



การ

ศึกษากลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศ
ของแพลตฟอร์มออนไลน์ไต้หวันหลิว ยิน^{1*} ภูมิพัฒน์ แก้วตารณวัฒนา ² จำริญ คังคะศรี ³ นิสากร ยินดีจันทร์ ⁴

รับบทความ: 21 พฤศจิกายน 2568 แก้ไขบทความ: 24 พฤศจิกายน 2568 ตอรับบทความ: 25 พฤศจิกายน 2568

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษา 1) ความต้องการด้านความปลอดภัยของระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน และ 2) กลยุทธ์การจัดการความปลอดภัยของระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน โดยใช้ระเบียบวิธีวิจัยแบบผสมผสาน การวิจัยเชิงปริมาณ กลุ่มตัวอย่าง ได้แก่ ผู้ใช้งานแพลตฟอร์มออนไลน์ไต้หวัน จำนวน 400 คน สุ่มตัวอย่างตามวิธีที่กำหนดให้ครอบคลุมผู้ใช้งานที่เกี่ยวข้องเครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูล คือ แบบสอบถาม วิเคราะห์ข้อมูลโดยใช้สถิติเชิงพรรณนา ได้แก่ ร้อยละ ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐาน การวิจัยเชิงคุณภาพ ผู้ให้ข้อมูลสำคัญ ได้แก่ เจ้าหน้าที่ภาครัฐ ผู้บริหาร และบล็อกเกอร์หรือผู้พัฒนาแพลตฟอร์มออนไลน์ไต้หวันที่มีบทบาทหรือความรับผิดชอบเกี่ยวกับการกำกับดูแลและการจัดการความปลอดภัยของระบบสารสนเทศ จำนวน 20 คน คัดเลือกแบบเจาะจงเครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูล คือ แบบสัมภาษณ์กึ่งโครงสร้าง โดยมุ่งศึกษาแนวทางและกลยุทธ์การจัดการความปลอดภัยของระบบสารสนเทศ ข้อมูลเชิงคุณภาพนำมาวิเคราะห์ด้วยการวิเคราะห์เชิงเนื้อหาและตรวจสอบความน่าเชื่อถือของข้อมูลโดยใช้วิธีการตรวจสอบแบบสามเส้า ผลการวิจัยพบว่า 1) ผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันมีความต้องการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันโดยรวมอยู่ในระดับมากที่สุด 2) กลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน 5 กลยุทธ์ ดังนี้ (1) กลยุทธ์การกำหนดระบบการจัดการความปลอดภัยสารสนเทศ (2) กลยุทธ์การกำหนดเป้าหมายความปลอดภัยระบบสารสนเทศ (3) กลยุทธ์การกำหนดนโยบายการกำกับดูแลความปลอดภัย (4) กลยุทธ์การพัฒนาบุคลากรด้านความปลอดภัยสารสนเทศ และ (5) กลยุทธ์การสร้างความปลอดภัยต่อผู้ใช้แพลตฟอร์มออนไลน์

คำสำคัญ: การจัดการความปลอดภัย ระบบสารสนเทศ แพลตฟอร์มออนไลน์ไต้หวัน¹⁻⁴ คณะนิเทศศาสตร์ มหาวิทยาลัยราชภัฏรำไพพรรณี จันทบุรี ประเทศไทย

* อีเมล : liuyin.rbru@outlook.com

A Study on Information System Security Management Strategies of the Douyin Online Platform

Liu Yin^{1*} Puripat Keawtathanawatthana²

Jamroen Kangsri³ Nisakorn Yindeechan⁴

Abstract

This study aimed to: 1) investigate users' needs regarding information security management of the Douyin online platform; and 2) examine strategies for managing information security of the Douyin online platform. A mixed methods research design was employed, comprising quantitative and qualitative approaches. For the quantitative phase, the sample consisted of 400 users of the Douyin online platform. The sample size was determined using Yamane's formula, and an appropriate sampling method was employed to obtain participants representing relevant platform users. Data were collected using a questionnaire and analyzed using descriptive statistics, including percentage, mean, and standard deviation. For the qualitative phase, 20 key informants, comprising government officials, executives, and bloggers or platform developers who were responsible for or involved in information security governance and management, were selected through purposive sampling. Data were collected using semi-structured interviews focusing on approaches and strategies for information security management. The qualitative data were analyzed using content analysis, and the credibility of the findings was established through triangulation.

The findings revealed that: 1) users of the Douyin online platform had an overall need for information security management at the highest level; and 2) five strategies for information security management of the Douyin online platform were identified: (1) establishing an information security management system; (2) defining information security objectives; (3) establishing security governance policies; (4) developing personnel competencies in information security; and (5) building user confidence in the online platform.

Keywords: Information Security Management; Online Platform Douyin

¹⁻⁴ Faculty of Communication Arts, Rambhai Barni Rajabhat university
E-mail: liuyin.rbru@outlook.com

บทนำ

การพัฒนาอย่างรวดเร็วของเทคโนโลยีอินเทอร์เน็ตและสื่อดิจิทัลได้เปลี่ยนแปลงรูปแบบการสื่อสาร การเผยแพร่ข้อมูล และการสร้างปฏิสัมพันธ์ทางสังคมอย่างมีนัยสำคัญ โดยเฉพาะแพลตฟอร์มวิดีโอสั้นซึ่งสามารถนำเสนอเนื้อหาแก่ผู้ใช้ได้อย่างรวดเร็วและต่อเนื่องผ่านระบบแนะนำเนื้อหาที่อาศัยอัลกอริทึม ข้อมูล พฤติกรรม และการมีส่วนร่วมของผู้ใช้ เช่น การกดถูกใจ การแสดงความคิดเห็น การแชร์ และระยะเวลาในการรับชม กลไกดังกล่าวทำให้แพลตฟอร์มสามารถคัดเลือกและนำเสนอเนื้อหาที่สอดคล้องกับความสนใจของผู้ใช้แต่ละราย และมีส่วนสำคัญต่อประสบการณ์การใช้งานและการมีส่วนร่วมบนแพลตฟอร์ม (Wu & Zhang, 2024) โดยเฉพาะแพลตฟอร์มโต่วยีน (Douyin) ซึ่งเป็นแพลตฟอร์มวิดีโอสั้นที่มีระบบแนะนำเนื้อหาเป็นกลไกสำคัญในการจัดลำดับและเผยแพร่เนื้อหาแก่ผู้ใช้ การขยายตัวของแพลตฟอร์มดิจิทัลดังกล่าวมิได้ก่อให้เกิดเพียงโอกาสด้านการสื่อสารและการสร้างสรรค์เนื้อหาเท่านั้น แต่ยังนำมาซึ่งความท้าทายด้านการจัดการข้อมูล และความมั่นคงปลอดภัยของระบบสารสนเทศ เนื่องจากการดำเนินงานของแพลตฟอร์มจำเป็นต้องรวบรวม ประมวลผล จัดเก็บ และใช้ข้อมูลผู้ใช้ในหลายรูปแบบ หากข้อมูลและระบบไม่ได้รับการป้องกันอย่างเหมาะสมย่อมมีความเสี่ยงต่อการเข้าถึง การใช้ การเปิดเผย การเปลี่ยนแปลง การรบกวน หรือการทำลายโดยไม่ได้รับอนุญาต ซึ่งอาจส่งผลกระทบต่อสิทธิและความเป็นส่วนตัวของผู้ใช้ ตลอดจนความน่าเชื่อถือและความต่อเนื่องในการให้บริการของแพลตฟอร์ม ดังนั้น ความมั่นคงปลอดภัยสารสนเทศจึงต้องครอบคลุมทั้งการป้องกันข้อมูล ระบบ และทรัพยากรสารสนเทศจากภัยคุกคาม ตลอดจนการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของสารสนเทศ (National Institute of Standards and Technology [NIST], 2020) ในบริบทของแพลตฟอร์มโต่วยีน ประเด็นดังกล่าวมีความซับซ้อนมากขึ้น เนื่องจากระบบแนะนำเนื้อหาด้วยอัลกอริทึมมีความสัมพันธ์โดยตรงกับข้อมูลพฤติกรรมของผู้ใช้ ขณะที่การสร้างและเผยแพร่เนื้อหาเกิดขึ้นอย่างต่อเนื่องและมีปริมาณสูง ความเชื่อมโยงระหว่างข้อมูลส่วนบุคคล อัลกอริทึม เนื้อหา และการมีส่วนร่วมของผู้ใช้จึงทำให้การรักษาความปลอดภัยไม่สามารถพิจารณาเฉพาะมาตรการทางเทคนิคได้ แต่จำเป็นต้องครอบคลุมการบริหารความเสี่ยง นโยบาย กระบวนการ บุคลากร และการกำกับดูแลอย่างเป็นระบบ การศึกษาความปลอดภัยระบบสารสนเทศของแพลตฟอร์มโต่วยีนจึงมีความสำคัญต่อการทำความเข้าใจความต้องการด้านความปลอดภัยของผู้ใช้และการกำหนดแนวทางการจัดการที่สามารถรองรับความเสี่ยงในสภาพแวดล้อมดิจิทัลที่เปลี่ยนแปลงอย่างต่อเนื่อง

