แนวทางรับมือด้านความปลอดภัยและความเป็นส่วนตัวในระบบสารสนเทศทางการบัญชี: ปัจจุบันและอนาคต

APPROACHES TO SECURITY AND PRIVACY IN ACCOUNTING INFORMATION SYSTEMS: CURRENT AND FUTURE PERSPECTIVES

อัครเดช ฉวีรักษ์

Aukkaradej Chaveerug

คณะบัญชี มหาวิทยาลัยราชภัฏเชียงราย

Faculty of Accounting, Chiang Rai Rajabhat University

Corresponding Author e-mail: aj.aukmsb@gmail.com

Received March 3, 2025; **Revised** May 27, 2025; **Accepted** May 29, 2025

บทคัดย่อ

ในยุคดิจิทัลที่ระบบสารสนเทศทางการบัญชีมีบทบาทสำคัญต่อการดำเนินธุรกิจ ความเสี่ยงด้านความปลอดภัยและความเป็นส่วนตัวของข้อมูลได้กลายเป็นประเด็นที่องค์กรต้องให้ความสำคัญอย่างยิ่ง เนื่องจากภัยคุกคามไซเบอร์มีความซับซ้อนและเปลี่ยนแปลงอยู่ตลอดเวลา การบริหารจัดการข้อมูลอย่างมีประสิทธิภาพจึงเป็นปัจจัยสำคัญในการสร้างความเชื่อมั่นและเสริมสร้างความยั่งยืนในการดำเนินงานขององค์กร

บทความวิชาการนี้ ผู้เขียนจะนำเสนอ 1) สถานการณ์และปัญหาด้านความปลอดภัยและความเป็นส่วนตัวของข้อมูลในระบบสารสนเทศทางการบัญชี 2) แนวทางด้านเทคโนโลยีเพื่อลดความเสี่ยง เช่น การเข้ารหัสข้อมูล การยืนยันตัวตนหลายขั้นตอน (Multi-Factor Authentication) และแนวคิด Zero Trust Security 3) การเสริมสร้างทักษะบุคลากรผ่านการฝึกอบรมด้านความปลอดภัยไซเบอร์ 4) การวิเคราะห์การปฏิบัติตามกฎหมายที่เกี่ยวข้อง ได้แก่ General Data Protection Regulation (GDPR) และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และ 5) แนวทางการสร้างวัฒนธรรมความปลอดภัยภายในองค์กรควบคู่กับการบูรณาการเทคโนโลยีที่เหมาะสม องค์ความรู้จากบทความนี้สามารถนำไปใช้กำหนดนโยบายหรือแนวทางการบริหารจัดการความมั่นคงของข้อมูลในระบบบัญชีได้อย่างมีประสิทธิภาพ ลดความเสี่ยงจากการละเมิดข้อมูล เสริมสร้างความเชื่อมั่นให้แก่ผู้มีส่วนได้ส่วนเสีย และสนับสนุนการดำเนินธุรกิจอย่างยั่งยืนในระยะยาว

คำสำคัญ: ข้อมูล; ระบบสารสนเทศทางการบัญชี; PDPA; ภัยคุกคามไซเบอร์

Abstract

In the digital era, where accounting information systems play a critical role in business operations, the risks related to data security and privacy have become a paramount concern for organizations. Cyber threats are increasingly complex and continuously evolving, making

effective data management essential for building trust and enhancing organizational sustainability.

This academic article presents 1) the current situation and challenges related to data security and privacy in accounting information systems; 2) technological approaches to mitigate risks, such as data encryption, multi-factor authentication (MFA), and the Zero Trust Security model; 3) capacity building through cybersecurity training for personnel; 4) an analysis of compliance with relevant laws, including the European Union's General Data Protection Regulation (GDPR) and Thailand's Personal Data Protection Act (PDPA) B.E. 2562; and 5) strategies for cultivating a security-conscious culture within organizations alongside appropriate technological integration. The knowledge gained from this study can guide the formulation of policies or frameworks for effectively managing information security in accounting systems, reducing data breach risks, strengthening stakeholder confidence, and supporting sustainable business operations in the long term.

Keywords: Data; Accounting Information Systems; PDPA; Cyber Threats

บทนำ

ในยุคดิจิทัลที่ระบบสารสนเทศทางการบัญชี (Accounting Information Systems: AIS) มีบทบาทสำคัญในการเก็บรวบรวม ประมวลผล และรายงานข้อมูลทางการเงิน ความปลอดภัยของข้อมูล (Data Security) และความเป็นส่วนตัวของข้อมูล (Data Privacy) กลายเป็นหัวใจหลักที่องค์กรไม่สามารถมองข้ามได้ ข้อมูลทางบัญชีมักเป็นข้อมูลที่มีความอ่อนไหว เช่น ข้อมูลลูกค้า รายละเอียดการเงิน และกลยุทธ์ทางธุรกิจ หากเกิดการรั่วไหลหรือถูกโจมตี ย่อมส่งผลต่อความเชื่อมั่นของผู้มีส่วนได้ส่วนเสียอย่างรุนแรง (Smith et al., 2020) รายงานของ IBM (2023) ระบุว่า ความเสียหายเฉลี่ยจากการละเมิดข้อมูลสูงถึง 4.45 ล้านดอลลาร์สหรัฐ และเพิ่มขึ้นต่อเนื่อง โดยเฉพาะในอุตสาหกรรมบัญชีและการเงินที่มีความเสี่ยงสูงเป็นอันดับต้น ๆ สาเหตุสำคัญของปัญหา ได้แก่ ระบบที่ล้าสมัย การขาดการเข้ารหัสที่มีประสิทธิภาพ และการไม่ปฏิบัติตามมาตรฐานความมั่นคง เช่น ISO/IEC 27001 หรือ COBIT 5 (Zhang et al., 2023)

แนวคิดที่เกี่ยวข้องกับการจัดการความปลอดภัยของระบบสารสนเทศที่ได้รับความสนใจในช่วงหลัง ได้แก่ แนวคิด Zero Trust Security เสนอว่า องค์กรไม่ควรไว้ใจผู้ใช้งานหรืออุปกรณ์ใด ๆ โดยไม่มีการตรวจสอบสิทธิ์แม้ภายในระบบของตนเอง (Kindervag, 2010) แนวคิดนี้ได้รับการสนับสนุนจากงานวิจัยหลากหลายที่ชี้ว่าการนำ Zero Trust มาปรับใช้ร่วมกับแนวทางการพิสูจน์ตัวตนแบบหลายขั้นตอน (Multi-Factor Authentication) และการจัดการสิทธิ์เข้าถึงข้อมูล สามารถลดโอกาสการถูกเจาะระบบได้อย่างมีนัยสำคัญ (Cheng et al., 2022) นอกจากนี้ องค์กรที่ประสบความสำเร็จในการรักษาความมั่นคงของข้อมูลมักให้ความสำคัญกับการพัฒนาทักษะของบุคลากรและสร้างวัฒนธรรมด้านความปลอดภัยอย่างยั่งยืน (Nguyen & Le, 2021)

