อมูลส่วนบุคคลในระหว่างการเก็บรักษาและการส่งข้อมูลตามมาตรการคุ้มครองข้อมูลในพระราชบัญญัติ
3. การฝึกอบรมและพัฒนา			
- อบรม Cybersecurity Awareness	จัดอบรมบุคลากรด้านความปลอดภัยข้อมูลและ PDPA	เพิ่มความรู้ความเข้าใจในความปลอดภัยไซเบอร์	การอบรมเพื่อเพิ่มความรู้ด้านการคุ้มครองข้อมูลส่วนบุคคลและการปฏิบัติตาม PDPA ตามหลักการของพระราชบัญญัติ
- การจำลองการโจมตี	จ้างบริษัทภายนอกทำ Penetration Testing เพื่อค้นหาช่องโหว่	ค้นหาและแก้ไขช่องโหว่ในระบบ	การทดสอบช่องโหว่เพื่อป้องกันการรั่วไหลของข้อมูลส่วนบุคคลและการรักษาความปลอดภัยของข้อมูลตามมาตรการในพระราชบัญญัติ

จากตารางที่ 3 สรุปได้ว่า แผนการจัดสรรทรัพยากรเพื่อป้องกันการละเมิดข้อมูลและการโจมตีทางไซเบอร์ในมหาวิทยาลัย โดยครอบคลุม 3 ด้านสำคัญ ได้แก่ การจัดสรรทรัพยากรบุคคล การพัฒนาโครงสร้างพื้นฐาน และการฝึกอบรมและพัฒนาบุคลากร ทั้งหมดสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) เพื่อเสริมสร้างความปลอดภัยของข้อมูลและลดความเสี่ยงจากภัยคุกคาม

1. การจัดสรรทรัพยากรบุคคล: มีการแต่งตั้งทีมงานความปลอดภัยไซเบอร์เพื่อเฝ้าระวังและตอบสนองต่อภัยคุกคามโดยตรง รวมถึงการจ้างและพัฒนาทักษะบุคลากร IT Security เพื่อเพิ่มประสิทธิภาพในการจัดการข้อมูลและการป้องกันภัยไซเบอร์

2. โครงสร้างพื้นฐาน: ใช้เทคโนโลยีป้องกัน เช่น Firewall และระบบตรวจจับการบุกรุก (IDPS) พร้อมทั้งอัปเดตระบบ CMS และเข้ารหัสข้อมูล เพื่อปิดช่องโหว่และป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

3. การฝึกอบรมและพัฒนา: จัดอบรม Cybersecurity Awareness ให้บุคลากรเข้าใจในแนวทางปฏิบัติที่ปลอดภัยตามมาตรฐาน PDPA นอกจากนี้ ยังมีการจำลองการโจมตี (Penetration Testing) เพื่อค้นหาและแก้ไขช่องโหว่ในระบบ แผนดังกล่าวมุ่งเน้นให้มหาวิทยาลัยมีระบบความปลอดภัยที่ครบวงจร ลดความเสี่ยงจากการละเมิดข้อมูลและการโจมตีทางไซเบอร์ พร้อมสร้างความมั่นใจในความปลอดภัยของข้อมูลส่วนบุคคล

การอภิปรายผล สรุป และข้อเสนอแนะ

1. อภิปรายผลการวิจัย

ผลการวิจัยชี้ให้เห็นถึงความสำคัญที่มหาวิทยาลัยต้องมีมาตรการในการรักษาความปลอดภัยทางไซเบอร์ โดยเฉพาะการควบคุมการ

