การพัฒนารูปแบบการจัดการความมั่นคงปลอดภัยระบบสารสนเทศของแพลตฟอร์มสื่อดิจิทัล*

THE DEVELOPMENT OF AN INFORMATION SYSTEM SECURITY MANAGEMENT MODEL FOR DIGITAL MEDIA PLATFORMS

ภูริพัฒน์ แก้วตาธนวัฒนา[1], ดนัย โชติแสง[2], หลู หยิน[3], ศิริญญา ศิริญานันท์[4] และ กัญญามน กาญจนาทวีกูล[5]

Puripat Keawtathanawatthana[1], Danai Chotseang[2], Liu Yin[3], Sirinya Siranan[4] and Kanyamon Kanchanathaveekul[5]

[1-3]คณะนิเทศศาสตร์ มหาวิทยาลัยราชภัฏรำไพพรรณี

[1-3]Faculty of Communication Arts, Rambhai Barni Rajabhat university, Thailand

[4-5]นักวิชาการอิสระ

[4-5]Independent Scholar, Thailand

Corresponding Author's Email: puripat.k@rbru.ac.th

วันที่รับบทความ : 17 พฤศจิกายน 2568; วันแก้ไขบทความ 14 ธันวาคม 2568; วันตอบรับบทความ : 16 ธันวาคม 2568

Received 17 November 2025; Revised 14 December 2025; Accepted 16 December 2025

บทคัดย่อ

การวิจัยในครั้งนี้มีวัตถุประสงค์เพื่อ 1) ศึกษากลยุทธ์การจัดการความมั่นคงปลอดภัยระบบสารสนเทศของแพลตฟอร์มสื่อดิจิทัล และ 2) เพื่อพัฒนารูปแบบการจัดการความมั่นคงปลอดภัยระบบสารสนเทศของแพลตฟอร์มสื่อดิจิทัล โดยใช้ระเบียบวิธีวิจัยแบบผสมผสานระหว่างการวิจัยเชิงปริมาณและการวิจัยเชิงคุณภาพ การวิจัยเชิงปริมาณเก็บรวบรวมข้อมูลจากกลุ่มผู้ใช้แพลตฟอร์มออนไลน์ใน 4 ภูมิภาคของประเทศจีน ได้แก่ ภาคตะวันออก (มณฑลซาน

Citation:

*ภูริพัฒน์ แก้วตาธนวัฒนา, ดนัย โชติแสง, หลู หยิน, ศิริญญา ศิริญานันท์ และ กัญญามน กาญจนาทวีกูล. (2568). การพัฒนารูปแบบการจัดการความมั่นคงปลอดภัยระบบสารสนเทศของแพลตฟอร์มสื่อดิจิทัล. วารสารสหศาสตร์การพัฒนาสังคม, 3(6), 1157-1174.

Puripat Keawtathanawatthana, Danai Chotseang, Liu Yin, Sirinya Siranan and Kanyamon Kanchanathaveekul. The Development Of An Information System Security Management Model For Digital Media Platforms. Journal of Interdisciplinary Social Development, 3(6), 1157-1174.;

DOI: https://doi.org/10.

Website: https://so12.tci-thaijo.org/index.php/JISDIADP/

ตง) ภาคเหนือ (มณฑลเหลียวหนิง) ภาคตะวันตก (มณฑลเสฉวน) และภาคใต้ (มณฑลกว่างตง) จำนวน 400 คน วิเคราะห์ข้อมูลโดยใช้สถิติเชิงพรรณนา ได้แก่ การแจกแจงความถี่ ค่าร้อยละ ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐาน เพื่ออธิบายลักษณะทั่วไปของกลุ่มตัวอย่าง ระดับการรับรู้และความคิดเห็นต่อกลยุทธ์การจัดการความมั่นคงปลอดภัยของระบบสารสนเทศบนแพลตฟอร์มสื่อดิจิทัล การวิจัยเชิงคุณภาพเก็บรวบรวมข้อมูลจากการสัมภาษณ์เชิงลึกและการประชุมกลุ่มกับเจ้าหน้าที่ภาครัฐ ผู้บริหาร และผู้พัฒนาแพลตฟอร์มสื่อดิจิทัลที่มีบทบาทในการกำกับดูแลความมั่นคงปลอดภัยของระบบสารสนเทศ จำนวน 20 คน วิเคราะห์ข้อมูลเชิงคุณภาพโดยการวิเคราะห์เชิงเนื้อหา ผ่านกระบวนการถอดเทปการสัมภาษณ์ การกำหนดรหัส การจัดหมวดหมู่ข้อมูล และการสังเคราะห์ประเด็นสาระสำคัญ

ผลการวิจัย

1) ผลการวิจัย พบว่า แพลตฟอร์มสื่อดิจิทัลมีกลยุทธ์การจัดการความมั่นคงปลอดภัยของระบบสารสนเทศที่สำคัญ 5 ประการ ได้แก่ (1) กลยุทธ์การกำหนดระบบการจัดการความมั่นคงปลอดภัยของระบบสารสนเทศ (2) กลยุทธ์การกำหนดเป้าหมายด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (3) กลยุทธ์การกำหนดนโยบายและการกำกับดูแลด้านความมั่นคงปลอดภัย (4) กลยุทธ์การพัฒนาบุคลากรด้านความมั่นคงปลอดภัยของสารสนเทศ (5) กลยุทธ์การสร้างความเชื่อมั่นและความไว้วางใจของผู้ใช้แพลตฟอร์มสื่อดิจิทัล

2) ผลการพัฒนารูปแบบ พบว่า รูปแบบการจัดการความมั่นคงปลอดภัยของระบบสารสนเทศของแพลตฟอร์มสื่อดิจิทัลได้มาจากการวิเคราะห์และสังเคราะห์ข้อมูลจากการวิจัยเชิงปริมาณและเชิงคุณภาพ และนำมาพัฒนาเป็น CIA Triad Model ประกอบด้วยองค์ประกอบหลัก 3 ประการ ได้แก่ การรักษาความลับของข้อมูลสารสนเทศโดยการควบคุมการเข้าถึงข้อมูลให้เฉพาะผู้ที่ได้รับอนุญาต การรักษาความถูกต้องครบถ้วนของข้อมูลสารสนเทศเพื่อป้องกันการแก้ไขหรือบิดเบือนข้อมูลโดยมิชอบ และ การสร้างความพร้อมใช้งานของระบบสารสนเทศอย่างต่อเนื่องและปลอดภัย

คำสำคัญ: การพัฒนารูปแบบ, การจัดการความมั่นคงปลอดภัย, ระบบสารสนเทศ, แพลตฟอร์มสื่อดิจิทัล

Abstract

This study aimed to (1) examine information system security management strategies of digital media platforms, and (2) develop an information system security management model for digital media platforms. A mixed-methods research design was employed, integrating quantitative and qualitative approaches.The quantitative component involved data collection from 400 users of online platforms across four regions of China: Eastern China (Shandong Province), Northern China (Liaoning Province), Western China (Sichuan Province), and Southern China (Guangdong Province). The data were analyzed using descriptive statistics, including frequency, percentage, mean, and standard deviation, to explain respondents' demographic characteristics, levels of perception, and opinions regarding information system security management strategies on digital media platforms. The qualitative component consisted of in-depth interviews and focus group discussions with 20 key informants, including government officials, executives, and online platform developers responsible for information system security governance. Qualitative data were analyzed using content analysis through systematic procedures of interview transcription, coding, data categorization, and thematic synthesis to identify key patterns, strategies, and practical insights related to information system security management.