บทความฉบับนี้มีวัตถุประสงค์เพื่อศึกษาแนวทางการบริหารจัดการความปลอดภัยและความเป็นส่วนตัวของข้อมูลในระบบสารสนเทศทางการบัญชี โดยวิเคราะห์จากเอกสารวิชาการและมาตรฐานสากล เพื่อเสนอแนวทางปฏิบัติที่สามารถนำไปใช้ได้จริงในองค์กรธุรกิจยุคดิจิทัล เน้นการวิเคราะห์จากมุมมองขององค์กรธุรกิจที่เป็นผู้ใช้งานจริง ทั้งในด้านนโยบาย เทคโนโลยี กฎหมาย และพฤติกรรมของบุคลากร วิธีการศึกษาประกอบด้วยการทบทวนวรรณกรรมที่เกี่ยวข้อง มาตรฐานสากลด้านความปลอดภัยไซเบอร์ โดยมุ่งนำเสนอข้อมูลที่สามารถประยุกต์ใช้ได้จริงในบริบทการทำงาน

บทความวิชาการนี้ ผู้เขียนจะนำเสนอ 1) สถานการณ์และความเสี่ยงด้านความปลอดภัยและความเป็นส่วนตัวในระบบสารสนเทศทางการบัญชี 2) แนวทางด้านเทคโนโลยีที่องค์กรควรใช้ เช่น การเข้ารหัส การพิสูจน์ตัวตนหลายขั้นตอน และแนวคิด Zero Trust Security 3) การเสริมสร้างทักษะของบุคลากรผ่านการอบรมด้านความปลอดภัยไซเบอร์ 4) การปฏิบัติตามกฎหมายสำคัญ เช่น GDPR และ PDPA และ 5) การสร้างวัฒนธรรมด้านความปลอดภัยในองค์กรเพื่อรองรับการเปลี่ยนแปลงในอนาคต องค์ความรู้จากบทความนี้จะเป็นประโยชน์ต่อการวางแผนนโยบายด้าน IT Security ขององค์กรธุรกิจ และส่งเสริมแนวทางการบริหารจัดการข้อมูลทางบัญชีอย่างยั่งยืนในยุคดิจิทัล

สถานการณ์และความเสี่ยงด้านความปลอดภัยและความเป็นส่วนตัวในระบบสารสนเทศทางการบัญชี

ในยุคดิจิทัลที่ข้อมูลกลายเป็นสินทรัพย์สำคัญขององค์กร ระบบสารสนเทศทางการบัญชี ถูกนำมาใช้เพื่อเพิ่มประสิทธิภาพในการจัดเก็บ ประมวลผล และรายงานข้อมูลทางการเงินอย่างกว้างขวาง (Romney & Steinbart, 2021) อย่างไรก็ตาม การพึ่งพาเทคโนโลยีสารสนเทศและการเชื่อมโยงระบบเข้ากับเครือข่ายภายนอกส่งผลให้ระบบ AIS เผชิญกับความเสี่ยงด้านความปลอดภัยไซเบอร์และความเป็นส่วนตัวของข้อมูลที่เพิ่มสูงขึ้นอย่างมีนัยสำคัญ (Kshetri & Voas, 2023; Symantec, 2024) หากไม่มีการบริหารจัดการอย่างเหมาะสม จะส่งผลกระทบต่อความน่าเชื่อถือและความถูกต้องของข้อมูลบัญชีที่เป็นหัวใจของการตัดสินใจทางธุรกิจ

สถานการณ์ปัจจุบัน

ในปัจจุบัน ธุรกิจจำนวนมากหันมาใช้เทคโนโลยีใหม่ ๆ เช่น Cloud Accounting, Artificial Intelligence (AI), Machine Learning (ML), Blockchain และ Internet of Things (IoT) เพื่อยกระดับประสิทธิภาพของ AIS (Brynjolfsson & McAfee, 2022; Rashid et al., 2023) อย่างไรก็ดี เทคโนโลยีเหล่านี้ก็ได้เปิดช่องโหว่และทางเข้าสำหรับการโจมตีทางไซเบอร์รูปแบบใหม่ (Newman, 2023) การศึกษาพบว่าองค์กรขนาดกลางและเล็กส่วนใหญ่ยังขาดการบูรณาการมาตรการรักษาความปลอดภัยอย่างเข้มงวดและครบถ้วน (Chen et al., 2023) ส่งผลให้ความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์และการละเมิดความเป็นส่วนตัวของข้อมูลบัญชียังคงเพิ่มขึ้นอย่างต่อเนื่อง

ความเสี่ยงหลักที่พบบ่อยในระบบ AIS

จากการศึกษางานวิจัยและรายงานล่าสุด พบว่า ความเสี่ยงหลักที่ระบบ AIS เผชิญในปัจจุบันมักส่งผลกระทบโดยตรงต่อความถูกต้องของข้อมูลทางบัญชี และความน่าเชื่อถือในการตัดสินใจทางธุรกิจ องค์กรจึงจำเป็นต้องเข้าใจและบริหารจัดการความเสี่ยงเหล่านี้อย่างมีประสิทธิภาพ ดังนี้

1. ภัยคุกคามจากแฮกเกอร์และมัลแวร์ เช่น การโจมตีด้วยแรนซัมแวร์ (ransomware) ผู้โจมตีจะเข้ารหัสข้อมูลบัญชีและเรียกค่าไถ่เพื่อปลดล็อก ทำให้ระบบบัญชีหยุดชะงักและธุรกิจได้รับผลกระทบอย่างรุนแรง (Symantec, 2024)

2. การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต (Unauthorized Access) มักเกิดจากการกำหนดสิทธิ์การเข้าถึงที่ไม่เหมาะสม หรือขาดการใช้มาตรการพิสูจน์ตัวตนแบบหลายขั้นตอน (Multi-Factor Authentication: MFA) ที่มีประสิทธิภาพ (Kshetri & Voas, 2023)

3. ความผิดพลาดของมนุษย์ (Human Error) เป็นสาเหตุอันดับต้น ๆ ของความเสี่ยงในระบบ AIS เช่น การกรอกข้อมูลผิด การคลิกลิงก์ฟิชชิง หรือการเปิดเผยข้อมูลโดยไม่ได้ตั้งใจ (Chen et al., 2023) แม้จะเป็นข้อผิดพลาดที่ไม่เจตนา แต่ก็ส่งผลกระทบร้ายแรงต่อความปลอดภัยของข้อมูล

