

การศึกษาปัจจัยที่มีอิทธิพลต่อการรักษาความมั่นคงปลอดภัยระบบงานหลักธนาคาร
ของธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร (ธ.ก.ส.)

A study of factors influencing the security of core banking systems.
of Bank for Agriculture and Agricultural Cooperatives (BAAC)

พิชัย แผ่กระโทก¹, อริสรา เสยานนท์²

Phichai Phaekrathok¹, Arisara Seyanont²

บัณฑิตวิทยาลัย กลุ่มวิชาการจัดการ คณะบริหารธุรกิจ มหาวิทยาลัยหอการค้าไทย¹

สาขาวิชาการจัดการโรงแรมและเรือสำราญ คณะการท่องเที่ยวและอุตสาหกรรมบริการ มหาวิทยาลัยหอการค้าไทย²

Graduate School, Management Program, School of Business Administration

University of the Thai Chamber of Commerce¹

Hotel and Cruise Management, School of Tourism and Services

University of the Thai Chamber of Commerce²

Corresponding author, email: phichai.ph@baac.or.th

Retrieved; 19-01-2026; Revised; 27-02-2026. Accepted; 8-08-2026

บทคัดย่อ

บทความนี้มีวัตถุประสงค์เพื่อวิเคราะห์ปัจจัยที่มีอิทธิพลต่อการรักษาความมั่นคงปลอดภัยของระบบงานหลักธนาคาร (Core Banking System: CBS) ของธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร (ธ.ก.ส.) โดยพิจารณาปัจจัย 3 ด้าน ได้แก่ พฤติกรรมการใช้ระบบ การตระหนักถึงความปลอดภัย และการฝึกอบรมและให้ความรู้ การวิจัยเป็นเชิงปริมาณ โดยเก็บข้อมูลจากพนักงาน ธ.ก.ส. จำนวน 400 คน ด้วยการสุ่มแบบสะดวก ใช้แบบสอบถามเป็นเครื่องมือ และวิเคราะห์ข้อมูลด้วยสถิติเชิงพรรณนา (ค่าเฉลี่ย ร้อยละ ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน) และสถิติเชิงอนุมาน (การถดถอยพหุคูณ) ผลการวิจัยพบว่า ปัจจัยทั้งสามมีอิทธิพลเชิงบวกต่อการรักษาความมั่นคงปลอดภัยของระบบ CBS อย่างมีนัยสำคัญทางสถิติ โดยพบว่าโมเดลสามารถอธิบายความแปรปรวนของการรักษาความมั่นคงปลอดภัยของระบบ CBS ได้ร้อยละ 60.3 ($R^2 = 0.603$) โดยปัจจัยการฝึกอบรมและให้ความรู้มีอิทธิพลสูงสุด ($\beta = 0.433$, $p < .001$) รองลงมาคือการตระหนักถึงความปลอดภัย ($\beta = 0.260$, $p < .001$) และพฤติกรรมการใช้ระบบ ($\beta = 0.200$, $p < .001$) ผลการศึกษาเสนอแนะว่า องค์กรควรให้ความสำคัญกับการจัดฝึกอบรมเชิงปฏิบัติที่สามารถนำไปใช้ได้จริง เพื่อสร้างความรู้ ทักษะ และความเชื่อมั่นแก่พนักงาน พร้อมเสริมสร้างทัศนคติและพฤติกรรมที่เหมาะสมในการป้องกันภัยคุกคามทางไซเบอร์ งานวิจัยก่อนหน้านี้นักเน้นเทคโนโลยีมากกว่าพฤติกรรม

บุคลากร โดยเฉพาะในบริบทระบบ CBS ของสถาบันการเงินเฉพาะกิจของรัฐที่ยังมีการศึกษาไม่มาก งานวิจัยนี้จึงบูรณาการ PMT, TPB และ COM-B เพื่ออธิบายพฤติกรรมความมั่นคงปลอดภัยของบุคลากร และขยายองค์ความรู้ด้านการบริหารความมั่นคงปลอดภัยแบบเน้นมนุษย์เป็นศูนย์กลางในภาครัฐไทย

คำสำคัญ: ความตระหนัก; ความปลอดภัย; ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร (ธ.ก.ส.); ความมั่นคง