Findings

1) The findings revealed that digital media platforms adopt five key information system security management strategies: (1) establishing an information security management system; (2) defining information system security objectives; (3) formulating security governance and regulatory policies; (4) developing human resources in information system security; and (5) enhancing user trust and confidence in digital media platforms.

2) The model development results indicated that the information system security management model for digital media platforms was derived from the

integrated analysis and synthesis of quantitative and qualitative data. The model was subsequently developed into a CIA Triad Model, consisting of three core components: ensuring information confidentiality through authorized access control; maintaining information integrity to prevent unauthorized modification or data manipulation; and ensuring the continuous and secure availability of information systems. The proposed model provides a comprehensive framework encompassing technical, managerial, and governance dimensions and can be applied as a practical guideline for enhancing information system security management in digital media platforms.

Keywords: Model Development, Information Security Management, Information Systems, Digital Media Platforms

บทนำ

การพัฒนาอย่างรวดเร็วของเทคโนโลยีอินเทอร์เน็ตและเทคโนโลยีดิจิทัลได้ส่งผลให้แพลตฟอร์มสื่อดิจิทัลกลายเป็นช่องทางสำคัญในการเผยแพร่และแลกเปลี่ยนข้อมูลข่าวสารในสังคมยุคปัจจุบัน โดยเฉพาะในประเทศจีน ซึ่งรัฐบาลให้ความสำคัญอย่างยิ่งต่อการกำกับดูแลเศรษฐกิจดิจิทัลและการสร้างสภาพแวดล้อมเครือข่ายที่ปลอดภัย มีประสิทธิภาพและเป็นระเบียบ หน่วยงานกำกับดูแลด้านนโยบายและกฎหมายระดับชาติจึงได้กำหนดกรอบแนวทางและข้อเสนอแนะเชิงนโยบายเพื่อสนับสนุนการพัฒนาแพลตฟอร์มสื่อดิจิทัลอย่างเหมาะสมและยั่งยืน (Chen & Peng, 2022) แพลตฟอร์มสื่อดิจิทัล โดยเฉพาะแพลตฟอร์มที่เน้นเนื้อหาในรูปแบบวิดีโอสั้น มีลักษณะเด่นด้านกลไกการเผยแพร่ข้อมูลที่รวดเร็วและกว้างขวาง ผ่านระบบการแนะนำเนื้อหาด้วยอัลกอริธึม การโต้ตอบของผู้ใช้และการผลิตเนื้อหาที่หลากหลาย ระบบการแนะนำตามอัลกอริธึมสามารถวิเคราะห์ข้อมูลพฤติกรรมผู้ใช้ เช่น ประวัติการรับชม การกดไลค์ การแสดงความคิดเห็น การแชร์ และระยะเวลาในการรับชม เพื่อคัดเลือกและนำเสนอเนื้อหาที่สอดคล้องกับความสนใจของผู้ใช้แต่ละราย ซึ่งช่วยเพิ่มการมีส่วนร่วมและเร่งการแพร่กระจายของข้อมูลอย่างมีนัยสำคัญ (Yeung, 2018)

แพลตฟอร์มดิจิทัลที่เกี่ยวข้องกับการเผยแพร่ข้อมูลและการจัดการระบบสารสนเทศในประเทศจีน ได้แก่ แพลตฟอร์มวิดีโอสั้น เช่น โต่วยิน (Douyin) และ Kuaishou แพลตฟอร์มสื่อ

สังคมออนไลน์ เช่น WeChat และ Weibo รวมถึงแพลตฟอร์มแบ่งปันเนื้อหาและสตรีมมิง เช่น Bilibili ซึ่งแพลตฟอร์มเหล่านี้มีลักษณะร่วมกันคือการพึ่งพาระบบสารสนเทศขนาดใหญ่ การประมวลผลข้อมูลผู้ใช้จำนวนมาก และการใช้กลไกอัลกอริทึมในการแนะนำเนื้อหา ส่งผลให้ประเด็นด้านความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศมีความสำคัญอย่างยิ่งต่อการบริหารจัดการแพลตฟอร์มให้มีประสิทธิภาพ น่าเชื่อถือ และยั่งยืนในบริบทเศรษฐกิจดิจิทัลของประเทศจีน สำหรับการโต้ตอบของผู้ใช้แพลตฟอร์มสื่อดิจิทัล เช่น การกดไลค์ การแสดงความคิดเห็น และการแชร์ ไม่เพียงทำให้ผู้ใช้มีบทบาทเป็นผู้รับสารเท่านั้น แต่ยังกลายเป็นผู้สร้างเนื้อหาและผู้ส่งสารที่สำคัญ ส่งผลให้เนื้อหาวิดีโอสั้นสามารถได้รับความนิยมอย่างรวดเร็ว แพลตฟอร์มยังมีระบบสนับสนุนและแรงจูงใจสำหรับการผลิตเนื้อหาคุณภาพสูง ซึ่งช่วยขยายขอบเขตการเผยแพร่ข้อมูลทั้งภายในแพลตฟอร์มและข้ามแพลตฟอร์มไปยังสื่อสังคมออนไลน์อื่น ๆ ทำให้แพลตฟอร์มสื่อดิจิทัลมีบทบาทสำคัญในฐานะเครื่องมือการสื่อสารทางสังคมและการสื่อสารสาธารณะในยุคดิจิทัล (Chen & Peng, 2022; Senapati et al., 2023)

อย่างไรก็ตาม ประสิทธิภาพสูงในการเผยแพร่ข้อมูลของแพลตฟอร์มสื่อดิจิทัลได้ก่อให้เกิดปัญหาและความท้าทายที่สำคัญควบคู่กัน โดยเฉพาะด้านการจัดการความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ เนื่องจากผู้ใช้สามารถสร้างและเผยแพร่เนื้อหาจำนวนมากในแต่ละวัน แม้แพลตฟอร์มจะใช้อัลกอริธึมขั้นสูงช่วยในการกลั่นกรองเนื้อหา แต่ก็ยังไม่สามารถคัดกรองข้อมูลที่ไม่เหมาะสม ข่าวลือ หรือเนื้อหาที่ผิดกฎหมายได้อย่างสมบูรณ์ ส่งผลให้ข้อมูลที่เป็นอันตรายอาจแพร่กระจายอย่างรวดเร็วและกว้างขวาง (Senapati et al., 2023)

นอกจากนี้ แพลตฟอร์มสื่อดิจิทัลจำเป็นต้องรวบรวมข้อมูลผู้ใช้จำนวนมาก เช่น ข้อมูลตำแหน่งที่ตั้ง ข้อมูลอุปกรณ์ และพฤติกรรมการใช้งาน ซึ่งหากขาดมาตรการปกป้องข้อมูลที่เหมาะสม อาจนำไปสู่การละเมิดความเป็นส่วนตัว การรั่วไหลของข้อมูล และการโจมตีทางไซเบอร์ ปัญหาเหล่านี้ส่งผลโดยตรงต่อความเชื่อมั่นของผู้ใช้ ผู้สร้างเนื้อหา ผู้ลงโฆษณา และสาธารณชนโดยรวม อีกทั้งกลไกการแนะนำเนื้อหาด้วยอัลกอริธึมยังอาจก่อให้เกิดการรับรู้ข้อมูลด้านเดียวหรือ “ฟองกรองข้อมูล” (information filter bubble) ซึ่งเพิ่มความเสี่ยงต่อความเข้าใจผิด ความแตกแยกทางสังคม และการบิดเบือนข้อมูลในพื้นที่สื่อดิจิทัล โดยเฉพาะในแพลตฟอร์มวิดีโอสั้นอย่าง TikTok/Douyin ที่อัลกอริธึมมีบทบาทสูงในการกำหนดการมองเห็นของเนื้อหา (Chen, 2023)