4. ช่องโหว่จากเทคโนโลยีใหม่ที่ยังไม่สมบูรณ์ (Immature Technology Risks) ตัวอย่างเช่น Blockchain อาจเพิ่มความโปร่งใสและความปลอดภัย แต่ยังขาดมาตรฐานทางเทคนิคที่เป็นที่ยอมรับทั่วไป และ Quantum Computing มีศักยภาพในการทำลายระบบเข้ารหัสข้อมูลแบบดั้งเดิมในอนาคตอันใกล้ (Arora et al., 2023; Deloitte, 2022)

5. การละเมิดกฎหมายด้านข้อมูลส่วนบุคคล การไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล เช่น PDPA หรือ GDPR ส่งผลให้บริษัทเสี่ยงต่อการถูกฟ้องร้องและถูกปรับเป็นจำนวนมาก (Voigt & Bussche, 2022)

6. การโจมตีจากภายในองค์กร (Insider Threats) บุคลากรภายในที่มีสิทธิ์เข้าถึงระบบ AIS อาจมีพฤติกรรมที่เป็นภัย เช่น ขโมยข้อมูล แก้ไขข้อมูลโดยเจตนา หรือเปิดเผยข้อมูลสำคัญแก่บุคคลภายนอก (Greitzer & Frincke, 2010)

ด้วยเหตุนี้ การเพิ่มความตระหนักรู้และการจัดการความเสี่ยงด้านความปลอดภัย รวมถึงความเป็นส่วนตัวของข้อมูลในระบบ AIS จึงเป็นเรื่องจำเป็นอย่างยิ่งในทุกระดับขององค์กร โดยเฉพาะอย่างยิ่งกับองค์กรขนาดเล็กและขนาดกลางที่มักมีข้อจำกัดด้านทรัพยากรและงบประมาณ การนำเทคโนโลยีป้องกันภัยคุกคามสมัยใหม่ เช่น การเข้ารหัสข้อมูล การพิสูจน์ตัวตนแบบหลายขั้นตอน และแนวคิด Zero Trust Security มาประยุกต์ใช้อย่างเหมาะสม ควบคู่กับการฝึกอบรมและพัฒนาทักษะบุคลากรอย่างต่อเนื่อง จะช่วยเสริมสร้างวัฒนธรรมความปลอดภัยของข้อมูลในองค์กรได้อย่างยั่งยืนและมีประสิทธิภาพ

เทคโนโลยีที่มีผลกระทบต่อความปลอดภัยและความเป็นส่วนตัวในระบบสารสนเทศทางการบัญชี และแนวทางเสริมสร้างความปลอดภัย

ความหมายของความปลอดภัยทางไซเบอร์ และความเป็นส่วนตัวของข้อมูล

ความปลอดภัยทางไซเบอร์ (Cybersecurity) หมายถึง มาตรการปกป้องข้อมูล ระบบ และเครือข่ายจากภัยคุกคามดิจิทัล เช่น แฮกเกอร์ มัลแวร์ และการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต (Stallings, 2021) ในระบบสารสนเทศทางการบัญชี (AIS) เน้นการปกป้องข้อมูลทางการเงินและเอกสารสำคัญจากการรั่วไหลหรือคุกคามที่ส่งผลต่อความน่าเชื่อถือของข้อมูล (Chen et al., 2022) ระบบ AIS จึงต้องมีมาตรการป้องกันภัยคุกคามในทุกขั้นตอนของการทำบัญชี

ความเป็นส่วนตัวของข้อมูล (Data Privacy) หมายถึง สิทธิในการควบคุมข้อมูลส่วนบุคคลและข้อมูลทางการเงินที่มีความละเอียดอ่อน (Westin, 2020) ในระบบสารสนเทศทางการบัญชี ข้อมูลดังกล่าวต้องได้รับการปกป้องจากการเข้าถึงหรือเปิดเผยโดยไม่ได้รับอนุญาต โดยนักบัญชีและผู้บริหารองค์กรจำเป็นต้องจัดการข้อมูลลูกค้าและองค์กรอย่างปลอดภัยตามมาตรการควบคุมที่เข้มงวด (Smith & Miller, 2023)

มาตรฐานและกฎหมายที่เกี่ยวข้อง

- IFRS (International Financial Reporting Standards) กำหนดหลักเกณฑ์การจัดทำรายงานทางการเงินให้โปร่งใสและมีการควบคุมภายในที่รัดกุม ช่วยป้องกันการเข้าถึงข้อมูลที่ไม่ได้รับอนุญาตและการแก้ไขข้อมูล (IASB, 2021)
- GDPR (General Data Protection Regulation) กฎหมายของสหภาพยุโรปกำหนดการจัดการข้อมูลส่วนบุคคลอย่างเข้มงวด โดยให้ความสำคัญกับการปกป้องข้อมูลและการให้ความโปร่งใสแก่เจ้าของข้อมูล (Voigt & Bussche, 2022)
- PDPA (Personal Data Protection Act) กฎหมายไทยที่กำหนดมาตรการปกป้องข้อมูลส่วนบุคคลและการขอความยินยอมจากเจ้าของข้อมูล โดยมุ่งป้องกันการรั่วไหลและการใช้ข้อมูลโดยมิชอบ (Electronic Transactions Development Agency, 2023)
- SOX (Sarbanes-Oxley Act) กฎหมายสหรัฐอเมริกาที่กำหนดการควบคุมภายในอย่างเข้มงวดเพื่อป้องกันการทุจริตทางบัญชีและการตรวจสอบการเข้าถึงข้อมูลทางการเงิน เพื่อให้มั่นใจว่ารายงานการเงินเป็นไปตามข้อกำหนด (Coates, 2021)

เทคโนโลยีที่มีผลกระทบต่อความปลอดภัยและความเป็นส่วนตัวในระบบสารสนเทศทางการบัญชี

ระบบสารสนเทศทางการบัญชี เป็นระบบที่รวบรวม ประมวลผล และจัดเก็บข้อมูลทางบัญชีเพื่อสนับสนุนการรายงานทางการเงินและการตัดสินใจขององค์กร โดยใช้เทคโนโลยีสารสนเทศเพิ่มประสิทธิภาพในการทำงาน (Romney & Steinbart, 2021) เทคโนโลยีที่เกี่ยวข้องกับระบบ AIS ส่งผลโดยตรงต่อความปลอดภัยและความเป็นส่วนตัวของข้อมูลบัญชี จำเป็นต้องมีมาตรการและแนวทางปกป้องที่เหมาะสม ปัจจุบันมีเทคโนโลยีที่นิยมใช้ในระบบสารสนเทศทางการบัญชี ดังนี้