เปิดเผยข้อมูลส่วนบุคคลผ่านเว็บไซต์ ซึ่งเพิ่มความเสี่ยงต่อการถูกโจมตีจากบุคคลภายนอกที่ไม่หวังดี การเปิดเผยข้อมูลที่ไม่เหมาะสมสามารถส่งผลกระทบต่อความเป็นส่วนตัวและความเชื่อมั่นในองค์กรได้โดยตรง นอกจากนี้ การโจมตีด้วยไวรัสเรียกค่าไถ่ยังสร้างความเสียหายต่อข้อมูลสำคัญของมหาวิทยาลัย ส่งผลให้จำเป็นต้องลงทุนในระบบสำรองข้อมูลและเทคโนโลยีการเข้ารหัสเพื่อความปลอดภัยในระยะยาว ซึ่งสอดคล้องกับงานวิจัยของ Taresh Mehra (2024) สนับสนุนแนวคิดนี้โดยพบว่า การเข้ารหัสช่วยให้มั่นใจได้ว่าข้อมูลสำรองปลอดภัยและไม่สามารถเข้าถึงได้โดยผู้โจมตี ซึ่งเป็นวิธีป้องกันที่จำเป็นต่อแรนซัมแวร์ การนำเทคนิคการเข้ารหัสมาใช้กับกลยุทธ์การสำรองข้อมูลแบบครอบคลุมสามารถลดความเสี่ยงจากการสูญเสข้อมูล ความเสียหายทางการเงิน และการหยุดชะงักของการดำเนินงานได้อย่างมีนัยสำคัญ นอกจากนี้ การสร้างระบบป้องกันภัยคุกคามทางไซเบอร์ควรดำเนินการควบคู่กับการกำหนดระเบียบการป้องกันภัยและบทลงโทษที่เข้มงวดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ซึ่งเป็นแนวทางสำคัญในการลดความเสี่ยงและสร้างมาตรฐานความปลอดภัยด้านข้อมูล การนำมาตรการคุ้มครองข้อมูลส่วนบุคคลตาม PDPA มาใช้ในกระบวนการเก็บรักษาและส่งข้อมูล จะช่วยลดโอกาสการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และเพิ่มความมั่นใจให้แก่บุคลากรและนักศึกษาในระบบข้อมูลของสถาบันการศึกษา ซึ่งสอดคล้องกับงานวิจัยของ Miskam et al. (2023) ระบุว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) มีความสำคัญต่อสถาบันอุดมศึกษาเอกชน ซึ่งต้องปฏิบัติตามข้อกำหนดทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคลของกลุ่มเป้าหมายหลากหลาย เช่น พนักงาน นักศึกษา ศิษย์เก่า และบุคคลภายนอก เช่น ผู้ขายหรือผู้รับเหมา ผลการวิเคราะห์ความ

ครอบคลุมและช่องโหว่ของกฎหมายเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลหรือโจมตีทางไซเบอร์ พบว่ากฎหมายในปัจจุบันมีบทลงโทษที่ครอบคลุมในระดับหนึ่ง โดยครอบคลุมทั้งบทลงโทษทางแพ่งอาญา และปกครอง ซึ่งบทลงโทษทั้งทางอาญาและแพ่ง สำหรับผู้ละเมิดข้อมูลส่วนบุคคลหรือกระทำความผิดทางคอมพิวเตอร์ เช่น การแฮ็กข้อมูลหรือเผยแพร่ข้อมูลเท็จ โทษอาจจำคุกสูงสุดถึง 5 ปี และปรับสูงสุดถึง 1,000,000 บาท หรือทั้งจำทั้งปรับ และเจ้าของข้อมูลสามารถฟ้องเรียกค่าเสียหายได้ตามจำนวนจริง แต่ยังมีปัญหาในด้านการบังคับใช้ที่ล่าช้าและขาดความชัดเจน โดยเฉพาะในกรณีที่ต้องการมาตรการเชิงเทคนิคที่ซับซ้อน อีกทั้งกฎหมายยังมีช่องโหว่สำคัญในด้านการป้องกัน โดยขาดแนวทางที่เน้นการป้องกันเชิงเทคโนโลยี ทั้งนี้การเพื่อแก้ไขปัญหาเหล่านี้อย่างยิ่งย่น ควรปรับปรุงกฎหมายให้ชัดเจนและเพิ่มมาตรการป้องกันเชิงรุกเพื่อสร้างความมั่นคงด้านข้อมูลให้มีประสิทธิภาพยิ่งขึ้น นอกเหนือจากนั้นงานวิจัยนี้ได้เสนอวิธีการปรับใช้กฎหมาย PDPA ให้เหมาะสมกับสภาพปัญหา ทรัพยากร และงบประมาณขององค์กรที่ตั้งไว้ตามแผนกลยุทธ์ประจำปี ซึ่งจะช่วยให้มหาวิทยาลัยเอกชนมีรอบการดำเนินงานที่ชัดเจนในการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งการบังคับใช้ PDPA และมาตรการทางกฎหมายที่เกี่ยวข้องให้เกิดประโยชน์อย่างกว้างขวางนั้น มหาวิทยาลัยควรส่งเสริมการฝึกอบรมและพัฒนาความรู้เกี่ยวกับกฎหมาย PDPA พร้อมปลูกฝังวัฒนธรรมองค์กรที่ให้ความสำคัญกับความปลอดภัยด้านข้อมูล ควบคู่กับการกำหนดและปรับปรุงนโยบายด้านความปลอดภัยที่มีความยืดหยุ่นและสอดคล้องกับรูปแบบปัญหาความท้าทายในอนาคต