ในบริบทดังกล่าว การจัดการความมั่นคงปลอดภัยของระบบสารสนเทศจึงกลายเป็นประเด็นเชิงยุทธศาสตร์ที่แพลตฟอร์มสื่อดิจิทัลจำเป็นต้องให้ความสำคัญอย่างยิ่ง ไม่เพียงเพื่อปกป้องข้อมูลและความเป็นส่วนตัวของผู้ใช้เท่านั้น แต่ยังเพื่อรักษาความน่าเชื่อถือ ความเป็นธรรม และเสถียรภาพของระบบการสื่อสารในสังคมดิจิทัล จากเหตุผลดังกล่าว จึงมีความสนใจศึกษาการพัฒนารูปแบบการจัดการความมั่นคงปลอดภัยของระบบสารสนเทศของแพลตฟอร์มสื่อดิจิทัล เพื่อเสนอแนวทางการบริหารจัดการที่เป็นระบบ ครอบคลุม และสามารถนำไปประยุกต์ใช้ได้อย่างเหมาะสมในบริบทแพลตฟอร์มสื่อดิจิทัลในยุคปัจจุบัน

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษากลยุทธ์การจัดการความมั่นคงปลอดภัยของระบบสารสนเทศของแพลตฟอร์มสื่อดิจิทัล

2. เพื่อพัฒนารูปแบบการจัดการความมั่นคงปลอดภัยของระบบสารสนเทศที่เหมาะสมสำหรับแพลตฟอร์มสื่อดิจิทัล

การทบทวนวรรณกรรม

แนวคิดการพัฒนาการของเทคโนโลยีอินเทอร์เน็ตและบริบทการกำกับดูแลสื่อดิจิทัลในจีน

การพัฒนาอย่างก้าวกระโดดของเทคโนโลยีอินเทอร์เน็ตได้ผลักดันให้สื่อดิจิทัลกลายเป็นช่องทางหลักในการเผยแพร่ข้อมูลข่าวสาร โดยเฉพาะในประเทศจีนซึ่งรัฐบาลให้ความสำคัญอย่างยิ่งต่อการกำกับดูแลเศรษฐกิจดิจิทัลและความปลอดภัยของระบบข้อมูล การพัฒนาเทคโนโลยีอินเทอร์เน็ตในจีนได้ผลักดันให้สื่อดิจิทัลกลายเป็นช่องทางหลักในการเผยแพร่ข้อมูลข่าวสาร โดยเฉพาะ แพลตฟอร์มดิจิทัลในประเทศจีน ได้แก่ แพลตฟอร์มวิดีโอสั้น เช่น โต่วยิน (Douyin) และ Kuaishou แพลตฟอร์มสื่อสังคมออนไลน์ เช่น WeChat และ Weibo รวมถึงแพลตฟอร์มแบ่งปันเนื้อหาและสตรีมมิง เช่น Bilibili ซึ่งแพลตฟอร์มเหล่านี้มีการพึ่งพาระบบสารสนเทศขนาดใหญ่ การประมวลผลข้อมูลผู้ใช้จำนวนมาก และการใช้กลไกอัลกอริทึมในการแนะนำเนื้อหา ส่งผลให้ประเด็นด้านความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศมีความสำคัญอย่างยิ่งต่อการบริหารจัดการแพลตฟอร์มให้มีประสิทธิภาพ น่าเชื่อถือ และยั่งยืนในบริบทเศรษฐกิจดิจิทัลของประเทศจีน (Li, X., 2020) สื่อดิจิทัลเหล่านี้มีบทบาท

สำคัญเป็นกรณีศึกษาที่แสดงให้เห็นถึงพลังของอัลกอริทึมในการคัดเลือกและเผยแพร่ข้อมูล ซึ่งไม่เพียงเพิ่มประสิทธิภาพการเข้าถึง แต่ยังเปลี่ยนผู้ใช้ให้เป็นผู้สร้างสื่อ พร้อมระบบรางวัลที่ส่งเสริมการผลิตเนื้อหาคุณภาพ จนกลายเป็นสื่อสังคมที่มีอิทธิพลต่อการรับรู้ข่าวสารทั้งในจีนและระดับโลก (Gao, J., 2022)

ความท้าทายด้านความปลอดภัยข้อมูล ผลกระทบทางสังคม และความเสี่ยงต่อผู้ใช้หลากหลายกลุ่ม

แม้ว่า กลไกของแพลตฟอร์มวิดีโอสั้นหรือแพลตฟอร์มสื่อดิจิทัลจะเพิ่มประสิทธิภาพการเผยแพร่ข้อมูลอย่างมาก แต่แพลตฟอร์มยังเผชิญความท้าทายสำคัญด้านความปลอดภัยและผลกระทบทางสังคม ปริมาณเนื้อหาที่สูงทำให้การกลั่นกรองเป็นภาระซับซ้อน แม้ใช้อัลกอริทึมและการตรวจสอบแบบผสมผสานก็ยังไม่สามารถป้องกันเนื้อหาผิดกฎหมาย ข่าวลือ เนื้อหาละเมิดลิขสิทธิ์ หรือเนื้อหาไม่เหมาะสมต่อผู้เยาว์ได้ทั้งหมด ข้อมูลส่วนบุคคลจำนวนมากที่ระบบเก็บรวบรวมตำแหน่งที่ตั้ง พฤติกรรมท่องเว็บ ข้อมูลอุปกรณ์เพิ่มความเสี่ยงของการรั่วไหลและการนำไปใช้โดยมิชอบ สอดคล้องกับรายงานปี 2023 ที่พบว่า ผู้ใช้โซเชียลกว่า 30% เผชิญปัญหาด้านความปลอดภัยบัญชี (Senapati et al., 2023) ผู้สร้างเนื้อหารายงานปัญหาการคัดลอกผลงานโดยไม่ได้รับอนุญาตเกิน 40% (Sengelmann, 2020) ขณะที่ผู้เยาว์มีความเสี่ยงสูงต่อเนื้อหาไม่เหมาะสม การกลั่นแกล้งออนไลน์ และการฉ้อโกงข้อมูล (Seo, 2021; Paat & Markham, 2021) นอกจากนี้ การแนะนำเนื้อหาจากอัลกอริทึมอาจสร้าง “ฟองกรองข้อมูล” (filter bubble) ซึ่งนำไปสู่ความแตกแยกทางสังคม ความเข้าใจผิด และการถูกใช้เป็นเครื่องมือโฆษณาชวนเชื่อ สิ่งเหล่านี้สะท้อนความจำเป็นของมาตรการกำกับดูแล การคุ้มครองข้อมูล และการยกระดับความรู้เท่าทันสื่อในระดับสังคม

จากมุมมองทางทฤษฎี การทำงานของแพลตฟอร์มวิดีโอสั้นหรือแพลตฟอร์มสื่อดิจิทัลสามารถอธิบายได้ภายใต้กรอบ Media Ecology Theory ของ Postman ซึ่งมองว่าเทคโนโลยีสื่อไม่ได้เป็นเพียงช่องทางสื่อสาร หากแต่เป็น “สภาพแวดล้อมทางสังคมใหม่” ที่หล่อหลอมพฤติกรรม การรับรู้ และความสัมพันธ์ระหว่างมนุษย์ (Postman, 2000) ในบริบทแพลตฟอร์มวิดีโอสั้น อัลกอริทึมได้กลายเป็นตัวกำหนด “ภูมิทัศน์ข้อมูล” ที่ผู้ใช้เผชิญจนเกิดวัฒนธรรมการรับรู้แบบใหม่ที่เน้นความเร็ว ความสั้น และอารมณ์เป็นตัวนำ ซึ่งเชื่อมโยงกับแนวคิด Algorithmic Governance ที่มองว่าการคัดเลือกและจัดลำดับข้อมูลโดยอัลกอริทึมทำหน้าที่เสมือน “โครงสร้างอำนาจใหม่” ที่ควบคุมพฤติกรรมและการตัดสินใจของผู้ใช้โดยไม่รู้ตัว