• ระบบบัญชีบนคลาวด์ (Cloud Accounting) เป็นส่วนหนึ่งของระบบสารสนเทศทางการบัญชี (AIS) ที่ช่วยให้ธุรกิจเข้าถึงและจัดการข้อมูลได้ทุกที่ทุกเวลาโดยไม่ต้องติดตั้งซอฟต์แวร์ภายในองค์กร ข้อดี ได้แก่ การทำงานร่วมกันสะดวก การสำรองข้อมูลอัตโนมัติ และการจัดการที่เป็นระบบ อย่างไรก็ตาม ยังมีความเสี่ยงด้านความปลอดภัย เช่น การเข้าถึงโดยไม่ได้รับอนุญาต สามารถลดได้ด้วยการเข้ารหัสข้อมูล การควบคุมสิทธิ์ และการเลือกใช้ผู้ให้บริการที่เชื่อถือได้ (Rashid et al., 2023)

• ปัญญาประดิษฐ์และการเรียนรู้ของเครื่อง มีบทบาทสำคัญใน AIS โดยช่วยวิเคราะห์ข้อมูลจำนวนมาก ตรวจจับธุรกรรมผิดปกติ เช่น การจ่ายเงินซ้ำ หรือพฤติกรรมที่อาจบ่งชี้ถึงการทุจริต เพิ่มความแม่นยำในการรายงาน ลดภาระงานซ้ำซ้อน และเพิ่มความน่าเชื่อถือของข้อมูลทางการเงิน (Brynjolfsson & McAfee, 2022)

• เทคโนโลยี Blockchain ช่วยจัดเก็บข้อมูลบัญชีอย่างปลอดภัย โปร่งใส และไม่สามารถแก้ไขย้อนหลังได้ ลดการพึ่งพาตัวกลาง และเพิ่มความเชื่อมั่นในธุรกรรมทางการเงิน เช่น การโอนเงินและการจัดการภาษี (Coyne & McMickle, 2017)

• การคำนวณควอนตัม (Quantum Computing) แม้อยู่ในช่วงพัฒนา แต่มีศักยภาพในการประมวลผลข้อมูลที่รวดเร็ว อาจคุกคามระบบเข้ารหัสปัจจุบัน ส่งผลต่อความปลอดภัยของข้อมูลทางบัญชี องค์กรจึงควรเตรียมรับมือด้วยเทคโนโลยีเข้ารหัสแบบใหม่ (Post-Quantum Cryptography) และติดตามความก้าวหน้าอย่างใกล้ชิด (Deloitte, 2022; Arora et al., 2023)

แนวทางการเสริมสร้างความปลอดภัยและความเป็นส่วนตัวในระบบสารสนเทศทางการบัญชี เพื่อรองรับผลกระทบจากเทคโนโลยีดังกล่าวและปกป้องข้อมูลทางบัญชีจากภัยคุกคามต่าง ๆ องค์กรควรนำแนวทางเสริมสร้างความปลอดภัยและความเป็นส่วนตัวมาปรับใช้ ดังนี้

• การเข้ารหัสข้อมูล ถือเป็นวิธีปกป้องข้อมูลที่มีประสิทธิภาพสูงสุด เทคนิคการเข้ารหัส เช่น AES-256 หรือ RSA จะเปลี่ยนข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถอ่านได้หากไม่มีคีย์ถอดรหัส ช่วยปกป้องข้อมูลทั้งในขั้นตอนการจัดเก็บและการส่งผ่านข้อมูลผ่านเครือข่ายอินเทอร์เน็ต ลดความเสี่ยงจากการถูกดักฟังหรือขโมยข้อมูลระหว่างทาง (Stallings, 2021) นอกจากนี้ การจัดการกุญแจเข้ารหัส (Key Management) อย่างเข้มงวดเป็นสิ่งสำคัญไม่แพ้กันเพื่อรักษาความปลอดภัยของระบบ

• การพิสูจน์ตัวตนแบบหลายขั้นตอน ช่วยเพิ่มชั้นความปลอดภัยในการเข้าถึงระบบ AIS โดยบังคับให้ผู้ใช้ผ่านการยืนยันตัวตนมากกว่าหนึ่งขั้นตอน เช่น รหัสผ่านควบคู่กับรหัส OTP ผ่านมือถือ หรือการสแกนลายนิ้วมือ ช่วยลดความเสี่ยงที่แฮกเกอร์จะเข้าถึงระบบเพียงแค่ขโมยรหัสผ่านได้ (Chen et al., 2022) การใช้ MFA เป็นมาตรฐานพื้นฐานจะช่วยปกป้องข้อมูลสำคัญจากการโจมตีด้วยการปลอมแปลงตัวตนอย่างมีประสิทธิภาพ

• นโยบาย Zero Trust Security เป็นการตั้งสมมติฐานว่าไม่มีใครในหรือภายนอกองค์กรที่ควรได้รับความไว้วางใจโดยอัตโนมัติ ทุกการเข้าถึงต้องได้รับการตรวจสอบและอนุมัติอย่างละเอียดทุกครั้ง (Rose et al., 2020) ด้วยการใช้เทคโนโลยี เช่น behavioral analytics เพื่อตรวจจับพฤติกรรมผิดปกติ การเข้ารหัส

ข้อมูลทั้งขณะพักและขณะส่งผ่าน และการจำกัดสิทธิ์เข้าถึงอย่างเข้มงวด องค์กรจะสามารถป้องกันภัยคุกคามทั้งจากภายนอกและภายในได้อย่างมีประสิทธิภาพ

- การสำรองข้อมูลและแผนฟื้นฟูระบบ การจัดทำแผนสำรองข้อมูลอย่างสม่ำเสมอในสถานที่แยกต่างหาก และการมีแผนฟื้นฟูระบบที่ชัดเจน เป็นสิ่งจำเป็นสำหรับรับมือเหตุฉุกเฉิน เช่น การโจมตีด้วยแรนซัมแวร์ ไฟไหม้ หรือภัยพิบัติธรรมชาติ (Rashid et al., 2023) การสำรองข้อมูลที่ครบถ้วนและเป็นปัจจุบันช่วยให้ธุรกิจกู้คืนข้อมูลสำคัญและกลับมาดำเนินงานได้อย่างรวดเร็ว ลดผลกระทบทางธุรกิจและสร้างความมั่นใจแก่ผู้มีส่วนได้ส่วนเสีย

สรุปได้ว่า เทคโนโลยีที่ใช้ในระบบ AIS ที่ทันสมัย เช่น Cloud Accounting, AI/ML, Blockchain และ Quantum Computing ต่างสร้างทั้งโอกาสและความเสี่ยงด้านความปลอดภัย ขณะเดียวกัน การนำแนวทางปฏิบัติด้านความปลอดภัย เช่น การเข้ารหัสข้อมูล, MFA, Zero Trust Security และการสำรองข้อมูล มาใช้จะช่วยเสริมสร้างความมั่นคงปลอดภัยของข้อมูลทางบัญชี และลดความเสี่ยงจากภัยคุกคามในยุคดิจิทัลได้อย่างมีประสิทธิภาพ