2. สรุปผลการวิจัย

ในช่วง 5 ปีที่ผ่านมา มหาวิทยาลัยต้องเผชิญกับปัญหาการละเมิดข้อมูลและการ

โจมตีทางไซเบอร์ที่สำคัญ 3 ประเด็น ได้แก่ การเผยแพร่ข้อมูลส่วนบุคคลบนเว็บไซต์, การโจมตีด้วยไวรัสเรียกค่าไถ่ต่อเซิร์ฟเวอร์ฐานข้อมูลวิจัย, และการโจมตีเว็บไซต์ที่พัฒนาด้วย WordPress ซึ่งส่งผลกระทบต่อความปลอดภัยของข้อมูล ภาพลักษณ์ และการดำเนินงานของมหาวิทยาลัย แนวทางแก้ไขที่เสนอ ได้แก่ การอัปเดตระบบและซอฟต์แวร์ การใช้เทคโนโลยีป้องกัน เช่น การเข้ารหัสและ MFA การฝึกอบรมบุคลากรให้มีความรู้ด้าน PDPA และกฎหมายที่เกี่ยวข้อง รวมถึงการเสนอการปรับปรุงเนื้อหาและรายละเอียดของกฎหมายเพื่อให้มีความชัดเจนและครอบคลุมทุกกรณีของการละเมิด พร้อมทั้งส่งเสริมมาตรการป้องกันในระดับองค์กรและบุคคล ซึ่งจะช่วยลดโอกาสการละเมิดล่วงหน้าและเสริมสร้างความมั่นคงในระบบข้อมูล และควรมีการจัดสรรทรัพยากรบุคคลโครงสร้างพื้นฐาน และการพัฒนาบุคลากรเพื่อสร้างระบบความปลอดภัยที่ยั่งยืนและครบวงจร

3. ข้อเสนอแนะ

3.1 ข้อเสนอแนะในการนำผลการวิจัยไปใช้ประโยชน์

3.1.1 มหาวิทยาลัยควรให้ความสำคัญกับการพัฒนาระบบความปลอดภัยทางไซเบอร์โดยการปรับปรุงระบบเว็บไซต์อย่างต่อเนื่องเพื่อป้องกันช่องโหว่ที่อาจทำให้ข้อมูลส่วนบุคคลถูกเปิดเผย การติดตั้งเทคโนโลยีป้องกันภัยคุกคามที่ทันสมัย เช่น ระบบการเข้ารหัสข้อมูลและระบบสำรองข้อมูล จะช่วยเสริมความปลอดภัยให้กับข้อมูล รวมทั้งควรมีการชี้แจงหรือนำเสนอบทลงโทษสำหรับการละเมิดความปลอดภัยบนหน้าเว็บไซต์เพื่อสร้างความตระหนักรู้และความรับผิดชอบต่อการรักษาความปลอดภัยทางไซเบอร์แก่สาธารณชน

3.1.2 มหาวิทยาลัยควรเสริมสร้างความรู้และความเข้าใจเกี่ยวกับ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

(PDPA) ให้แก่บุคลากร เพื่อให้การจัดการข้อมูลส่วนบุคคลเป็นไปตามกฎหมายและมาตรฐานที่กำหนด โดยการใช้มาตรการต่าง ๆ เช่น การเข้ารหัสข้อมูล จะช่วยปกป้องข้อมูลทั้งในระหว่างการส่งและการเก็บรักษา นอกจากนี้ การฝึกอบรมบุคลากรเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและการปฏิบัติตาม PDPA จะช่วยสร้างวัฒนธรรมองค์กรที่ให้ความสำคัญกับความปลอดภัยทางข้อมูล และทำให้บุคลากรเข้าใจถึงบทบาทของตนในการปกป้องข้อมูลส่วนบุคคล