(Yeung, 2018) อัลกอริทึมของแพลตฟอร์มวิดีโอสั้นหรือแพลตฟอร์มสื่อดิจิทัลจึงเป็นรูปแบบของ “การกำกับดูแลที่มองไม่เห็น” ผ่านการคัดกรองข้อมูลที่ผู้ใช้เห็นและไม่เห็น สอดคล้องกับแนวคิด Surveillance Capitalism ของ Zuboff (2019) ซึ่งอธิบายว่าแพลตฟอร์มสื่อดิจิทัลแสวงหาประโยชน์จากข้อมูลส่วนบุคคลเพื่อทำนายและควบคุมพฤติกรรมผู้ใช้เพื่อผลกำไรทางเศรษฐกิจ กระบวนการเก็บข้อมูลมหาศาลของโต่ยิน ตำแหน่ง การรับชม พฤติกรรมโต้ตอบ และข้อมูลอุปกรณ์สะท้อนการผสานระหว่าง “การเฝ้าระวัง” และ “การสร้างมูลค่าเชิงพาณิชย์จากข้อมูล” ซึ่งส่งผลโดยตรงต่อความเป็นส่วนตัว การรับรู้ของผู้ใช้ และโครงสร้างอำนาจทางข้อมูลในสังคมดิจิทัลร่วมสมัย

วิธีดำเนินการวิจัย

การวิจัยเรื่อง “การพัฒนารูปแบบการจัดการความมั่นคงปลอดภัยระบบสารสนเทศสารสนเทศของแพลตฟอร์มสื่อดิจิทัล” เป็นการวิจัยประยุกต์ (Applied research) เป็นการวิจัยแบบผสมผสาน (mixed methods research) ระหว่างการวิจัยเชิงปริมาณ (Quantitative research) กับการวิจัยเชิงคุณภาพ (Qualitative research) มีรายละเอียดดังนี้

1. การวิจัยเชิงปริมาณ (Quantitative Research) เพื่อเก็บรวมรวบข้อมูล และวิเคราะห์ถึงลักษณะข้อมูลส่วนบุคคล พฤติกรรมการใช้แพลตฟอร์มสื่อดิจิทัล ความคาดหวังต่อการจัดการความปลอดภัยระบบสารสนเทศของผู้ใช้แพลตฟอร์ม และความต้องการการจัดการความปลอดภัยระบบสารสนเทศของผู้ใช้แพลตฟอร์มสื่อดิจิทัล

การวิจัยเชิงปริมาณในครั้งนี้กำหนดประชากรเป็นผู้ใช้แพลตฟอร์มสื่อดิจิทัลที่อาศัยอยู่ใน 4 ภูมิภาคของประเทศจีน ได้แก่ ภาคตะวันออกมณฑลซานตง ภาคเหนือมณฑลเหลียวหนิง ภาคตะวันตกมณฑลเสฉวน และภาคใต้มณฑลกว่างตง โดยใช้กลุ่มตัวอย่างจำนวน 400 คน ซึ่งคัดเลือกแบบการสุ่มอย่างมีระบบตามสัดส่วนของผู้ใช้ในแต่ละภูมิภาค (Stratified Sampling) เพื่อให้ได้ตัวแทนกลุ่มตัวอย่างที่สะท้อนลักษณะของประชากรผู้ใช้แพลตฟอร์มได้อย่างเหมาะสม ทั้งนี้ ใช้แบบสอบถามเป็นเครื่องมือหลักในการเก็บรวบรวมข้อมูล โดยใช้แบบสอบถาม (Questionnaire) การวิจัยเชิงปริมาณใช้แบบสอบถามมาตร Likert 5 ระดับ ครอบคลุมข้อมูลส่วนบุคคล พฤติกรรมการใช้แพลตฟอร์ม ความคาดหวัง และความต้องการด้านความปลอดภัยระบบสารสนเทศของผู้ใช้โดยผ่านการตรวจสอบคุณภาพเครื่องมือด้วย IOC จากผู้เชี่ยวชาญ 3 คน (≥ 0.50) การทดสอบแบบสอบถามนำร่อง (Pilot test) จำนวน 30 คน

และการวัดความเชื่อมั่นด้วย Cronbach's Alpha (≥ .80) วิเคราะห์ข้อมูลด้วยสถิติเชิงพรรณนา ได้แก่ ความถี่ ร้อยละ ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐาน เพื่ออธิบายลักษณะผู้ใช้และระดับความคาดหวัง–ความต้องการด้านความปลอดภัยระบบสารสนเทศอย่างเป็นระบบ

2. การวิจัยเชิงคุณภาพ (Qualitative Research) ใช้วิธีศึกษาวิจัยดังนี้

กำหนดประชากรเป็นบุคคลที่มีส่วนเกี่ยวข้องกับการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มสื่อดิจิทัล ได้แก่ เจ้าหน้าที่ภาครัฐ ผู้บริหาร และบล็อกเกอร์ผู้พัฒนาแพลตฟอร์ม โดยคัดเลือกผู้ให้ข้อมูลสำคัญ (Key Informants) จำนวน 20 คน ด้วยวิธีการเลือกแบบเจาะจง (Purposive Sampling) จากผู้ที่มีประสบการณ์ตรงด้านการกำกับดูแลความปลอดภัยไซเบอร์และการบริหารจัดการแพลตฟอร์ม ดำเนินการเก็บข้อมูลผ่านการสัมภาษณ์เชิงลึกและการประชุมกลุ่มจนข้อมูลมีความอิ่มตัว (Data Saturation)

2.1 การสัมภาษณ์แบบเจาะลึก (In-depth Interview) เพื่อศึกษากลยุทธ์การจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มสื่อดิจิทัล เป็นการสัมภาษณ์ในรูปแบบที่ไม่เป็นทางการ โดยมีการใช้ประเด็น/แนวคำถามกว้างๆ เพื่อกระตุ้นให้ผู้ใช้ข้อมูลสำคัญเล่าเรื่องราวอย่างมีเป้าหมาย โดยมีการสัมภาษณ์บุคคลซึ่งเป็นแหล่งข้อมูลกลุ่มเป้าหมายที่ได้กำหนดไว้เป็นผู้ให้ข้อมูลหลัก (Key Informant) ที่เป็นตัวแทนจากผู้บริหารระดับสูง ผู้บริหารระดับกลาง ผู้บริหารระดับปฏิบัติการ และบลอกเกอร์ผู้พัฒนาแพลตฟอร์มออนไลน์ เจ้าหน้าที่ภาครัฐ ที่มีส่วนเกี่ยวข้องกับการรักษาความปลอดภัยระบบสารสนเทศของแพลตฟอร์ม