การเสริมสร้างทักษะของบุคลากรผ่านการฝึกอบรมด้านความปลอดภัยไซเบอร์

ในยุคดิจิทัลที่เทคโนโลยีสารสนเทศเข้ามามีบทบาทอย่างลึกซึ้งในระบบงานบัญชี บุคลากรในองค์กรกลายเป็นแนวป้องกันด่านแรกในการรักษาความปลอดภัยของระบบสารสนเทศทางการบัญชี เนื่องจากภัยคุกคามจำนวนมาก เช่น การโจมตีแบบฟิชชิง (Phishing) การแนบไฟล์มัลแวร์ การโจมตีผ่านอีเมลหลอกลวง หรือแม้แต่การใช้รหัสผ่านที่อ่อนแอ มักเกิดจากพฤติกรรมหรือความไม่รู้ของพนักงาน (Verizon, 2023) จากรายงานของ Ponemon Institute (2022) พบว่า มากกว่า 82% ของเหตุการณ์การละเมิดข้อมูลเกิดจากข้อผิดพลาดของมนุษย์ ไม่ว่าจะเป็นการคลิกลิงก์อันตราย การให้สิทธิ์เข้าถึงระบบโดยไม่เหมาะสม หรือการไม่ปฏิบัติตามนโยบายความปลอดภัยองค์กร ดังนั้น การพัฒนาทักษะและความตระหนักรู้ของบุคลากรผ่านการฝึกอบรมด้านความปลอดภัยไซเบอร์ (Cybersecurity Training) จึงเป็นกลยุทธ์สำคัญในการลดความเสี่ยงในระดับองค์กร สำหรับประเภทของการฝึกอบรมด้านความปลอดภัยไซเบอร์ ประกอบด้วย

1. การอบรมทั่วไปด้านความตระหนักรู้ (Security Awareness Training) มุ่งเน้นให้บุคลากรทุกระดับในองค์กรมีความเข้าใจพื้นฐานเกี่ยวกับภัยคุกคามทางไซเบอร์ เช่น การหลอกลวงแบบฟิชชิง การตั้งรหัสผ่านที่ปลอดภัย การใช้เครือข่าย Wi-Fi สาธารณะอย่างระมัดระวัง และการล็อกหน้าจอเมื่อไม่อยู่ที่โต๊ะทำงาน โดยแนะนำให้จัดการอบรมลักษณะนี้อย่างน้อยปีละ 1–2 ครั้ง ควบคู่กับการประเมินความเข้าใจหลังการอบรม (ENISA, 2023)

2. การจำลองเหตุการณ์ (Simulation Training) ใช้สถานการณ์จำลอง เช่น การส่งอีเมลฟิชชิงเทียมเพื่อประเมินการตอบสนองของบุคลากร หรือการฝึกซ้อมสถานการณ์ฉุกเฉิน เช่น การโจมตีด้วย Ransomware เพื่อให้พนักงานสามารถตัดสินใจภายใต้ความกดดันได้อย่างถูกต้องและทันเวลา (KnowBe4, 2023)

3. การอบรมเฉพาะทาง (Role-Based Training) การอบรมนี้มุ่งเน้นที่หน้าที่เฉพาะของแต่ละกลุ่มบุคลากร ยังสนับสนุนการจัดระบบควบคุมภายในให้สอดคล้องกับมาตรฐานสากล เช่น ISO/IEC 27001 และ Sarbanes-Oxley Act (SOX) (ISACA, 2022) เช่น ฝ่ายบัญชี/การเงิน ควรเรียนรู้เกี่ยวกับการตรวจจับธุรกรรมต้องสงสัย และการป้องกันการหลอกลวงแบบ CEO fraud ฝ่าย IT ต้องเข้าใจการตั้งค่าระบบ เช่น Firewall, การควบคุมสิทธิ์ผู้ใช้ และการจัดการ log file และผู้บริหาร ควรเข้าใจภาพรวมของความเสี่ยงและสามารถกำหนดนโยบายด้านความปลอดภัยขององค์กรได้

ปัจจัยที่ส่งเสริมให้การฝึกอบรมมีประสิทธิภาพ

- การฝึกอบรมอย่างต่อเนื่องและทันสมัย เนื้อหาควรอัปเดตภัยคุกคามใหม่ที่องค์กรพบเจอเป็นประจำ เพื่อให้ทันต่อสถานการณ์
- การสนับสนุนจากผู้บริหารระดับสูง (Top-down Support) การแสดงจุดยืนของผู้บริหารจะสร้างแรงผลักดันเชิงวัฒนธรรมในองค์กร
- การประเมินผลหลังการอบรม เช่น การใช้แบบสอบถามพฤติกรรมหรือการวิเคราะห์แนวโน้มการตอบสนองต่อภัยไซเบอร์
- การบูรณาการความปลอดภัยเข้ากับกระบวนการปฏิบัติงาน เช่น การกำหนดให้ใช้การยืนยันตัวตนหลายขั้นตอน (Multi-Factor Authentication – MFA) ในการอนุมัติธุรกรรมบัญชี

รายงานของ European Union Agency for Cybersecurity (ENISA, 2023) ชี้ว่า องค์กรที่มีการอบรมพนักงานด้านความปลอดภัยทางไซเบอร์อย่างสม่ำเสมอสามารถลดอัตราการตกเป็นเหยื่อของฟิชชิงได้ถึง 70% ภายใน 6 เดือน และมีแนวโน้มที่จะปฏิบัติตามข้อกำหนดของกฎหมาย เช่น PDPA ของไทย และ GDPR ของสหภาพยุโรป ได้อย่างมีประสิทธิภาพมากขึ้น ตัวอย่างการนำไปใช้จริงในองค์กร เช่น บริษัทผู้ให้บริการบัญชีข้ามชาติแห่งหนึ่งในประเทศสิงคโปร์ ได้นำโครงการ Cyber Hygiene for Accountants มาใช้ โดยฝึกอบรมให้พนักงานบัญชีสามารถวิเคราะห์ความถูกต้องของอีเมลคำสั่งโอนเงิน และจำลองสถานการณ์ฉุกเฉินแบบ Tabletop Exercise เพื่อฝึกตอบสนองต่อเหตุการณ์ที่อาจเกิดขึ้นจริง ส่งผลให้สามารถลดอัตราการโอนเงินผิดบัญชีจากการหลอกลวงแบบฟิชชิงลงได้มากกว่า 90% ภายในเวลาเพียง 1 ปี

การวิเคราะห์การปฏิบัติตามกฎหมายที่เกี่ยวข้อง

ในยุคที่ข้อมูลกลายเป็นทรัพยากรเชิงกลยุทธ์ การปกป้องข้อมูลส่วนบุคคลไม่เพียงแต่เป็นข้อกำหนดทางกฎหมายเท่านั้น หากยังเป็นรากฐานสำคัญของการสร้างความไว้วางใจระหว่างองค์กรกับผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกองค์กร โดยเฉพาะอย่างยิ่งเมื่อองค์กรมีการใช้ระบบสารสนเทศทางการบัญชี มีการจัดเก็บ ประมวลผล และเปิดเผยข้อมูลที่เกี่ยวข้องกับลูกค้า พนักงาน และคู่ค้าอย่างต่อเนื่อง