แม้แพลตฟอร์มออนไลน์จะมีระบบเทคโนโลยีและอัลกอริทึมสำหรับบริหารจัดการข้อมูลและกลั่นกรองเนื้อหา แต่ลักษณะการเผยแพร่ข้อมูลที่มีความรวดเร็วและมีปริมาณสูงยังสร้างความท้าทายด้านความปลอดภัยหลายประการ ได้แก่ การรั่วไหลของข้อมูลส่วนบุคคล การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การแพร่กระจายของข้อมูลที่ไม่ถูกต้องหรือทำให้เข้าใจผิด และความเสี่ยงจากการโจมตีทางไซเบอร์ ทั้งนี้ แพลตฟอร์มดิจิทัลยังเผชิญความท้าทายด้านการกลั่นกรองและการคัดสรรเนื้อหา เนื่องจากระบบอัลกอริทึมสามารถขยายการเข้าถึงข้อมูลบางประเภทได้อย่างรวดเร็ว ซึ่งทำให้การจัดการข้อมูลที่ไม่ถูกต้องหรือเป็นอันตรายมีความซับซ้อน

มากขึ้น (United Nations Educational, Scientific and Cultural Organization [UNESCO], 2023) นอกจากนี้ การจัดการความมั่นคงปลอดภัยของแพลตฟอร์มไม่ควรจำกัดอยู่เฉพาะมาตรการทางเทคนิค แต่ควรครอบคลุมการกำกับดูแล การบริหารความเสี่ยง การกำหนดนโยบาย การควบคุม การตรวจจับ การตอบสนอง และการฟื้นฟูระบบอย่างเป็นระบบ รวมถึงการกำหนดบทบาทและความรับผิดชอบของผู้เกี่ยวข้อง (Pascoe et al., 2024)

สำหรับประเทศจีน การเติบโตของเศรษฐกิจดิจิทัลและแพลตฟอร์มออนไลน์ทำให้ภาครัฐให้ความสำคัญกับการกำกับดูแลบริการข้อมูลบนอินเทอร์เน็ต ความมั่นคงปลอดภัยทางไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคลอย่างต่อเนื่อง โดยกฎหมายความมั่นคงทางไซเบอร์ของจีนกำหนดกรอบความรับผิดชอบของผู้ดำเนินการเครือข่ายในการคุ้มครองข้อมูลผู้ใช้และการรักษาความปลอดภัยของระบบสารสนเทศ (Cyberspace Administration of China [CAC], 2025) ขณะเดียวกัน ข้อกำหนดว่าด้วยการจัดการบริการแนะนำอัลกอริทึมสำหรับบริการข้อมูลทางอินเทอร์เน็ตกำหนดให้ผู้ให้บริการต้องรับผิดชอบต่อความปลอดภัยของอัลกอริทึม จัดให้มีระบบการตรวจสอบเนื้อหา การคุ้มครองข้อมูลและข้อมูลส่วนบุคคล การประเมินความปลอดภัย การติดตาม และการจัดการเหตุการณ์ด้านความปลอดภัย รวมถึงต้องเพิ่มความโปร่งใสและความสามารถในการอธิบายหลักการทำงานของระบบแนะนำ (Cyberspace Administration of China et al., 2022) ดังนั้น ความซับซ้อนของระบบนิเวศดิจิทัล การพึ่งพาอัลกอริทึม และปริมาณข้อมูลที่เพิ่มขึ้น จึงทำให้การจัดการความปลอดภัยจำเป็นต้องพัฒนาไปสู่การบริหารจัดการเชิงระบบและเชิงกลยุทธ์ โดยเฉพาะการเชื่อมโยงความต้องการด้านความปลอดภัยของผู้ใช้เข้ากับระบบ นโยบาย บุคลากร การบริหารความเสี่ยง และกลไกการกำกับดูแลของแพลตฟอร์ม ซึ่งเป็นประเด็นสำคัญที่ควรได้รับการศึกษาอย่างเป็นระบบ

จากบริบทดังกล่าว การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันจำเป็นต้องบูรณาการการคุ้มครองข้อมูล การบริหารความเสี่ยง การพัฒนาบุคลากร และการกำกับดูแลอย่างเป็นระบบ ผู้วิจัยจึงสนใจศึกษาความต้องการด้านความปลอดภัยของผู้ใช้และสังเคราะห์กลยุทธ์การจัดการความปลอดภัย เพื่อยกระดับการคุ้มครองข้อมูลส่วนบุคคล ลดความเสี่ยงจากการหลอกลวงและข้อมูลที่ทำให้เข้าใจผิด ตลอดจนสร้างความโปร่งใส ความน่าเชื่อถือ และความเชื่อมั่นต่อแพลตฟอร์มอย่างยั่งยืน

วัตถุประสงค์ของการวิจัย

1. ศึกษาความต้องการด้านความปลอดภัยของระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน
2. ศึกษากลยุทธ์การจัดการความปลอดภัยของระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน

วรรณกรรมและทฤษฎีที่เกี่ยวข้อง

แนวคิดการรักษาความมั่นคงปลอดภัยสารสนเทศตามกรอบ CIA Triad

แนวคิด CIA Triad เป็นกรอบพื้นฐานสำคัญในการอธิบายและประเมินความมั่นคงปลอดภัยของสารสนเทศ โดยประกอบด้วย 3 องค์ประกอบหลัก ได้แก่ การรักษาความลับของข้อมูล (Confidentiality)

การรักษาความถูกต้องครบถ้วนของข้อมูล (Integrity) และการทำให้ข้อมูลและระบบพร้อมใช้งาน (Availability) แนวคิดดังกล่าวมองว่าความมั่นคงปลอดภัยของสารสนเทศมิได้จำกัดอยู่เพียงการป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต แต่ครอบคลุมถึงการป้องกันข้อมูลจากการถูกเปลี่ยนแปลง ทำลาย หรือทำให้ไม่สามารถใช้งานได้ตามความจำเป็น ในบริบทของแพลตฟอร์มออนไลน์ ความลับของข้อมูลมีความสำคัญต่อการคุ้มครองข้อมูลส่วนบุคคล ข้อมูลบัญชีผู้ใช้ และข้อมูลพฤติกรรมการใช้งาน ขณะที่ความถูกต้องครบถ้วนของข้อมูลมีความเกี่ยวข้องกับการป้องกันการแก้ไขข้อมูลโดยไม่ได้รับอนุญาต ตลอดจนการรักษาความน่าเชื่อถือของเนื้อหาและธุรกรรมบนแพลตฟอร์ม ส่วนความพร้อมใช้งานสะท้อนความสามารถของระบบในการให้บริการแก่ผู้ใช้ได้อย่างต่อเนื่องและมีประสิทธิภาพ (National Institute of Standards and Technology [NIST], 2020; International Organization for Standardization [ISO], 2022) สำหรับการวิจัยครั้งนี้ CIA Triad สามารถใช้เป็นกรอบในการทำความเข้าใจความต้องการด้านความปลอดภัยของผู้ใช้งานแพลตฟอร์มออนไลน์ได้โดยพิจารณาว่าผู้ใช้ให้ความสำคัญต่อการคุ้มครองข้อมูลส่วนบุคคล ความถูกต้องของข้อมูล และความต่อเนื่องในการให้บริการในระดับใด ทั้งสามองค์ประกอบจึงเป็นฐานสำคัญสำหรับการกำหนดมาตรการและกลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์

แนวคิดเกี่ยวกับระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ

ระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) เป็นกรอบการบริหารจัดการที่มุ่งให้องค์กรสามารถจัดการความเสี่ยงด้านสารสนเทศอย่างเป็นระบบและต่อเนื่อง โดยไม่ได้จำกัดอยู่เฉพาะการใช้มาตรการทางเทคนิค แต่ครอบคลุมถึงบุคลากร กระบวนการ นโยบาย การบริหารความเสี่ยง และมาตรการควบคุมที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของสารสนเทศ องค์การระหว่างประเทศว่าด้วยการมาตรฐาน (ISO) กำหนดให้ ISO/IEC 27001:2022 เป็นมาตรฐานสำหรับระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ ซึ่งครอบคลุมการจัดตั้ง การนำไปปฏิบัติ การดำเนินงาน การติดตามตรวจสอบ การทบทวน การบำรุงรักษา และการปรับปรุง ISMS อย่างต่อเนื่อง โดยใช้กระบวนการบริหารความเสี่ยงเป็นพื้นฐานสำคัญของการจัดการความปลอดภัยสารสนเทศ (International Organization for Standardization [ISO], 2022) สาระสำคัญของ ISMS จึงอยู่ที่การเชื่อมโยงความมั่นคงปลอดภัยสารสนเทศเข้ากับกระบวนการบริหารขององค์กร โดยองค์กรต้องกำหนดบริบทและเป้าหมายด้านความปลอดภัย ระบุทรัพย์สินและความเสี่ยง ประเมินภัยคุกคามและช่องโหว่ กำหนดมาตรการควบคุม รวมทั้งกำหนดบทบาทและความรับผิดชอบของผู้เกี่ยวข้องอย่างชัดเจน ขณะเดียวกัน NIST Cybersecurity Framework 2.0 เสนอกรอบการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยผ่าน 6 หน้าที่สำคัญ ได้แก่ Govern, Identify, Protect, Detect, Respond และ Recover ซึ่งช่วยให้องค์กรสามารถกำหนดนโยบาย ระบุและจัดลำดับความเสี่ยง ป้องกัน ตรวจสอบ ตอบสนอง และฟื้นฟูจากเหตุการณ์ด้านความมั่นคงปลอดภัยได้อย่างเป็นระบบ (Pascoe et al., 2024)

แนวคิดการกำกับดูแลความมั่นคงปลอดภัยสารสนเทศ

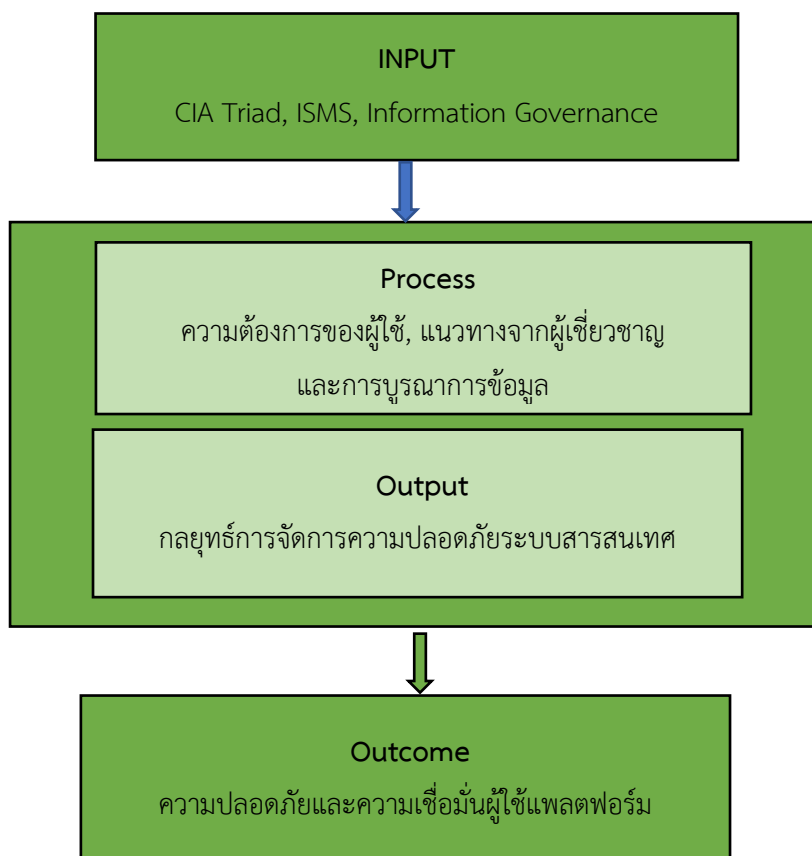
แนวคิดการกำกับดูแลความมั่นคงปลอดภัยสารสนเทศ (Information Security Governance) เป็นแนวคิดที่มุ่งให้องค์กรสามารถกำหนดทิศทาง นโยบาย บทบาท ความรับผิดชอบ และกระบวนการตัดสินใจด้านความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องกับพันธกิจ วัตถุประสงค์ และความเสี่ยงขององค์กร การกำกับดูแลจึงมิได้เป็นเพียงหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศ แต่เป็นส่วนหนึ่งของการบริหารความเสี่ยงระดับองค์กรที่ผู้บริหารและผู้มีส่วนเกี่ยวข้องต้องมีส่วนร่วม โดย NIST Cybersecurity Framework (CSF) 2.0 ได้ยกระดับการกำกับดูแลเป็นหนึ่งในหน้าที่หลักของกรอบการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ โดยเน้นการกำหนดและสื่อสารกลยุทธ์ ความคาดหวัง และนโยบายด้านความมั่นคงปลอดภัย ตลอดจนการกำหนดบริบทขององค์กร ผู้มีส่วนได้ส่วนเสีย บทบาท ความรับผิดชอบ อำนาจหน้าที่ และการกำกับติดตามผลการดำเนินงาน (Pascoe et al., 2024) การกำกับดูแลที่มีประสิทธิภาพควรประกอบด้วย การกำหนดนโยบายด้านความมั่นคงปลอดภัยที่ได้รับการรับรองจากผู้บริหาร การกำหนดบทบาทและความรับผิดชอบของผู้เกี่ยวข้องอย่างชัดเจน การกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ ตลอดจนการประเมินและติดตามความเสี่ยงอย่างต่อเนื่อง ทั้งนี้ NIST ได้ให้ความสำคัญกับการกำกับดูแลเชื่อมโยงกับการบริหารความเสี่ยงขององค์กรโดยรวม และควรมีการปรับปรุงกลยุทธ์และแนวปฏิบัติให้สอดคล้องกับการเปลี่ยนแปลงของภารกิจ ภัยคุกคาม เทคโนโลยี และข้อกำหนดทางกฎหมายหรือสัญญาที่เกี่ยวข้อง