2.2 การสังเคราะห์ (Synthesis) โดยวิธีการดังนี้ (1) นำผลข้อมูลจากการวิเคราะห์ข้อมูลเชิงปริมาณ เกี่ยวกับแพลตฟอร์มสื่อดิจิทัล และความต้องการต่อการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์ม (2) นำผลจากการศึกษาเชิงคุณภาพด้วยการสัมภาษณ์เชิงลึก (In-depth Interview) เกี่ยวกับประเด็นกลยุทธ์การจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มมาหาข้อสรุปโดยการวิธีการวิเคราะห์ SWOT เพื่อพัฒนาเป็นรูปแบบการจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มเบื้องต้น และ (3) การระดมสมอง/ focus group/ การประชุมกลุ่ม โดยนำข้อมูลจากการสังเคราะห์ (Synthesis) ข้อมูลจาก (1) เกี่ยวกับความคาดหวังต่อการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มและความต้องการต่อการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มและข้อมูลจาก (2) กลยุทธ์การจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มเพื่อยืนยันรูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มสื่อดิจิทัล

ผลการวิจัย

ผลการวิจัยครั้งนี้สะท้อนให้เห็นลักษณะการบริหารจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มสื่อดิจิทัลในมิติที่ครอบคลุมทั้งกลยุทธ์องค์กร กลไกเทคโนโลยี และผลลัพธ์เชิงพฤติกรรมผู้ใช้ ซึ่งสามารถอภิปรายตามวัตถุประสงค์ของการวิจัยได้ดังนี้

วัตถุประสงค์ที่ 1 ผลการสัมภาษณ์เชิงลึกพบว่า โต่ยินมีกลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศสำคัญ 5 ประการ ได้แก่ 1. กลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มสื่อดิจิทัล พบว่า แพลตฟอร์มสื่อดิจิทัล มีกลยุทธ์การจัดการความปลอดภัย 5 กลยุทธ์ ดังนี้

1) กลยุทธ์การกำหนดระบบการจัดการความปลอดภัยสารสนเทศ (InfoSec Governance)แพลตฟอร์มสื่อดิจิทัลมีการกำหนดระบบการจัดการความปลอดภัยสารสนเทศอย่างเป็นระบบผ่านคณะกรรมการความปลอดภัยสารสนเทศ (InfoSec Committee) ซึ่งมีหน้าที่ควบคุมสิทธิ์การเข้าถึงข้อมูลตามระดับชั้นความรับผิดชอบ และจัดทำคู่มือให้บุคลากรทุกระดับใช้เป็นแนวทางในการรักษาความปลอดภัยของข้อมูลส่วนบุคคล ระบบดังกล่าวเป็นการออกแบบขั้นตอนการรักษาความปลอดภัยพร้อมระบุเครื่องมือที่จำเป็นในการปกป้องข้อมูลขององค์กรและผู้ใช้ รวมถึงการกำหนดสิทธิ์การเข้าถึงที่เข้มงวด โดยผู้บริหารระดับปฏิบัติการไม่สามารถเข้าถึงระบบได้หากไม่ได้รับอนุญาตจากคณะกรรมการ InfoSec ซึ่งช่วยลดความเสี่ยงจากการเข้าถึงข้อมูลโดยมิชอบและเพิ่มความปลอดภัยในระดับองค์กร

2) กลยุทธ์การกำหนดเป้าหมายความปลอดภัยระบบสารสนเทศ (Cybersecurity Risk Assessment) แพลตฟอร์มดิจิทัล เช่น Douyin วิดีโอสั้นต่างๆ โซเชียลมีเดีย แพลตฟอร์มแชร์เนื้อหา ให้ความสำคัญกับการประเมินความเสี่ยงไซเบอร์เป็นลำดับแรกในการพัฒนาเป้าหมายความปลอดภัยขององค์กร โดยมีการวิเคราะห์ความเสี่ยงอย่างเป็นระบบเพื่อให้เข้าใจภัยคุกคามที่อาจเกิดขึ้นกับระบบสารสนเทศ และกำหนดมาตรการตอบสนองอย่างเคร่งครัดในทุกหน่วยงาน การประเมินความเสี่ยงนี้อยู่ในแผนเป้าหมายหลักขององค์กร ซึ่งทำหน้าที่ทั้งในการตรวจจับ ป้องกัน และปรับปรุงระบบตามผลการประเมินเพื่อป้องกันปัญหาความปลอดภัยหรือเพื่อลดความเสี่ยงที่จะเกิดขึ้นในอนาคตอย่างยั่งยืน

3) กลยุทธ์การกำหนดนโยบายการกำกับดูแลความปลอดภัย (Security Policy Management) นโยบายด้านความปลอดภัยของแพลตฟอร์มดิจิทัล เช่น Douyin วิดีโอสั้น, โซเชียลมีเดีย แพลตฟอร์มแชร์เนื้อหาถูกกำหนดขึ้นเพื่อสร้างสมดุลระหว่างการใช้เทคโนโลยี AI

และการตอบสนองต่อความคาดหวังของผู้ใช้ท่ามกลางเทคโนโลยีที่เปลี่ยนแปลงรวดเร็ว แพลตฟอร์มดิจิทัล เช่น Douyin มีบทบาทสำคัญทางสังคมและเศรษฐกิจ จึงต้องรับมือกับภัยคุกคามดิจิทัลที่ซับซ้อนมากขึ้น นโยบายความปลอดภัยถูกใช้เป็นเครื่องมือบริหารความเสี่ยงและคุ้มครองข้อมูลผู้ใช้ในทุกระดับ รวมถึงการกำหนดมาตรฐานการใช้งาน แอปพลิเคชัน และกลไกปกป้องข้อมูลส่วนบุคคล เพื่อลดปัญหาที่อาจกระทบต่อความปลอดภัยและความเชื่อมั่นของผู้ใช้แพลตฟอร์ม

4) กลยุทธ์การพัฒนาบุคลากรด้านความปลอดภัยสารสนเทศ (Security Workforce Development) กลุ่มแพลตฟอร์มดิจิทัลต่างๆ เช่น แพลตฟอร์มวิดีโอสั้น (Short-form Video Platforms) เช่น Douyin ได้ดำเนินการพัฒนาศักยภาพบุคลากรด้านความปลอดภัยสารสนเทศอย่างเป็นระบบตามนโยบายภาครัฐของจีน โดยส่งเสริมให้บุคลากรทุกระดับมีทักษะในการจัดการความปลอดภัยข้อมูลอย่างทันสมัย ด้วยการใช้เทคโนโลยีสารสนเทศยุคใหม่เพื่อการอบรมในรูปแบบออนไลน์และออนไซต์ ส่งผลให้การพัฒนาเกิดขึ้นได้สะดวก รวดเร็ว และครอบคลุมฟังก์ชันงานทั้งหมดของแพลตฟอร์ม ความต่อเนื่องของการพัฒนาบุคลากรทำให้แพลตฟอร์มสามารถรับมือกับภัยคุกคามใหม่ได้อย่างมีประสิทธิภาพ

5) ผลการวิจัยชี้ให้เห็นว่า กลยุทธ์การสร้างความเชื่อมั่นและความโปร่งใสต่อผู้ใช้เป็นองค์ประกอบสำคัญของการจัดการความมั่นคงปลอดภัยระบบสารสนเทศของแพลตฟอร์มสื่อดิจิทัล โดยเฉพาะการเปิดเผยแนวทางการจัดการข้อมูลและการคุ้มครองข้อมูลส่วนบุคคลอย่างชัดเจน ซึ่งช่วยเสริมสร้างความไว้วางใจระหว่างผู้ใช้กับแพลตฟอร์ม ความเชื่อมั่นดังกล่าวนำไปสู่การยอมรับ การมีส่วนร่วม และความภักดีของผู้ใช้ในระยะยาว ส่งผลให้แพลตฟอร์มสามารถเติบโตและรักษาความสามารถในการแข่งขันได้อย่างยั่งยืนในบริบทของเศรษฐกิจดิจิทัล