ในระดับสากล กฎหมาย General Data Protection Regulation (GDPR) ของสหภาพยุโรป ซึ่งมีผลบังคับใช้ตั้งแต่ปี ค.ศ. 2018 ถือเป็นมาตรฐานสำคัญด้านการคุ้มครองข้อมูลส่วนบุคคล โดยระบุสิทธิของเจ้าของข้อมูลไว้อย่างชัดเจน เช่น สิทธิในการเข้าถึงข้อมูล (Right of Access), สิทธิในการลบข้อมูล (Right to

Erasure) และสิทธิในการโอนย้ายข้อมูล (Right to Data Portability) (European Commission, 2022) องค์กรที่ฝ่าฝืนอาจต้องรับโทษปรับสูงสุดถึง 20 ล้านยูโร หรือ 4% ของรายได้ทั่วโลกในปีบัญชีที่ผ่านมา แล้วแต่จำนวนใดจะสูงกว่า (European Data Protection Board, 2023) สำหรับประเทศไทย มีการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act: PDPA) อย่างเต็มรูปแบบตั้งแต่วันที่ 1 มิถุนายน 2565 มีหลักการคล้ายคลึงกับ GDPR โดยมุ่งเน้นการปกป้องข้อมูลส่วนบุคคลตั้งแต่ขั้นตอนการเก็บรวบรวม ใช้ ไปจนถึงการเปิดเผยข้อมูล และกำหนดให้องค์กรต้องขอความยินยอม (Consent) จากเจ้าของข้อมูลอย่างชัดเจนก่อนดำเนินการใด ๆ กับข้อมูลเหล่านั้น พร้อมทั้งต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) หากกิจกรรมขององค์กรมีความเสี่ยงสูงหรือประมวลผลข้อมูลในปริมาณมาก (Electronic Transactions Development Agency, 2023)

ระบบ AIS จำเป็นต้องมีการออกแบบและดำเนินงานให้สอดคล้องกับกฎหมายเหล่านี้อย่างครบถ้วน โดยเฉพาะด้าน มาตรการความปลอดภัยของข้อมูล เช่น การเข้ารหัสข้อมูล การควบคุมสิทธิ์เข้าถึง และการแจ้งเหตุข้อมูลรั่วไหล (Data Breach Notification) ภายใน 72 ชั่วโมงตามข้อกำหนดของ GDPR (ENISA, 2023) นอกจากนี้ องค์กรยังต้องดำเนินการในด้านอื่น ๆ เพื่อให้เป็นไปตามข้อกำหนดของ GDPR และ PDPA ได้แก่

- การมีนโยบายความเป็นส่วนตัว ที่ชัดเจน โปร่งใส และเข้าถึงได้ง่าย
- การจัดทำ บันทึกกิจกรรมการประมวลผลข้อมูล เพื่อใช้ในการตรวจสอบภายในและภายนอก
- การฝึกอบรมบุคลากรเพื่อเสริมสร้างความเข้าใจในบทบาทและหน้าที่ที่เกี่ยวข้องกับการคุ้มครองข้อมูล
- การดำเนินการตรวจสอบและประเมินความเสี่ยงเป็นระยะ เพื่อให้แน่ใจว่าระบบ AIS และกระบวนการที่เกี่ยวข้องมีความสอดคล้องกับกฎหมายที่เกี่ยวข้อง

หากองค์กรละเลยข้อกำหนดเหล่านี้ ย่อมเผชิญความเสี่ยงด้านกฎหมายและความเสียหายด้านชื่อเสียงอย่างรุนแรง โดย PDPA ของไทย กำหนดโทษปรับทางปกครองสูงสุด 5 ล้านบาท รวมถึงโทษทางแพ่งและอาญาในกรณีการละเมิดโดยเจตนา (สำนักงานคณะกรรมการข้อมูลส่วนบุคคล, 2566) จากรายงานของ PwC (2023) พบว่า องค์กรที่มีการปฏิบัติตามข้อกำหนดของ GDPR และ PDPA อย่างเคร่งครัด ไม่เพียงช่วยลดความเสี่ยงทางกฎหมาย แต่ยังช่วยส่งเสริมความไว้วางใจจากลูกค้าและคู่ค้าในระดับสูง นำไปสู่การยกระดับความสามารถในการแข่งขันขององค์กรในระยะยาว และส่งเสริมการดำเนินธุรกิจอย่างยั่งยืน

แนวทางในการสร้างวัฒนธรรมด้านความปลอดภัยภายในองค์กร

ในยุคที่ภัยคุกคามด้านไซเบอร์และความเสี่ยงทางข้อมูลมีความซับซ้อนและรุนแรงเพิ่มขึ้น การสร้างวัฒนธรรมด้านความปลอดภัยภายในองค์กร (Security Culture) ถือเป็นปัจจัยสำคัญที่จะช่วยให้องค์กรสามารถปกป้องข้อมูลและทรัพย์สินทางดิจิทัลได้อย่างมีประสิทธิภาพ (Safa et al., 2018) วัฒนธรรมนี้ไม่ใช่เพียงแค่การใช้เทคโนโลยีหรือมาตรการทางเทคนิคเท่านั้น แต่ยังรวมถึงการสร้างความตระหนักรู้และพฤติกรรม

ของบุคลากรในทุกระดับที่มีต่อความปลอดภัยของข้อมูลและระบบสารสนเทศ แนวทางหลักในการสร้างวัฒนธรรมด้านความปลอดภัยภายในองค์กร ได้แก่

1. การส่งเสริมความตระหนักรู้และการอบรมอย่างสม่ำเสมอ การให้ความรู้เกี่ยวกับภัยคุกคามด้านไซเบอร์ วิธีการป้องกัน และแนวปฏิบัติที่ดีในการรักษาความปลอดภัยข้อมูลแก่พนักงานทุกระดับอย่างต่อเนื่อง จะช่วยลดความเสี่ยงจากความผิดพลาดของมนุษย์ซึ่งเป็นช่องโหว่ที่พบได้บ่อย (Bulgurcu et al., 2010) เช่น การอบรมเรื่องการจัดการรหัสผ่าน การระวังฟิชชิ่ง และการใช้เครือข่ายอย่างปลอดภัย