จากแนวคิดและทฤษฎีดังกล่าวข้างต้น ผู้วิจัยได้ใช้เป็นฐานคิดโดย CIA Triad, ISMS และ Information Security Governance มีความเชื่อมโยงกันอย่างเป็นระบบ โดย CIA Triad เน้นสิ่งที่ต้องคุ้มครอง ได้แก่ ความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของสารสนเทศ ขณะที่ ISMS มุ่งจัดระบบการบริหารความปลอดภัยผ่านนโยบาย การบริหารความเสี่ยง บุคลากร และการปรับปรุงอย่างต่อเนื่อง ส่วน Information Security Governance เน้นการกำกับทิศทาง บทบาท ความรับผิดชอบ และการตัดสินใจเชิงนโยบาย ทั้งสามแนวคิดจึงสามารถใช้เป็นฐานในการวิเคราะห์ความต้องการและพัฒนากลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันได้อย่างเหมาะสม

กรอบแนวคิดการวิจัย

การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์เป็นประเด็นที่ต้องพิจารณาอย่างเป็นองค์รวม เนื่องจากเกี่ยวข้องทั้งการคุ้มครองข้อมูล การบริหารจัดการระบบ และการกำกับดูแลเชิงองค์กร โดยแนวคิด CIA Triad มุ่งรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของสารสนเทศ ซึ่งเป็นพื้นฐานสำคัญในการประเมินความต้องการด้านความปลอดภัยของผู้ใช้ ขณะที่แนวคิด Information Security Management System (ISMS) ให้ความสำคัญกับการกำหนดนโยบาย การบริหารความเสี่ยง กระบวนการควบคุม บุคลากร การติดตามประเมินผล และการปรับปรุงอย่างต่อเนื่อง ส่วนแนวคิด Information Security Governance เน้นการ

กำหนดทิศทาง นโยบาย บทบาท อำนาจหน้าที่ ความรับผิดชอบ และกลไกการกำกับติดตาม เพื่อให้การจัดการความปลอดภัยสอดคล้องกับเป้าหมายขององค์กร ดังนั้น ผู้วิจัยจึงบูรณาการแนวคิดทั้งสามเข้ากับข้อมูลความต้องการของผู้ใช้งานและข้อมูลจากผู้ให้ข้อมูลสำคัญ โดยกำหนดเป็นกรอบแนวคิดการวิจัยแบบกระบวนการ Input–Process–Output (IPO) เพื่อวิเคราะห์ สังเคราะห์ และพัฒนากลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันอย่างเป็นระบบ และพัฒนาได้ดังแผนภาพที่ 1



ภาพที่ 1 กรอบแนวคิดการวิจัย

วิธีการดำเนินการวิจัย

การวิจัยเรื่อง “การศึกษากลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน” เป็นการวิจัยประยุกต์ (Applied Research) โดยใช้ระเบียบวิธีวิจัยแบบผสมผสาน (Mixed Methods Research) ในลักษณะการดำเนินงานต่อเนื่องจากการวิจัยเชิงปริมาณไปสู่การวิจัยเชิงคุณภาพ (QUAN -QUAL) เพื่อศึกษาความต้องการด้านความปลอดภัยของผู้ใช้ และนำผลไปสังเคราะห์เป็นกลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน ดังนี้

ประชากรและผู้ให้ข้อมูลสำคัญ

สำหรับงานวิจัยเชิงปริมาณ ประชากร ได้แก่ ประชาชนชาวจีนที่ใช้แพลตฟอร์มออนไลน์ไต้หวันและอาศัยอยู่ใน 4 มณฑล ซึ่งเป็นตัวแทนของ 4 ภูมิภาค ได้แก่ มณฑลซานตง มณฑลเหอหนาน มณฑลเสฉวน และมณฑลกวางตุ้ง กลุ่มตัวอย่าง จำนวน 400 คน กำหนดขนาดโดยใช้สูตรของ Yamane ที่ระดับความเชื่อมั่นร้อยละ 95 และค่าความคลาดเคลื่อน .05

การสุ่มตัวอย่าง ใช้การสุ่มตัวอย่างแบบสะดวก (Convenience Sampling) โดยกำหนดพื้นที่เก็บข้อมูลในเขตเมืองของทั้ง 4 มณฑล และคัดเลือกผู้ที่ปฏิบัติงานแพลตฟอร์มออนไลน์ไต้หวันและสมัครใจเข้าร่วมการวิจัย

สำหรับงานวิจัยเชิงคุณภาพนั้น ผู้ให้ข้อมูลสำคัญ ได้แก่ ผู้บริหาร เจ้าหน้าที่ภาครัฐ และบล็อกเกอร์หรือผู้พัฒนาแพลตฟอร์มออนไลน์ไต้หวันที่มีบทบาทเกี่ยวข้องกับการจัดการและกำกับดูแลความปลอดภัยระบบสารสนเทศ จำนวน 20 คน คัดเลือกแบบเจาะจง (Purposive Sampling) เก็บข้อมูลโดยการสัมภาษณ์เชิงลึก (In-depth Interview) ด้วยแบบสัมภาษณ์กึ่งโครงสร้าง (Semi-structured Interview) ครอบคลุมประเด็นระบบและนโยบายความปลอดภัย การบริหารความเสี่ยง การพัฒนาบุคลากร การกำกับดูแล และแนวทางสร้างความเชื่อมั่นแก่ผู้ใช้