3.2 ข้อเสนอแนะในการวิจัยครั้งต่อไป

3.2.1 ควรศึกษาถึงประสิทธิภาพของเทคโนโลยีการเข้ารหัสข้อมูลในการปกป้องความปลอดภัยของข้อมูลภายในสถาบันการศึกษา โดยการวิจัยจะสามารถประเมินว่าเทคโนโลยีเหล่านี้

นี้ช่วยลดความเสี่ยงจากการโจมตีทางไซเบอร์และปกป้องข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพหรือไม่

3.2.2 ควรศึกษาความคิดเห็นและความพึงพอใจของบุคลากรและนักศึกษาต่อระบบความปลอดภัยและมาตรการคุ้มครองข้อมูลส่วนบุคคลที่นำไปใช้ในสถาบันการศึกษา ซึ่งจะช่วยให้อาจสามารถปรับปรุงมาตรการเหล่านี้ได้ดียิ่งขึ้น

3.2.3 ควรประเมินผลกระทบของโปรแกรมฝึกอบรมเกี่ยวกับการปฏิบัติตาม PDPA และการคุ้มครองข้อมูลส่วนบุคคลที่จัดให้แก่บุคลากร โดยการวิจัยจะช่วยให้เข้าใจว่าการฝึกอบรมดังกล่าวมีผลต่อความเข้าใจและการปฏิบัติตามมาตรการการปกป้องข้อมูลอย่างไร

เอกสารอ้างอิง

- กฤษณ์ เหล่ากอ, & สมบูรณ์สุข สำราญ. (2567). การตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในจังหวัดปทุมธานี. วารสาร มจร อุบล ปรีทรรศน์, 9(2), 2315–2330.
- กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2565). ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565. www.mdes.go.th/law/detail/6336-ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล-เรื่อง-หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล-พ-ศ-2565.
- เกียรติเฉลิม รักงาม, & สังเวียน เทพผา. (2567). มาตรการทางกฎหมายในการคุ้มครองป้องกันการนำเข้าสู่ข้อมูลส่วนบุคคลตามคอมพิวเตอร์ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์. วารสารสังคมศาสตร์และวัฒนธรรม, 8(3), 14–24.
- ชรินทร์ทิพย์ ปันสุวรรณ, & สุนทีย์ จิตสว่าง. (2565). แนวทางการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ขององค์กรในยุคดิจิทัล. วิทยานิพนธ์จุฬาลงกรณ์มหาวิทยาลัย, 6715. <https://digital.car.chula.ac.th/chulaetd/6715>.
- สำนักงานราชบัณฑิตยสภา. (2562). พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒. ราชกิจจานุเบกษา, 136(50 ง), 1–37.
- อภิชน จันทรเสน. (2562). แนวคิดในการกำหนดมาตรการทางกฎหมายเพื่อการบังคับใช้ที่มีประสิทธิภาพ. สำนักงานคณะกรรมการกฤษฎีกา. <https://lawreform.go.th/uploads/files/1589344915-ig3n5-7x6v2.pdf>.

- Amo-Filva, D., Mauri, S. A., Escudero, D. F., Sanchez-Sepulveda, M. V., Hasti, H., García-Holgado, A., ... & Paes, C. (2024). Empowering student data privacy in schools through open educational resources. In *Innovation and technologies for the digital transformation of education: European and Latin American perspectives* (pp. 253–263). Springer Nature Singapore.
- Melchior, C., & Soler, U. (2024). Security of personal data in cyberspace in the opinion of students of the University of Udine. *Cybersecurity and Law*, 11(1), 227–247.
- Mehra, T. (2024). The role of encryption in securing backup data against ransomware threats. *International Journal of Science and Research Archive*, 13(2), 1971–1974.
- Miskam, S., Sholehuddin, N., Shahwahid, F. M., Aziz, T. N. R. A., & Mansor, N. (2023). Data privacy practices of private higher education institutions in Malaysia: A preliminary study. *Malaysian Journal of Information and Communication Technology (MyJICT)*, 88–99.
- Ting, T. T., Cheah, K. M., Khiew, J. X., Lee, Y. C., Chaw, J. K., & Teoh, C. K. (2024). Validation of cyber security behaviour among adolescents at Malaysia university: Revisiting gender as a role. *International Journal of Innovative Research and Scientific Studies*, 7(1), 127–137.