2. การกำหนดนโยบายและมาตรฐานความปลอดภัยที่ชัดเจน องค์กรควรกำหนดนโยบายด้านความปลอดภัยข้อมูลที่ครอบคลุมและเข้มงวด พร้อมทั้งสื่อสารอย่างชัดเจนถึงบทบาทและความรับผิดชอบของแต่ละฝ่าย (Dhillon & Backhouse, 2001) นโยบายเหล่านี้ควรได้รับการทบทวนและปรับปรุงอย่างต่อเนื่องให้ทันสมัยและสอดคล้องกับเทคโนโลยีและภัยคุกคามที่เปลี่ยนแปลง

3. การนำระบบบริหารความปลอดภัยสารสนเทศ (Information Security Management System: ISMS) มาใช้ การมีระบบ ISMS เช่น มาตรฐาน ISO/IEC 27001 ช่วยให้องค์กรสามารถบริหารจัดการความเสี่ยงด้านความปลอดภัยได้อย่างเป็นระบบและมีขั้นตอนชัดเจน (ISO, 2013) พร้อมทั้งช่วยสร้างความน่าเชื่อถือแก่ผู้มีส่วนได้ส่วนเสียภายนอก

4. การสนับสนุนจากผู้บริหารระดับสูง ผู้บริหารควรเป็นตัวอย่างและสนับสนุนการสร้างวัฒนธรรมด้านความปลอดภัยผ่านการจัดสรรทรัพยากร การกำหนดนโยบาย และการส่งเสริมให้พนักงานทุกคนตระหนักถึงความสำคัญของการรักษาความปลอดภัย (Von Solms & Von Solms, 2004)

5. การสร้างช่องทางการสื่อสารและรายงานปัญหาความปลอดภัยอย่างเปิดเผย องค์กรควรส่งเสริมให้พนักงานสามารถรายงานเหตุการณ์หรือความเสี่ยงด้านความปลอดภัยได้โดยไม่ต้องกลัวการถูกลงโทษ เพื่อให้สามารถตรวจสอบและแก้ไขปัญหาได้ทันท่วงที (Ifinedo, 2012)

6. การประเมินและวัดผลวัฒนธรรมความปลอดภัยการประเมินประสิทธิภาพของวัฒนธรรมด้านความปลอดภัยโดยใช้แบบสำรวจหรือการวิเคราะห์ความเสี่ยงจะช่วยให้องค์กรเห็นภาพรวมและช่องว่างที่ต้องพัฒนา (Da Veiga & Martins, 2015)

การสร้างวัฒนธรรมด้านความปลอดภัยที่แข็งแรงส่งผลให้องค์กรสามารถปกป้องข้อมูลส่วนบุคคลและทรัพย์สินทางดิจิทัลได้อย่างยั่งยืน ลดความเสี่ยงจากการละเมิดข้อมูล และเสริมสร้างความไว้วางใจจากลูกค้าและคู่ค้าในระยะยาว (PwC, 2023)

สรุปองค์ความรู้

บทความนี้นำเสนอข้อค้นพบสำคัญว่า การบริหารจัดการด้านความปลอดภัยและความเป็นส่วนตัวของข้อมูลทางบัญชีในยุคดิจิทัล จำเป็นต้องบูรณาการมาตรการเชิงรุกทั้งในด้านเทคโนโลยีและการบริหารจัดการองค์กร เพื่อรับมือกับภัยคุกคามไซเบอร์ที่มีความซับซ้อนและเพิ่มขึ้นอย่างต่อเนื่อง เช่น การโจมตีด้วยมัลแวร์ การลักลอบเข้าถึงข้อมูล และการขโมยข้อมูลส่วนบุคคล โดยเฉพาะองค์กรที่พึ่งพาระบบสารสนเทศทางบัญชี

ควรให้ความสำคัญกับการใช้เทคโนโลยีที่เหมาะสม เช่น การเข้ารหัสข้อมูล ระบบยืนยันตัวตนหลายชั้น และแนวคิด Zero Trust Security ควบคู่กับการส่งเสริมทักษะด้านความปลอดภัยไซเบอร์ของบุคลากร เพื่อเพิ่มประสิทธิภาพในการป้องกันข้อมูล ลดความเสี่ยง และสร้างความเชื่อมั่นในระบบสารสนเทศทางการเงินและการบัญชี

องค์ความรู้และนวัตกรรม องค์ความรู้ที่ได้จากการศึกษานี้สะท้อนถึงแนวทางการพัฒนากลยุทธ์การรักษาความปลอดภัยที่มีความครอบคลุม โดยการประยุกต์ใช้เทคโนโลยีสมัยใหม่ เช่น ปัญญาประดิษฐ์ และเทคโนโลยีบล็อกเชน เพื่อเพิ่มศักยภาพในการตรวจจับและตอบสนองต่อภัยคุกคามได้อย่างแม่นยำและทันท่วงที องค์ความรู้ดังกล่าวสอดคล้องกับเป้าหมายในการส่งเสริมความมั่นคงปลอดภัย ความโปร่งใส และความน่าเชื่อถือของข้อมูลทางบัญชีในบริบทของการดำเนินธุรกิจยุคดิจิทัล

การถ่ายทอดและการนำไปใช้ประโยชน์ องค์ความรู้ที่ได้สามารถนำไปประยุกต์ใช้ผ่านการจัดสัมมนา อบรมวิชาชีพ และกิจกรรมให้ความรู้แก่บุคลากรในวิชาชีพบัญชี รวมถึงการเผยแพร่ผ่านบทความวิชาการและสื่อดิจิทัล เพื่อเสริมสร้างความตระหนักรู้และทักษะด้านการรักษาความปลอดภัยของข้อมูล นอกจากนี้ ยังสามารถพัฒนาเป็นแนวทางหรือมาตรฐานการบริหารจัดการความปลอดภัยสารสนเทศสำหรับสำนักงานบัญชีและองค์กรธุรกิจ ช่วยยกระดับความน่าเชื่อถือของระบบสารสนเทศทางบัญชีในระดับสากล และส่งเสริมการพัฒนาเศรษฐกิจดิจิทัลอย่างยั่งยืนในระยะยาว

เอกสารอ้างอิง

Arora, S., Bhardwaj, R., & Kaur, P. (2023). Quantum computing and its implications for cybersecurity in financial systems. *Journal of Financial Innovation and Technology, 5*(1), 44–59.

Arora, S., Singh, R., & Kumar, V. (2023). Quantum computing and its impact on information security: A review. *Journal of Information Security, 18*(2), 85–101.

Brynjolfsson, E., & McAfee, A. (2022). *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*. W. W. Norton & Company.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–548.

Chen, Y., Tan, Z., & Ali, M. (2023). Cybersecurity adoption challenges among SMEs using AIS: A case study approach. *Journal of Small Business and Enterprise Development, 30*(2), 245–263.

Chen, Y., Wang, J., & Li, X. (2022). Cybersecurity risk in accounting information systems: The role of human error and protection mechanisms. *Information Systems Frontiers, 24*(3), 543–560.