เครื่องมือที่ใช้ในการวิจัย เครื่องมือ ได้แก่ แบบสอบถาม ที่พัฒนาจากแนวคิด CIA Triad, Information Security Management System (ISMS), Information Security Governance และเอกสารงานวิจัยที่เกี่ยวข้อง แบ่งเป็น 3 ตอน ได้แก่ (1) ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม (2) พฤติกรรมการใช้แพลตฟอร์มออนไลน์ไต้หวัน และ (3) ความต้องการด้านความปลอดภัยระบบสารสนเทศ โดยใช้มาตราส่วนประมาณค่า 5 ระดับตามแนวคิดของ Likert

การตรวจสอบคุณภาพเครื่องมือ ตรวจสอบความตรงเชิงเนื้อหา (Content Validity) โดยผู้เชี่ยวชาญจำนวน 3 คน และประเมินความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์การวิจัยด้วยดัชนีความสอดคล้อง (Index of Item-Objective Congruence: IOC) โดยกำหนดเกณฑ์ยอมรับตั้งแต่ 0.50 ขึ้นไป ผลการตรวจสอบพบว่าแบบสอบถามมีค่า IOC โดยรวมเท่ากับ 0.95 จากนั้นปรับปรุงข้อคำถามตามข้อเสนอแนะของผู้เชี่ยวชาญก่อนนำไปเก็บรวบรวมข้อมูล

การวิเคราะห์ข้อมูล วิเคราะห์ข้อมูลเชิงปริมาณโดยใช้สถิติเชิงพรรณนา ได้แก่ ความถี่ (Frequency) ร้อยละ (Percentage) ค่าเฉลี่ย (Mean) และส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) ส่วนข้อมูลเชิงคุณภาพ ใช้วิธีการวิเคราะห์เนื้อหา (Content Analysis) โดยจัดหมวดหมู่ข้อมูล ติความ และสังเคราะห์ประเด็นร่วม จากนั้นนำผลการวิจัยเชิงปริมาณและเชิงคุณภาพมาบูรณาการร่วมกัน และใช้การวิเคราะห์ SWOT เพื่อกำหนดประเด็นเชิงกลยุทธ์ ก่อนจัดทำร่างกลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน

การตรวจสอบและยืนยันกลยุทธ์ นำร่างกลยุทธ์ที่ได้จากการสังเคราะห์เข้าสู่การสนทนากลุ่ม (Focus Group Discussion) กับผู้ทรงคุณวุฒิและผู้มีส่วนเกี่ยวข้อง เพื่อพิจารณาความเหมาะสม ความเป็นไปได้ และความสอดคล้องของกลยุทธ์ จากนั้นปรับปรุงและสังเคราะห์เป็น กลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน ฉบับสมบูรณ์

ผลการวิจัย

วัตถุประสงค์ที่ 1 ความต้องการด้านความปลอดภัยของระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน ผลการศึกษาพบว่า

1.1 ผลการวิเคราะห์ข้อมูลทั่วไปของผู้ตอบแบบสอบถามจำนวน 400 คน พบว่า ส่วนใหญ่เป็นเพศหญิง จำนวน 212 คน (ร้อยละ 53.00) มีอายุระหว่าง 20–29 ปี จำนวน 146 คน (ร้อยละ 36.50) สำเร็จการศึกษาระดับปริญญาตรี จำนวน 231 คน (ร้อยละ 57.75) และประกอบอาชีพในภาคเอกชน จำนวน 126 คน (ร้อยละ 31.50) สำหรับพฤติกรรมการใช้งาน พบว่าส่วนใหญ่ใช้แพลตฟอร์มออนไลน์ไต้หวัน ทุกวัน จำนวน 208 คน (ร้อยละ 52.00) และใช้เวลา 2–3 ชั่วโมงต่อวัน จำนวน 137 คน (ร้อยละ 34.25) โดยมีวัตถุประสงค์หลักเพื่อรับชมวิดีโอ จำนวน 163 คน (ร้อยละ 40.75)

1.2 ผลการศึกษาความต้องการด้านความปลอดภัยระบบสารสนเทศ ดังตารางที่ 1

ตารางที่ 1 การศึกษาความต้องการด้านความปลอดภัยระบบสารสนเทศ

ประเด็น	ผลการศึกษา (n=400)		
	$\bar{X}$	S.D.	ระดับ
1. การคุ้มครองข้อมูลส่วนบุคคล	4.43	0.59	มาก
2. การตรวจจับและป้องกันภัยคุกคามทางไซเบอร์	4.36	0.63	มาก
3. ความโปร่งใสในการจัดการข้อมูล	4.35	0.64	มาก
4. การควบคุมสิทธิ์และความเป็นส่วนตัว	4.31	0.67	มาก
5. การบริหารจัดการและนโยบายความปลอดภัย	4.29	0.62	มาก
6. การพัฒนาบุคลากรด้านความปลอดภัย	4.16	0.71	มาก
รวม	4.30	0.58	มาก

จากตารางที่ 1 ผลการวิเคราะห์ความต้องการด้านความปลอดภัยระบบสารสนเทศของผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน พบว่า โดยรวมอยู่ในระดับมาก ($\bar{X} = 4.30$, S.D. = 0.58) โดยเรียงลำดับค่าเฉลี่ยจากมากไปน้อยจากตารางพบว่า การคุ้มครองข้อมูลส่วนบุคคล มีค่าเฉลี่ยสูงที่สุด ($\bar{X} = 4.43$, S.D. = 0.59) สะท้อนว่าผู้ใช้ให้ความสำคัญอย่างยิ่งกับการป้องกันข้อมูลส่วนบุคคลจากการรั่วไหล การเข้าถึงโดยไม่ได้รับอนุญาต และการนำข้อมูลไปใช้โดยปราศจากความยินยอม รองลงมา ได้แก่ การตรวจจับ

และป้องกันภัยคุกคามทางไซเบอร์ ($\bar{X}$ = 4.36, S.D. = 0.63) และ ความโปร่งใสในการจัดการข้อมูล ($\bar{X}$ = 4.35, S.D. = 0.64) ตามลำดับ

วัตถุประสงค์ที่ 2 กลยุทธ์การจัดการความปลอดภัยของระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน ผลการศึกษาจากการสัมภาษณ์เชิงลึกและการสังเคราะห์ข้อมูล พบว่า กลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันประกอบด้วย 5 กลยุทธ์หลัก ดังนี้

1. กลยุทธ์การกำหนดระบบการจัดการความปลอดภัยสารสนเทศ กำหนดโครงสร้างและกลไกการบริหารความปลอดภัยอย่างชัดเจน โดยจัดตั้งคณะกรรมการหรือผู้รับผิดชอบด้านความปลอดภัย กำหนดระดับสิทธิ์การเข้าถึงข้อมูลตามบทบาทหน้าที่ จัดทำคู่มือและมาตรฐานการปฏิบัติงาน รวมถึงพัฒนาระบบเฝ้าระวังและแจ้งเตือนความผิดปกติ เพื่อป้องกันการเข้าถึงหรือใช้ข้อมูลโดยไม่ได้รับอนุญาต