ผลการวิจัยตามวัตถุประสงค์ที่ 2 สะท้อนให้เห็นว่า การบูรณาการข้อมูลเชิงปริมาณซึ่งแสดงถึงความต้องการของผู้ใช้แพลตฟอร์มสื่อดิจิทัลในด้านความลับของข้อมูล ความถูกต้องครบถ้วน และความน่าเชื่อถือของระบบสารสนเทศ ร่วมกับข้อมูลเชิงคุณภาพที่สะท้อนแนวปฏิบัติและประสบการณ์ด้านความมั่นคงปลอดภัยของระบบสารสนเทศจากผู้เชี่ยวชาญ ผู้กำหนดนโยบาย และผู้ปฏิบัติงานที่เกี่ยวข้อง ได้นำไปสู่การพัฒนารูปแบบการจัดการความมั่นคงปลอดภัยของระบบสารสนเทศสำหรับแพลตฟอร์มสื่อดิจิทัล โดยอาศัยกรอบแนวคิด CIA Triad ซึ่งประกอบด้วย (1) ความลับของข้อมูล (Confidentiality) (2) ความถูกต้องครบถ้วนของข้อมูล (Integrity) และ (3) ความพร้อมใช้งานของระบบสารสนเทศ (Availability) ทั้งนี้

รูปแบบที่พัฒนาขึ้นได้รับการตรวจสอบความเหมาะสมและความเป็นไปได้จากผู้เชี่ยวชาญผ่านการประชุมกลุ่ม และได้รับการยืนยันว่ามีศักยภาพในการนำไปประยุกต์ใช้เป็นแนวทางในการบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศในบริบทของแพลตฟอร์มสื่อดิจิทัลได้อย่างมีประสิทธิภาพ น่าเชื่อถือ และสามารถปรับใช้ได้กับแพลตฟอร์มที่มีลักษณะการให้บริการและกลุ่มผู้ใช้ที่หลากหลาย

ทั้งนี้มีผลวิเคราะห์สภาพแวดล้อมเชิงกลยุทธ์ขององค์กรหรือระบบ โดยพิจารณาองค์ประกอบ 4 ด้าน ได้แก่ จุดแข็ง จุดอ่อน โอกาส และอุปสรรค เพื่อประกอบการวางแผนและพัฒนากลยุทธ์ให้มีประสิทธิภาพสูงสุดสรุปในตาราง 1 ดังนี้

ตารางที่ 1 ผลการวิเคราะห์สภาพแวดล้อมเชิงกลยุทธ์ขององค์กรและการเชื่อมโยงสู่การพัฒนาโมเดล CIA Triad สำหรับแพลตฟอร์มดิจิทัล

องค์ประกอบ SWOT	**รายละเอียดสาระสำคัญ**	**การเชื่อมโยงสู่โมเดล CIA Triad**
Strengths (จุดแข็ง)	- มีคณะกรรมการ InfoSec และระบบควบคุมสิทธิ์เข้าถึงหลายระดับ - อัลกอริทึมตรวจจับพฤติกรรมเสี่ยงได้แบบเรียลไทม์ - นโยบายด้านความปลอดภัยสอดคล้องกฎหมายจีน - การพัฒนาบุคลากรด้านความปลอดภัยอย่างต่อเนื่อง	C – Confidentiality: ใช้จุดแข็งด้าน InfoSec และ Access Control ปกป้องข้อมูลส่วนบุคคลและข้อมูลสำคัญของผู้ใช้ I – Integrity: อัลกอริทึมและการกำกับข้อมูลช่วยเพิ่มความถูกต้องของข้อมูล A – Availability: โครงสร้างองค์กรที่เป็นระบบสนับสนุนเสถียรภาพของบริการ
Weaknesses (จุดอ่อน)	- ปริมาณข้อมูลจำนวนมากเสี่ยงต่อการรั่วไหล - เนื้อหาบางส่วนยังหลุดจากการกลั่นกรอง - ผู้ใช้บางกลุ่มยังขาดความรู้เท่าทันสื่อ - ระบบความปลอดภัยมีความซับซ้อนสูงทำให้ผู้ใช้ไม่เข้าใจ	C – Confidentiality: ต้องเพิ่มการเข้ารหัสและระบบแจ้งเตือนเพื่อลดการรั่วไหล I – Integrity: ต้องเสริมระบบตรวจสอบเนื้อหาเพื่อรักษาความถูกต้อง A – Availability: ต้องพัฒนาระบบช่วยเหลือผู้ใช้และปรับปรุง UX ความปลอดภัย

Opportunities (โอกาส)	- ผู้ใช้ให้ความสำคัญการปกป้องข้อมูลมากขึ้น - การเติบโตของเศรษฐกิจดิจิทัล - การร่วมมือรัฐ - เอกชนด้านความปลอดภัย - ความก้าวหน้าของ AI และ Machine Learning	C – Confidentiality: ใช้เทคโนโลยี AI ในการเพิ่มมาตรการปกป้องข้อมูล I – Integrity: ใช้ ML ตรวจจับข้อมูลปลอมและพฤติกรรมผิดปกติ A – Availability: สนับสนุนการขยายขีดความสามารถระบบเพื่อรองรับผู้ใช้จำนวนมาก
Threats (อุปสรรค)	- ภัยคุกคามไซเบอร์ซับซ้อนขึ้น (Deepfake, Botnet, Phishing) - ความแข่งขันระหว่างแพลตฟอร์มวิดีโอสั้นสูง - ความเสี่ยงด้านกฎหมายและข้อบังคับ - ความคาดหวังผู้ใช้เพิ่มสูงขึ้น	C – Confidentiality: ต้องป้องกันภัยคุกคามที่จงใจเจาะข้อมูล I – Integrity: ต้องลดผลกระทบจากข้อมูลเท็จและ Deepfake A – Availability: ต้องเสริมความทนทานของระบบต่อการโจมตีไซเบอร์

จากการวิเคราะห์ SWOT พบว่า แพลตฟอร์มดิจิทัลของประเทศจีน เช่น โต่วยิน (Douyin) Kuaishou WeChat Weibo และ Bilibili มีจุดเด่นสำคัญคือการใช้ระบบสารสนเทศขนาดใหญ่และอัลกอริทึมอัจฉริยะในการประมวลผลข้อมูลผู้ใช้และแนะนำเนื้อหาได้อย่างมีประสิทธิภาพ ส่งผลให้การเผยแพร่ข้อมูลเป็นไปอย่างรวดเร็ว เข้าถึงผู้ใช้จำนวนมาก และสร้างการมีส่วนร่วมสูง อย่างไรก็ตาม ความเข้มข้นของการใช้ข้อมูลขนาดใหญ่และระบบอัลกอริทึมยังเป็นจุดพัฒนาที่สำคัญ โดยเฉพาะด้านการจัดการความมั่นคงปลอดภัยของข้อมูล การคุ้มครองความเป็นส่วนตัวของผู้ใช้ การกลั่นกรองเนื้อหา และการลดความเสี่ยงจากการบิดเบือนข้อมูลหรือการรับรู้ด้านเดียว ดังนั้น การพัฒนารูปแบบการจัดการความมั่นคงปลอดภัยของระบบสารสนเทศที่ครอบคลุมทั้งมิติด้านเทคนิค การบริหารจัดการ และการกำกับดูแล จึงเป็นปัจจัยสำคัญต่อความยั่งยืนและความน่าเชื่อถือของแพลตฟอร์มดิจิทัลในบริบทประเทศจีน และการใช้กลไกอัลกอริทึมในการแนะนำเนื้อหา ส่งผลให้ประเด็นด้านความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศมีความสำคัญอย่างยิ่งต่อการบริหารจัดการแพลตฟอร์มอย่างมีประสิทธิภาพและยั่งยืน มีโครงสร้างความปลอดภัยที่แข็งแรงจากระบบกำกับดูแล InfoSec การควบคุมสิทธิ์เข้าถึงหลายระดับ อัลกอริทึมตรวจจับพฤติกรรมเสี่ยง และการพัฒนาบุคลากรอย่างต่อเนื่อง ซึ่งสนับสนุนความลับ ความถูกต้อง และความพร้อมใช้งานตามโมเดล CIA Triad อย่างชัดเจน แพลตฟอร์มดิจิทัลมีจุดเด่นด้านศักยภาพการจัดการข้อมูลขนาดใหญ่ การใช้