Chen, Y., Zhang, L., & Morales, J. (2023). Enhancing cybersecurity in financial information systems: A framework based on ISO/IEC 27001 and COBIT 5. *International Journal of Accounting Information Systems, 51*, 100567.

Chen, Y., Zhang, Z., & Li, M. (2023). Cyber threats to SMEs in the digital era: Challenges and policy recommendations. *Small Business Management Journal, 61*(1), 22–39.

Cheng, H., Zhao, M., & Li, W. (2022). Implementing Zero Trust with Multi-Factor Authentication: A practical approach for enterprise security. *Journal of Cybersecurity Technology, 6*(4), 291–310.

Coates, J. C. (2021). The goals and promise(s) of the Sarbanes-Oxley Act. *Harvard Law Review, 134*(2), 1215–1248.

Coyne, E. M., & McMickle, P. L. (2017). Can blockchains serve an accounting purpose? *Journal of Emerging Technologies in Accounting, 14*(2), 101–111.

Da Veiga, A., & Martins, N. (2015). A framework for analysis of information security culture in organizations. *Computers & Security, 49*, 151–165.

Deloitte. (2022). *The future of cybersecurity in a quantum world.* Deloitte. https://www2.deloitte.com/global/en/pages/risk/articles/quantum-security.html

Deloitte. (2022). *The impact of quantum computing on Cybersecurity*. Deloitte. https://www2.deloitte.com/insights/us/en/industry/technology/quantum-computing-and-cybersecurity.html

Electronic Transactions Development Agency. (2023). *Handbook on compliance with the Personal Data Protection Act (PDPA).* etda. https://www.etda.or.th/th/Useful-Resources/pdpa-handbook.aspx

ENISA. (2023). *Cybersecurity training and awareness: Guidelines and best practices. European Union Agency for Cybersecurity.* ENISA. https://www.enisa.europa.eu/publications

ENISA. (2023*). Guidelines on personal data breach notification under the GDPR. European Union Agency for Cybersecurity*. ENISA. https://www.enisa.europa.eu/publications

European Commission. (2022*). Your rights under the General Data Protection Regulation (GDPR).* European Commission. https://commission.europa.eu/law/law-topic/data-protection/reform/rights-citizens_en

European Data Protection Board. (2023). *Guidelines 01/2023 on fines under the GDPR*. EDPB. https://edpb.europa.eu

Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation. In *Insider Threats in Cyber Security* (pp. 85–113).

IASB. (2021). *IFRS® Standards: Consolidated without early application*. International Accounting Standards Board. IFRS. https://www.ifrs.org

ISACA. (2022). *Role-based training for cybersecurity risk management: A governance perspective.* ISACA. https://www.isaca.org/resources/research

IBM. (2023). *Cost of a Data Breach Report 2023*. IBM Security. https://www.ibm.com/reports/data-breach

Kindervag, J. (2010). *Build security into your network's DNA: The Zero Trust Network Architecture.* Forrester Research.

KnowBe4. (2023). *Phishing simulation and security awareness benchmark report 2023.* KnowBe4. https://www.knowbe4.com/phishing-security-test

Kshetri, N., & Voas, J. (2023). Cybersecurity and privacy challenges in accounting information systems. *IT Professional, 25*(1), 50–56.

Kshetri, N., & Voas, J. (2023). Cybersecurity challenges in the accounting and finance sector: A risk-based approach. *IT Professional, 25*(2), 40–48.

Nguyen, T., & Le, H. (2021). Building a security-aware culture: Human factor in information security management. *Information & Computer Security, 29*(3), 462–477.

Newman, L. H. (2023). *How AI is reshaping cyberattacks*. Wired. https://www.wired.com/story/ai-cyberattacks-2023

Newman, L. H. (2023). *The evolving threat landscape of AI and IoT-integrated accounting systems.* Wired Magazine. https://www.wired.com/story/accounting-systems-ai-iot-security/

Office of the Personal Data Protection Committee. (2023). *Handbook for compliance with the Personal Data Protection Act B.E. 2562 (PDPA). Electronic Transactions Development Agency (ETDA).* ETDA. https://www.etda.or.th/th/Useful-Resources/pdpa-handbook.aspx

Ponemon Institute. (2022). *Cost of a data breach report 2022*. IBM. https://www.ibm.com/reports/data-breach

PwC. (2023). *Data protection compliance: How GDPR and PDPA readiness build trust and long-term competitiveness.* PwC. https://www.pwc.com

Rashid, A., Ahmed, S., & Ali, M. (2023). Cloud accounting and data security: A new era of AIS management. *International Journal of Accounting Information Systems, 48*, 100611.

Rashid, A., Ibrahim, H., & Wong, T. (2023). Emerging technologies in accounting information systems: Opportunities and cybersecurity risks. *International Journal of Accounting Information Systems, 50*, 100563.

Romney, M. B., & Steinbart, P. J. (2021). *Accounting information systems* (15th ed.). Pearson.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture (NIST Special Publication 800-207)*. National Institute of Standards and Technology.

Smith, J., Lee, A., & Kumar, R. (2020). The impact of data breaches on stakeholder trust in accounting systems. *Journal of Information Security and Privacy, 15*(2), 89–105.

Smith, J., & Miller, A. (2023). Data privacy practices in financial information systems: Compliance and enforcement. *Journal of Financial Regulation and Compliance, 31*(1), 33–50.

Tang, Q., & Man, K. L. (2023). Enhancing information security training effectiveness: The role of interactive learning and gamification. *Computers & Security, 124*, 102982.

Tang, Q., Man, K. L., & Li, X. (2022). Cybersecurity risk management in accounting firms: Framework and case study. *International Journal of Accounting Information Systems, 43*, 100512.

Thales Group. (2023). *Data security trends 2023: Threat landscape and best practices*. Thales Group. https://www.thalesgroup.com/en/markets/digital-identity-and-security

Thompson, R., & Garcia, M. (2021). Cybersecurity awareness and the human factor: Empirical evidence from accounting professionals. *Journal of Information Systems, 35*(2), 45–60.

Van Schaik, P., & Flynn, R. (2023). The future of auditing: Integrating blockchain and AI for secure accounting systems. *Auditing: A Journal of Practice & Theory, 42*(1), 109–130.

Wang, J., & Liu, H. (2023). Cybersecurity governance in accounting firms: Challenges and best practices. *Journal of Accounting & Organizational Change, 19*(1), 85–101.

Wheeler, A. (2023). AI and cybersecurity: Protecting financial data in the digital age. *Financial Technology Review, 12*(1), 15–29.

Wong, T., & Rashid, A. (2023). The role of cloud accounting in digital transformation: Benefits and security challenges. *Journal of Accounting and Finance, 78*(3), 210–228.

Zhou, W., & Xu, Y. (2023). Cybersecurity risks and mitigation strategies for blockchain-based accounting systems. *International Journal of Accounting Information Systems, 52*, 100576.