2. กลยุทธ์การกำหนดเป้าหมายความปลอดภัยระบบสารสนเทศ กำหนดเป้าหมายด้านความปลอดภัยบนพื้นฐานของการประเมินและบริหารความเสี่ยงทางไซเบอร์ โดยระบุภัยคุกคาม ช่องโหว่ และระดับความเสี่ยงอย่างเป็นระบบ พร้อมกำหนดมาตรการป้องกันและลดผลกระทบ ตลอดจนติดตามประเมินผลให้สอดคล้องกับสถานการณ์ภัยคุกคามที่เปลี่ยนแปลงอย่างต่อเนื่อง

3. กลยุทธ์การกำหนดนโยบายการกำกับดูแลความปลอดภัย พัฒนานโยบายและมาตรการกำกับดูแลความปลอดภัยให้สอดคล้องกับบริบทของเทคโนโลยีดิจิทัล ปัญญาประดิษฐ์ กฎหมาย และความต้องการของผู้ใช้ โดยกำหนดบทบาท ความรับผิดชอบ และแนวทางการคุ้มครองข้อมูล แอปพลิเคชัน และผู้ใช้งานอย่างชัดเจน พร้อมมีกลไกติดตามและทบทวนนโยบายอย่างต่อเนื่อง

4. กลยุทธ์การพัฒนาบุคลากรด้านความปลอดภัยสารสนเทศ พัฒนาความรู้ ทักษะ และความตระหนักด้านความปลอดภัยของบุคลากรทุกระดับให้สอดคล้องกับมาตรฐาน นโยบาย และกฎหมายที่เกี่ยวข้อง โดยใช้ทั้งการฝึกอบรมออนไลน์และออนไซต์ รวมถึงการพัฒนาอย่างต่อเนื่อง เพื่อให้บุคลากรสามารถป้องกัน ตรวจสอบ และตอบสนองต่อภัยคุกคามด้านสารสนเทศได้อย่างมีประสิทธิภาพ

5. กลยุทธ์การสร้างเชื่อมั่นต่อผู้ใช้แพลตฟอร์มออนไลน์ มุ่งสร้างความไว้วางใจผ่านการคุ้มครองข้อมูลส่วนบุคคล ความโปร่งใสในการเก็บและใช้ข้อมูล การสื่อสารมาตรการความปลอดภัย และการตอบสนองต่อเหตุการณ์ด้านความปลอดภัยอย่างรวดเร็วและรับผิดชอบ ทั้งนี้ ความเชื่อมั่นของผู้ใช้เป็นปัจจัยสำคัญต่อการยอมรับ การใช้งานอย่างต่อเนื่อง และความยั่งยืนของแพลตฟอร์ม

จากผลการวิเคราะห์ข้อมูลเชิงคุณภาพ พบว่า กลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันไม่ได้ขึ้นอยู่กับมาตรการทางเทคโนโลยีเพียงอย่างเดียว แต่ครอบคลุมทั้งระบบการบริหาร เป้าหมายและการบริหารความเสี่ยง นโยบายและการกำกับดูแล การพัฒนาบุคลากร และการสร้างความเชื่อมั่นของผู้ใช้ ทั้งนี้ ผลการสนทนากลุ่มได้ช่วยยืนยันและขยายความหมายของกลยุทธ์ทั้ง 5 ด้านดังปรากฏในคำกล่าวของผู้ให้ข้อมูลสำคัญต่อไปนี้

“แพลตฟอร์มควรมีระบบรักษาความปลอดภัยที่ชัดเจน กำหนดสิทธิ์การเข้าถึงข้อมูลตามหน้าที่ และมีผู้รับผิดชอบโดยตรง เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต”

(ผู้บริหารแพลตฟอร์ม, ผู้ให้ข้อมูลคนที่ 3)

“การรักษาความปลอดภัยไม่ควรเน้นเฉพาะเทคโนโลยี แต่ต้องมีนโยบายที่ชัดเจน พัฒนาบุคลากรอย่างต่อเนื่อง และประเมินความเสี่ยงให้ทันต่อรูปแบบภัยคุกคามที่เปลี่ยนแปลง”

(เจ้าหน้าที่ภาครัฐ, ผู้ให้ข้อมูลคนที่ 8)

“ผู้ใช้งานเกิดความเชื่อมั่นเมื่อแพลตฟอร์มมีความโปร่งใสในการใช้ข้อมูล แจ้งให้ทราบเมื่อเกิดปัญหา และแสดงความรับผิดชอบต่อความปลอดภัยของข้อมูลส่วนบุคคลอย่างจริงจัง”

(ผู้พัฒนาแพลตฟอร์ม, ผู้ให้ข้อมูลคนที่ 15)

อภิปรายผล

วัตถุประสงค์ที่ 1 ผลการศึกษาพบว่า ผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันมีความต้องการด้านความปลอดภัยระบบสารสนเทศโดยรวมอยู่ในระดับมาก อาจเป็นเพราะแพลตฟอร์มมีการรวบรวม ประมวลผล และใช้ข้อมูลส่วนบุคคล รวมถึงข้อมูลพฤติกรรมการใช้งานของผู้ใช้ในปริมาณมาก จึงทำให้ผู้ใช้ตระหนักถึงความเสี่ยงจากการรั่วไหลของข้อมูล การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการนำข้อมูลไปใช้โดยขาดความโปร่งใส โดยเฉพาะด้านการคุ้มครองข้อมูลส่วนบุคคลที่มีค่าเฉลี่ยสูงสุด สะท้อนว่าผู้ใช้ให้ความสำคัญกับสิทธิในการควบคุมข้อมูลของตนเองและความปลอดภัยของข้อมูลที่อยู่ภายใต้การดูแลของแพลตฟอร์ม เนื่องจากการรับรู้ความเสี่ยงด้านความเป็นส่วนตัวมีความสัมพันธ์กับความไว้วางใจและพฤติกรรมการใช้แพลตฟอร์ม ดิจิทัล สอดคล้องกับ Liu et al. (2024) ที่พบว่าการใช้อินเทอร์เน็ตมีความสัมพันธ์กับการรับรู้ความเสี่ยงด้านความเป็นส่วนตัวของผู้ใช้ชาวจีน และสอดคล้องกับ Liu and Chen (2024) ที่ชี้ให้เห็นว่าการกำกับดูแลข้อมูลส่วนบุคคลของแพลตฟอร์มดิจิทัลในจีนมีความสำคัญต่อการสร้างความโปร่งใส ความรับผิดชอบ และความไว้วางใจของผู้ใช้ ดังนั้น การจัดการความปลอดภัยของแพลตฟอร์มจึงควรดำเนินการอย่างบูรณาการ ทั้งการใช้มาตรการทางเทคนิค การกำหนดนโยบายคุ้มครองข้อมูล การบริหารความเสี่ยง และการกำกับดูแลที่มีประสิทธิภาพ เพื่อให้สามารถตอบสนองต่อความต้องการของผู้ใช้และสร้างความเชื่อมั่นต่อแพลตฟอร์มได้อย่างยั่งยืน สามารถอภิปรายสรุปได้ว่า ความต้องการด้านความปลอดภัยระบบสารสนเทศของผู้ใช้สะท้อนความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล ความโปร่งใส และการป้องกันภัยคุกคามทางไซเบอร์ ดังนั้น แพลตฟอร์มจึงควรบูรณาการมาตรการทางเทคโนโลยี นโยบาย และการกำกับดูแล เพื่อสร้างความปลอดภัยและความเชื่อมั่นแก่ผู้ใช้อย่างยั่งยืน