อัลกอริทึมและ AI เพื่อเพิ่มประสิทธิภาพการเผยแพร่ข้อมูลและการรักษาความมั่นคงปลอดภัย ตามกรอบ C–I–A อย่างไรก็ตาม ยังมีจุดพัฒนาที่สำคัญ ได้แก่ ความเสี่ยงจากข้อมูลรั่วไหล เนื้อหาที่หลุดจากการกลั่นกรอง และความซับซ้อนของระบบที่ผู้ใช้เข้าใจได้จำกัด จึงจำเป็นต้อง เสริมมาตรการด้านการเข้ารหัส การตรวจสอบความถูกต้องของข้อมูล และกลไกช่วยเหลือผู้ใช้ ขณะเดียวกัน โอกาสจากการเติบโตของเศรษฐกิจดิจิทัล ความร่วมมือระหว่างรัฐและเอกชน และความก้าวหน้าของเทคโนโลยี AI/ML เอื้อต่อการยกระดับความมั่นคงปลอดภัยของระบบ สารสนเทศ แต่แพลตฟอร์มยังต้องบริหารจัดการภัยคุกคามไซเบอร์รูปแบบใหม่ การแข่งขันที่ รุนแรง และความคาดหวังของผู้ใช้ที่สูงขึ้นอย่างเชิงรุก เพื่อคงไว้ซึ่งเสถียรภาพ ความน่าเชื่อถือ และความยั่งยืนของระบบโดยรวม

อภิปรายผล

ผลจากการวิจัยวัตถุประสงค์ข้อที่ 1 พบว่า กลยุทธ์การจัดการความมั่นคงปลอดภัย ของระบบสารสนเทศของแพลตฟอร์มสื่อดิจิทัลมีลักษณะเป็นการบริหารจัดการเชิงระบบที่ ผสานกลไกด้านการกำกับดูแลองค์กร นโยบายความปลอดภัย การประเมินความเสี่ยงไซเบอร์ การพัฒนาศักยภาพบุคลากร และการสร้างความโปร่งใสต่อผู้ใช้เข้าด้วยกัน ทั้งนี้เป็นเพราะ แพลตฟอร์มสื่อดิจิทัลมิได้ทำหน้าที่เพียงเป็นช่องทางเผยแพร่ข้อมูลข่าวสาร แต่เป็นโครงสร้าง สภาพแวดล้อมข้อมูลที่มีอิทธิพลต่อการรับรู้ พฤติกรรม และความไว้วางใจของผู้ใช้ในระดับ สังคม การจัดการความมั่นคงปลอดภัยจึงจำเป็นต้องดำเนินการในระดับเชิงกลยุทธ์ขององค์กร ไม่ใช่เพียงมาตรการเชิงเทคนิคเฉพาะจุด สอดคล้องกับแนวคิด Media Ecology Theory ของ Postman (2000) ที่มองว่าสื่อและเทคโนโลยีเป็นสภาพแวดล้อมที่หล่อหลอมรูปแบบ ปฏิสัมพันธ์ของมนุษย์ รวมถึงสอดคล้องกับแนวคิด Algorithmic Governance ของ Yeung (2018) ที่อธิบายว่าอัลกอริทึมทำหน้าที่เป็นกลไกกำกับดูแลที่มองไม่เห็นซึ่งมีบทบาทต่อการ คัดเลือกและจัดลำดับข้อมูล อย่างไรก็ดี เมื่อเปรียบเทียบกับแนวคิด Surveillance Capitalism ของ Zuboff (2019) พบว่าผลการวิจัยสะท้อนทั้งความสอดคล้องและความแตกต่าง กล่าวคือ แม้แพลตฟอร์มจะมีกลไกกำกับดูแลด้านความปลอดภัยที่ชัดเจน แต่การพึ่งพาการเก็บข้อมูล ขนาดใหญ่ยังคงเป็นประเด็นท้าทายด้านความเป็นส่วนตัวและสมดุลอำนาจข้อมูล ซึ่งต้องอาศัย การบริหารจัดการเชิงนโยบายและจริยธรรมควบคู่กัน

ผลจากการวิจัยวัตถุประสงค์ข้อที่ 2 พบว่า การพัฒนารูปแบบการจัดการความมั่นคงปลอดภัยของระบบสารสนเทศที่เหมาะสมสำหรับแพลตฟอร์มสื่อดิจิทัลควรอยู่บนฐานของการบูรณาการข้อมูลเชิงประจักษ์จากผู้ใช้แพลตฟอร์มร่วมกับแนวปฏิบัติและประสบการณ์ของผู้เชี่ยวชาญด้านความปลอดภัยและการกำกับดูแลระบบสารสนเทศ ทั้งนี้เป็นเพราะแพลตฟอร์มสื่อดิจิทัลต้องเผชิญความเสี่ยงหลากหลายมิติพร้อมกัน ทั้งด้านข้อมูลส่วนบุคคล ความถูกต้องของเนื้อหา ความเสถียรของระบบ และความคาดหวังของผู้ใช้ การพัฒนารูปแบบจึงไม่สามารถอาศัยมุมมองด้านเทคนิคหรือด้านผู้ใช้เพียงฝ่ายเดียว แต่ต้องผสานทั้งสองมิติอย่างเป็นระบบ สอดคล้องกับกรอบแนวคิด CIA Triad ซึ่งประกอบด้วยความลับของข้อมูล (Confidentiality) ความถูกต้องครบถ้วนของข้อมูล (Integrity) และความพร้อมใช้งานของระบบ (Availability) ที่เป็นหลักการสากลในการจัดการความมั่นคงปลอดภัยระบบสารสนเทศ นอกจากนี้ ผลการอภิปรายยังสอดคล้องกับงานวิจัยที่ชี้ว่าการยกระดับความปลอดภัยของแพลตฟอร์มดิจิทัลต้องเชื่อมโยงกับความเชื่อมั่นของผู้ใช้และการบริหารความเสี่ยงเชิงรุก มากกว่าการป้องกันเชิงรับเพียงอย่างเดียว (Senapati et al., 2023; Seo, 2021; Paat & Markham, 2021) ขณะเดียวกันความแตกต่างจากงานวิจัยบางส่วนในอดีตคือ การศึกษานี้ให้ความสำคัญกับบทบาทของความโปร่งใสและการสื่อสารนโยบายความปลอดภัยในฐานะองค์ประกอบเชิงกลยุทธ์ของรูปแบบการจัดการความมั่นคงปลอดภัย ซึ่งช่วยเชื่อมโยงมาตรการด้านเทคนิคเข้ากับการยอมรับและความไว้วางใจของผู้ใช้ในระยะยาว

สรุป/ข้อเสนอแนะ

การวิจัยครั้งนี้สรุปได้ว่า การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มสื่อดิจิทัลมีความสำคัญอย่างยิ่งต่อความเชื่อมั่นของผู้ใช้และเสถียรภาพของระบบ โดยผลการวิจัยชี้ว่า โต่ยินมีกลยุทธ์ความปลอดภัยสำคัญ 5 ด้าน ได้แก่ การกำกับดูแลผ่านคณะกรรมการ InfoSec การประเมินความเสี่ยงไซเบอร์อย่างเป็นระบบ การกำหนดนโยบายความปลอดภัยที่สมดุลกับเทคโนโลยี AI การพัฒนาศักยภาพบุคลากรด้านความปลอดภัย และการสร้างความเชื่อมั่นผู้ใช้ผ่านความโปร่งใส ซึ่งล้วนมีผลต่อประสิทธิภาพและความปลอดภัยของระบบสารสนเทศอย่างมีนัยสำคัญ นอกจากนี้ การบูรณาการข้อมูลเชิงปริมาณและเชิงคุณภาพได้นำไปสู่การพัฒนาโมเดล “CIA Triad” ที่ประกอบด้วย ความลับของข้อมูล (Confidentiality) ความสมบูรณ์ของข้อมูล (Integrity) และความพร้อมใช้งานของระบบ

(Availability) ซึ่งเป็นปัจจัยสำคัญต่อการพัฒนารูปแบบการรักษาความปลอดภัยที่เหมาะสมสำหรับแพลตฟอร์มสื่อดิจิทัลในยุคปัจจุบัน **ข้อเสนอของผลวิจัย ประกอบด้วย 1. ข้อเสนอแนะในการนำผลวิจัยไปใช้ประโยชน์** ได้แก่ 1.1 ข้อเสนอเชิงนโยบาย เสนอให้กำหนดกรอบการกำกับดูแลความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ให้มีมาตรฐานกลาง โดยเน้นบทบาทของคณะกรรมการ InfoSec ในการควบคุมสิทธิ์การเข้าถึงข้อมูลและการตรวจสอบความปลอดภัย ภาครัฐควรพัฒนาแนวทางการตรวจสอบอัลกอริทึม (Algorithmic Auditing) เพื่อเพิ่มความโปร่งใสในการคัดเลือกเนื้อหาและลดความเสี่ยงจากข่าวปลอมและการบิดเบือนข้อมูล พัฒนานโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับมาตรฐานสากล เช่น GDPR และเพิ่มกลไกการลงโทษเมื่อเกิดการละเมิดข้อมูล 1.2 ข้อเสนอเชิงปฏิบัติ ได้แก่ แพลตฟอร์มควรนำโมเดล CIA Triad ไปประยุกต์ใช้ในการออกแบบระบบความปลอดภัย โดยเน้นการควบคุมสิทธิ์ การเข้ารหัสข้อมูล และการจัดทำระบบสำรองข้อมูลที่พร้อมใช้งาน ควรมีการพัฒนาหลักสูตรอบรมด้าน Cybersecurity สำหรับบุคลากรทุกระดับ โดยเฉพาะผู้ปฏิบัติงานด้าน Data & AI เพื่อยกระดับความรู้และการเฝ้าระวังภัยคุกคาม สร้างช่องทางสื่อสารกับผู้ใช้เกี่ยวกับนโยบายความปลอดภัย เช่น ศูนย์ข้อมูลความปลอดภัย (Security Information Center) ภายในแอปพลิเคชัน 1.3 ข้อเสนอเชิงวิชาการ ได้แก่ เสนอให้นำโมเดล CIA Triad ที่พัฒนาขึ้นไปใช้เป็นแนวทางในการศึกษารูปแบบความปลอดภัยของแพลตฟอร์มอื่น เช่น TikTok, WeChat, Kuaishou ทั้งนี้ สามารถประยุกต์โมเดลนี้ในงานวิจัยด้านสื่อดิจิทัล การกำกับดูแลแพลตฟอร์ม และความปลอดภัยไซเบอร์ขององค์กรภาครัฐและเอกชน แนะนำให้นักวิจัยใช้ผลการวิจัยชุดนี้เป็นฐานในการพัฒนากรอบการตรวจสอบ (Assessment Framework) ด้านความปลอดภัยเพื่อวิเคราะห์แพลตฟอร์มใหม่ ๆ สำหรับ **2. ข้อเสนอแนะเพื่อการวิจัยครั้งต่อไป** ประกอบด้วย 2.1 การศึกษาครั้งต่อไปควรมุ่งศึกษาผลกระทบของอัลกอริทึมต่อความปลอดภัยข้อมูล เช่น การแพร่กระจายข้อมูลผิดพลาด การแนะนำเนื้อหาที่ไม่เหมาะสม หรือการละเมิดความเป็นส่วนตัว การเปรียบเทียบระบบความปลอดภัยของแพลตฟอร์มวิดีโอสั้นแต่ละแพลตฟอร์ม เพื่อหาองค์ประกอบร่วมและองค์ประกอบเฉพาะที่ส่งผลต่อความปลอดภัย 2.2 การศึกษาครั้งต่อไปควรศึกษาระดับความรู้เท่าทันดิจิทัล (Digital Literacy) ของผู้ใช้ที่สัมพันธ์กับพฤติกรรมความปลอดภัยบนแพลตฟอร์ม กลไกการตอบสนองต่อภัยคุกคามไซเบอร์ของ AI เช่น Deepfake, Phishing และ Malware ที่แพร่ในรูปแบบวิดีโอสั้น 2.3 งานวิจัยในอนาคตควรพัฒนาเพิ่มเติมการประเมินความปลอดภัยเชิงทดลอง (Experimental Security Testing) เพื่อทดสอบประสิทธิภาพของ

โมเดล CIA Triad ในสถานการณ์เสมือนจริง การพัฒนาโมเดลเชิงสถิติหรือโมเดลเชิงระบบ (System Dynamics) เพื่อคาดการณ์ความเสี่ยงความปลอดภัยของแพลตฟอร์มในอนาคต

เอกสารอ้างอิง

Chen, Q., & Peng, Y. (2022). Traffic rewards, algorithmic visibility, and advertiser satisfaction: How Chinese short-video platforms cultivate creators in stages. Convergence: The International Journal of Research into New Media Technologies, 28(6), 1537–1554. https://doi.org/10.1177/13548565221128206

Chen, S. (2023). How social media can solve the problem of “filter bubbles” under the new media algorithm recommendation mechanism: The example of TikTok. Proceedings of the 2023 2nd International Conference on Social Sciences and Humanities and Arts (SSHA 2023), 1284–1288. Atlantis Press. https://doi.org/10.2991/978-2-38476-062-6_165

Paat, Y., & Markham, C. (2021). Digital crime, trauma, and abuse: Internet safety and cyber risks for adolescents and emerging adults in the 21st century. Social Work in Mental Health, 19(5), 367–386. https://doi.org/10.1080/15332985.2021.1914085

Postman, N. (2000). The humanism of media ecology. Proceedings of the Media Ecology Association, 1, 10–16.

Senapati, A., et al. (2023). Digital 2023: Global overview report. DataReportal (We Are Social & Meltwater).

Seo, M. (2021). Adolescents’ exposure to online risks: Gender disparities and vulnerabilities related to online behaviors. International Journal of Environmental Research and Public Health, 18(4), 2185. https://doi.org/10.3390/ijerph18042185

Yeung, K. (2018). Algorithmic regulation: A critical interrogation. Regulation & Governance, 12(4), 505–523. https://doi.org/10.1111/rego.12132

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. New York: PublicAffairs.