วัตถุประสงค์ที่ 2 ผลการศึกษาพบว่า กลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันประกอบด้วย 5 กลยุทธ์ ได้แก่ การกำหนดระบบการจัดการความปลอดภัย การกำหนดเป้าหมายความปลอดภัย การกำหนดนโยบายการกำกับดูแล การพัฒนาบุคลากร และการสร้างความเชื่อมั่นต่อผู้ใช้ อาจเป็นเพราะการจัดการความปลอดภัยของแพลตฟอร์มดิจิทัลมีความซับซ้อนและเกี่ยวข้องกับทั้งเทคโนโลยี กระบวนการ บุคลากร และการบริหารจัดการระดับองค์กร จึงไม่สามารถพึ่งพามาตรการทางเทคนิคเพียงด้านเดียวได้ เนื่องจากภัยคุกคามทางไซเบอร์มีการเปลี่ยนแปลงอย่างต่อเนื่องและมีรูปแบบที่ซับซ้อนมากขึ้น องค์กรจึงจำเป็นต้องประเมินและจัดลำดับความเสี่ยง กำหนดโครงสร้าง บทบาท และความรับผิดชอบที่ชัดเจน พัฒนานโยบายและมาตรการควบคุม ตลอดจนเสริมสร้างความรู้และทักษะของบุคลากรอย่างต่อเนื่อง สอดคล้องกับ ISO/IEC 27001:2022 ซึ่งให้ความสำคัญกับการจัดตั้งระบบการจัดการความมั่นคงปลอดภัยสารสนเทศบนฐานการประเมินและจัดการความเสี่ยง การกำหนดกระบวนการควบคุม และการปรับปรุงระบบอย่างต่อเนื่อง และสอดคล้องกับ Pascoe et al. (2024) ที่เสนอกรอบ NIST Cybersecurity Framework 2.0 ซึ่งประกอบด้วย Govern, Identify, Protect, Detect, Respond และ Recover เพื่อสนับสนุนการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ ทั้งนี้ การสร้างความเชื่อมั่นของผู้ใช้เป็นองค์ประกอบสำคัญที่เชื่อมโยงผลการดำเนินงานด้านความปลอดภัยกับการยอมรับและการใช้งานแพลตฟอร์มในระยะยาว โดยเฉพาะการคุ้มครองข้อมูลส่วนบุคคล ความโปร่งใสในการเก็บและใช้ข้อมูล การสื่อสารเมื่อเกิดเหตุการณ์ด้านความปลอดภัย และความรับผิดชอบของแพลตฟอร์ม ซึ่งจะช่วยลดการรับรู้ความเสี่ยงและเสริมสร้างความไว้วางใจของผู้ใช้ ดังนั้น กลยุทธ์ทั้ง 5 ด้านจึงควรดำเนินการเชื่อมโยงกันเป็นระบบ เพื่อให้การจัดการความปลอดภัยมีประสิทธิภาพ สามารถรองรับภัยคุกคามที่เปลี่ยนแปลง และสร้างความยั่งยืนให้แก่แพลตฟอร์มออนไลน์ได้

องค์ความรู้จากการศึกษา

องค์ความรู้จากการศึกษานี้สะท้อนให้เห็นว่า การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันไม่ควรพิจารณาเฉพาะมิติทางเทคนิค แต่ต้องเป็นระบบการจัดการเชิงบูรณาการที่เชื่อมโยงการคุ้มครองข้อมูล การบริหารความเสี่ยง การกำกับดูแล บุคลากร และความเชื่อมั่นของผู้ใช้งานเข้าด้วยกัน โดยสามารถสังเคราะห์เป็น “Douyin Information Security Strategic Management Model” ประกอบด้วย 4 องค์ประกอบสำคัญ ได้แก่ 1) การคุ้มครองสารสนเทศ (Information Protection) บนฐาน CIA Triad ครอบคลุมความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูล 2) การบริหารจัดการความปลอดภัย (Security Management) ตามแนวคิด ISMS ครอบคลุมนโยบาย การบริหารความเสี่ยง มาตรการควบคุม บุคลากร และการปรับปรุงอย่างต่อเนื่อง 3) การกำกับดูแลความปลอดภัย (Security Governance) โดยกำหนดทิศทาง บทบาท ความรับผิดชอบ อำนาจหน้าที่ และระบบติดตามประเมินผล และ 4) ความเชื่อมั่นของผู้ใช้ (User Trust) ซึ่งเกิดจากการคุ้มครองข้อมูล ความโปร่งใส ความรับผิดชอบ และการตอบสนองต่อเหตุการณ์ด้านความปลอดภัยอย่างมีประสิทธิภาพ สามารถสรุปได้ดังแผนภาพที่ 2



ภาพที่ 2 แสดงองค์ความรู้จากการศึกษา

ที่มา: สังเคราะห์โดยผู้วิจัยและพัฒนาแผนภาพโดยปัญญาประดิษฐ์ GEMINI

จากแผนภาพที่ 2 สาระสำคัญขององค์ความรู้จึงอยู่ที่ “การเปลี่ยนจากการป้องกันภัยคุกคามเชิงเทคนิคไปสู่การบริหารความปลอดภัยเชิงกลยุทธ์ที่ยึดผู้ใช้เป็นศูนย์กลาง” โดยผลการศึกษาค้นคว้าความต้องการของผู้ใช้ควรถูกนำมาเชื่อมโยงกับการกำหนดนโยบาย ระบบ บุคลากร และกลไกการกำกับดูแล เพื่อพัฒนาเป็นกลยุทธ์ที่สามารถลดความเสี่ยง ยกระดับความปลอดภัย และสร้างความเชื่อมั่นต่อแพลตฟอร์มได้อย่างต่อเนื่องและยั่งยืน และข้อเสนอเพื่อนำไปสู่การประยุกต์ใช้ ดังนี้

1. การคุ้มครองสารสนเทศ ควรประยุกต์ใช้หลัก CIA Triad เพื่อรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูลและระบบ อันเป็นพื้นฐานของความมั่นคงปลอดภัยสารสนเทศ
2. การบริหารจัดการความปลอดภัย ควรนำแนวคิด ISMS มาใช้ในการกำหนดนโยบาย ประเมินและจัดการความเสี่ยง พัฒนาบุคลากร และติดตามปรับปรุงมาตรการให้สอดคล้องกับภัยคุกคามที่เปลี่ยนแปลง
3. การกำกับดูแลความปลอดภัย ควรกำหนดโครงสร้าง บทบาท ความรับผิดชอบ และอำนาจหน้าที่ของผู้เกี่ยวข้องอย่างชัดเจน พร้อมจัดให้มีระบบติดตามและประเมินผลเพื่อให้การดำเนินงานมีความโปร่งใสและตรวจสอบได้
4. การสร้างความเชื่อมั่นของผู้ใช้ ควรให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล การสื่อสารนโยบายอย่างโปร่งใส และการตอบสนองต่อเหตุการณ์ด้านความปลอดภัยอย่างรวดเร็ว เพื่อสร้างความไว้วางใจและความเชื่อมั่นต่อแพลตฟอร์มอย่างยั่งยืน

สรุปและข้อเสนอแนะ

การพัฒนาเทคโนโลยีอินเทอร์เน็ตและแพลตฟอร์มสื่อดิจิทัลได้ทำให้แพลตฟอร์มวิดีโอสั้นเข้ามามีบทบาทสำคัญต่อการสื่อสาร การเผยแพร่ข้อมูล และการสร้างปฏิสัมพันธ์ทางสังคม โดยเฉพาะแพลตฟอร์มโดวอิน (Douyin) ที่ใช้ระบบแนะนำเนื้อหาด้วยอัลกอริทึมร่วมกับข้อมูลพฤติกรรมและการมีส่วนร่วมของผู้ใช้ ส่งผลให้สามารถเผยแพร่เนื้อหาได้อย่างรวดเร็วและตอบสนองความสนใจของผู้ใช้แต่ละราย อย่างไรก็ตาม การดำเนินงานดังกล่าวต้องอาศัยการรวบรวมและประมวลผลข้อมูลจำนวนมาก จึงก่อให้เกิดความเสี่ยงด้านความปลอดภัยระบบสารสนเทศ ทั้งการรั่วไหลของข้อมูลส่วนบุคคล การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การเผยแพร่ข้อมูลที่ไม่ถูกต้อง การฉ้อโกงออนไลน์ และการละเมิดสิทธิของผู้ใช้ ความท้าทายดังกล่าวสะท้อนว่าการรักษาความปลอดภัยของแพลตฟอร์มไม่ควรจำกัดเฉพาะมาตรการทางเทคนิค แต่ต้องบูรณาการการบริหารความเสี่ยง นโยบาย บุคลากร กระบวนการ และการกำกับดูแลอย่างเป็นระบบ ดังนั้น การศึกษาครั้งนี้จึงมุ่งศึกษาความต้องการด้านความปลอดภัยของผู้ใช้และกลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์โดวอิน โดยประยุกต์ใช้แนวคิด CIA Triad ซึ่งเน้นความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของสารสนเทศ ร่วมกับแนวคิด ISMS ที่เน้นการบริหารความเสี่ยงและการปรับปรุงอย่างต่อเนื่อง และ Information Security Governance ที่ให้ความสำคัญกับนโยบาย บทบาท ความรับผิดชอบ และการกำกับติดตาม ผลการศึกษาจะนำไปสู่การสังเคราะห์กลยุทธ์การจัดการความปลอดภัยที่เหมาะสม สามารถยกระดับการคุ้มครองข้อมูล ลดความเสี่ยง และสร้างความเชื่อมั่นแก่ผู้ใช้และผู้มีส่วนได้ส่วนเสียได้อย่างเป็นระบบ

ข้อเสนอแนะจากการศึกษา

1. ด้านนโยบายและระบบ ควรกำหนดมาตรฐานความปลอดภัยสารสนเทศที่ชัดเจน ครอบคลุมการคุ้มครองข้อมูล การควบคุมการเข้าถึง และการตอบสนองต่อภัยคุกคาม พร้อมปรับปรุงระบบอย่างต่อเนื่อง
2. ด้านบุคลากรและการกำกับดูแล ควรพัฒนาความรู้และทักษะด้านความปลอดภัยของบุคลากร กำหนดบทบาทและความรับผิดชอบอย่างชัดเจน และจัดให้มีระบบกำกับติดตามและประเมินผลอย่างสม่ำเสมอ
3. ด้านผู้ใช้และความเชื่อมั่น ควรส่งเสริมให้ผู้ใช้สามารถควบคุมข้อมูลส่วนบุคคลได้อย่างเหมาะสม พร้อมสื่อสารนโยบายความปลอดภัยอย่างโปร่งใส และจัดช่องทางรับแจ้งเหตุเพื่อสร้างความเชื่อมั่นต่อแพลตฟอร์ม

ข้อเสนอแนะการศึกษาครั้งต่อไป

1. ควรศึกษาประสิทธิผลของกลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศที่พัฒนาขึ้น โดยทดลองใช้ในบริบทจริงและประเมินผลก่อนและหลังการดำเนินงาน เพื่อยืนยันความเหมาะสมและประสิทธิผลของกลยุทธ์

2. ควรศึกษาเปรียบเทียบการจัดการความปลอดภัยของแพลตฟอร์มวิดีโอสั้นหลายแพลตฟอร์ม รวมถึงความคิดเห็นของผู้ใช้และผู้มีส่วนได้ส่วนเสีย เพื่อพัฒนาแนวทางการกำกับดูแลที่ครอบคลุมและสอดคล้องกับบริบทดิจิทัลที่เปลี่ยนแปลง

บรรณานุกรม

- Cyberspace Administration of China, Ministry of Industry and Information Technology, Ministry of Public Security, & State Administration for Market Regulation. (2022). *Provisions on the administration of algorithmic recommendation services in internet information services*. Official text of the provisions
- Cyberspace Administration of China. (2025). *Cybersecurity Law of the People's Republic of China*. Cyberspace Administration of China
- International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. ISO.
- Liu, L., & Chen, Y. (2024). A triple-layered comparative approach to understanding new privacy policy practices of digital platforms and users in China after implementation of the PIPL. *Social Media + Society*, 10(4).
<https://doi.org/10.1177/20563051241301265>
- Liu, X. Z., Ling, S., & Liu, Y. (2024). How internet use affects personal privacy risk perception: Empirical evidence from China. *Online Information Review*, 48(4), 676–693.
<https://doi.org/10.1108/OIR-02-2023-0078>
- National Institute of Standards and Technology. (2020). *Data integrity: Detecting and responding to ransomware and other destructive events (NIST Special Publication 1800-26)*. National Cybersecurity Center of Excellence.
- National Institute of Standards and Technology. (2020). Data integrity: Detecting and responding to ransomware and other destructive events. in NIST Special Publication 1800-26). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.SP.1800-26>
- Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Paper 29)*. National Institute of Standards and Technology.
<https://doi.org/10.6028/NIST.CSWP.29>

- Quinn, S., Eliot, D., Prebil, M., Witte, G., & Smith, M. (2026). *NIST Cybersecurity Framework 2.0: Cybersecurity, Enterprise Risk Management, and Workforce Management Quick-Start Guide (NIST Special Publication 1308)*. National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.1308>
- United Nations Educational, Scientific and Cultural Organization. (2023). Guidelines for the governance of digital platforms: Safeguarding freedom of expression and access to information through a multistakeholder approach. UNESCO. <https://doi.org/10.54676/UZID6630>
- Wu, B., & Zhang, Z. (2024). An inquiry into user perceptions of algorithmic recommendations in short video platforms: A case study of TikTok. *Journal of Hangzhou Dianzi University*, 20(2), 27–35. <https://doi.org/10.13954/j.cnki.hduss.2024.02.003>