Abstract

This article aims to analyze the factors influencing the security of the Core Banking System (CBS) of the Bank for Agriculture and Agricultural Cooperatives (BAAC). Three factors were examined: system usage behavior, security awareness, and training and education. The study employed a quantitative approach, collecting data from 400 BAAC employees using convenience sampling. A questionnaire was used as the research instrument, and data were analyzed using descriptive statistics (frequency, percentage, mean, and standard deviation) and inferential statistics (multiple regression analysis). The results revealed that all three factors had a statistically significant positive influence on CBS security. The model explained 60.3% of the variance in CBS security ($R^2 = 0.603$). Training and education had the strongest influence ($\beta = 0.433$, $p < .001$), followed by security awareness ($\beta = 0.260$, $p < .001$) and system usage behavior ($\beta = 0.200$, $p < .001$). The findings suggest that organizations should prioritize practical training programs that can be applied in real work settings to enhance employees' knowledge, skills, and confidence, while also strengthening appropriate attitudes and behaviors for preventing cyber threats. Previous studies have primarily focused on technology rather than employee behavior, particularly in the context of Core Banking Systems (CBS) within state-owned specialized financial institutions, where research remains limited. This study integrates PMT, TPB, and the COM-B model to explain employees' security behavior and to expand the body of knowledge on human-centered cybersecurity management in the Thai public sector

Keywords: Awareness; Security; Bank for Agriculture and Agricultural Cooperatives (BAAC); Stability

บทนำ

ในยุคดิจิทัล สถาบันการเงินมีการพึ่งพาระบบสารสนเทศหลักธนาคาร (Core Banking System: CBS) อย่างเข้มข้น เพื่อสนับสนุนการดำเนินธุรกรรมทางการเงินที่สำคัญ อาทิ การฝาก ถอน โอนเงิน การให้สินเชื่อ และการบริหารจัดการบัญชีลูกค้า ซึ่งระบบดังกล่าวถือเป็นโครงสร้างพื้นฐานที่มีความสำคัญต่อเสถียรภาพและความน่าเชื่อถือขององค์กรทางการเงิน (Whitman & Mattord, 2022) อย่างไรก็ตาม การ

ฟังก์ชันระบบ CBS ที่มีความซับซ้อนและเชื่อมโยงข้อมูลจำนวนมาก ทำให้ความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ทวีความรุนแรงมากขึ้น โดยเฉพาะในภาคการเงินซึ่งเป็นหนึ่งในเป้าหมายหลักของการโจมตีทางไซเบอร์ งานวิจัยและรายงานในช่วงไม่กี่ปีที่ผ่านมาได้ชี้ให้เห็นอย่างชัดเจนว่า ปัจจัยมนุษย์เป็นสาเหตุสำคัญของเหตุการณ์ละเมิดข้อมูล โดยรายงาน Data Breach Investigations Report (DBIR) ของ Verizon (2024) ระบุว่า ร้อยละ 68 ของเหตุการณ์การละเมิดข้อมูลทั่วโลกมีสาเหตุมาจากความผิดพลาดของมนุษย์ ขณะที่ Keepnet Labs (2025) พบว่าปัจจัยมนุษย์มีส่วนเกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยในสัดส่วนสูงถึงร้อยละ 68-95 สะท้อนให้เห็นว่า แม้องค์กรจะมีมาตรการด้านเทคโนโลยีที่ทันสมัยเพียงใด หากขาดการจัดการด้านพฤติกรรมและการตระหนักรู้ของผู้ใช้งาน ยังคงมีความเสี่ยงต่อความมั่นคงของระบบสารสนเทศอย่างมีนัยสำคัญ

ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร (ธ.ก.ส.) เป็นสถาบันการเงินเฉพาะกิจของรัฐที่จัดตั้งขึ้นเพื่อสนับสนุนภาคเกษตรกรรมและเศรษฐกิจฐานรากของประเทศ โดยให้บริการทางการเงินแก่เกษตรกร กลุ่มเกษตรกร และประชาชนในระดับพื้นที่ทั่วประเทศ ภายใต้การกำกับดูแลของธนาคารแห่งประเทศไทยตามหลักการบริหารความเสี่ยง (Risk-Based Supervision) ซึ่งให้ความสำคัญกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยของระบบ (ธนาคารแห่งประเทศไทย, 2566) ด้วยลักษณะขององค์กรที่มีบุคลากรกระจายอยู่ในทุกภูมิภาค และต้องให้บริการผ่านระบบ CBS อย่างต่อเนื่อง ความผิดพลาดของระบบหรือเหตุการณ์ละเมิดความปลอดภัยทางไซเบอร์อาจก่อให้เกิดผลกระทบในวงกว้าง ทั้งต่อการดำเนินงาน ความเชื่อมั่นของลูกค้า และเสถียรภาพของระบบการเงิน งานวิจัยของ IBM Security (2023) ระบุว่า ร้อยละ 23 ของเหตุการณ์ละเมิดข้อมูลในสถาบันการเงินมีสาเหตุมาจากความผิดพลาดของบุคลากรภายใน ซึ่งสอดคล้องกับบริบทของ ธ.ก.ส. ที่ต้องเผชิญความท้าทายในการรักษาสมดุลระหว่างการเข้าถึงบริการทางการเงินของประชาชนในวงกว้างกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แม้ว่างานวิจัยด้านความมั่นคงปลอดภัยไซเบอร์ในสถาบันการเงินจะมีจำนวนมากและให้ความสำคัญกับการพัฒนาเทคโนโลยี มาตรการเชิงเทคนิค และระบบป้องกันภัยคุกคามเป็นหลัก แต่การศึกษาที่มุ่งเน้น “ปัจจัยด้านมนุษย์” โดยเฉพาะในมิติของการฝึกอบรมและให้ความรู้ การตระหนักรู้ด้านความมั่นคงปลอดภัย และพฤติกรรมการใช้ระบบของบุคลากรในระบบงานหลักธนาคาร (Core Banking System: CBS) ของสถาบันการเงินเฉพาะกิจของรัฐ เช่น ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร (ธ.ก.ส.) ยังมีอยู่อย่างจำกัด งานวิจัยส่วนใหญ่มุ่งศึกษาบริบทของธนาคารพาณิชย์หรือองค์กรเอกชน และให้ความสำคัญกับกลไกด้านเทคโนโลยีมากกว่ามิติด้านพฤติกรรมและการพัฒนาศักยภาพบุคลากร ซึ่งเป็นองค์ประกอบสำคัญของความมั่นคงปลอดภัยเชิงองค์กร ดังนั้น งานวิจัยนี้จึงมุ่งเติมเต็มช่องว่างดังกล่าวด้วยการศึกษาพื้นฐานเชิงประจักษ์เกี่ยวกับบทบาทและอิทธิพลของปัจจัยมนุษย์ต่อความมั่นคงปลอดภัยของระบบ CBS ในบริบทของสถาบันการเงินเฉพาะกิจของรัฐ เพื่อขยายองค์ความรู้และ

สนับสนุนการกำหนดแนวทางบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศทางการเงินอย่างรอบด้านและเป็นระบบมากยิ่งขึ้น

ดังนั้น งานวิจัยนี้จึงมีวัตถุประสงค์เพื่อศึกษาปัจจัยที่มีอิทธิพลต่อความปลอดภัยของระบบ Core Banking System ของธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร โดยมุ่งเน้นปัจจัยด้านมนุษย์ ได้แก่ การฝึกอบรมและให้ความรู้ด้านความมั่นคงปลอดภัย การตระหนักรู้ด้านความปลอดภัย และพฤติกรรมการใช้ระบบของบุคลากร งานวิจัยใช้ระเบียบวิธีวิจัยที่เหมาะสมกับบริบทขององค์กรภาครัฐขนาดใหญ่ เพื่อให้ได้ข้อมูลเชิงประจักษ์ที่สะท้อนสถานการณ์จริง ผลการศึกษาที่ได้คาดว่าจะประโยชน์ต่อการพัฒนากลยุทธ์และแนวปฏิบัติด้านความมั่นคงปลอดภัยของระบบ CBS ของ ธ.ก.ส. รวมถึงเป็นแนวทางให้แก่สถาบันการเงินอื่น ๆ ในการเสริมสร้างความมั่นคงปลอดภัยของระบบธนาคารดิจิทัลอย่างยั่งยืน และช่วยเติมเต็มช่องว่างองค์ความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ให้ความสำคัญกับปัจจัยมนุษย์ในเชิงลึก

วัตถุประสงค์การวิจัย

1. เพื่อศึกษาพฤติกรรมผู้ใช้งานระบบงานหลักธนาคาร (CBS) ที่มีต่อการรักษาความปลอดภัยของระบบ CBS
2. เพื่อศึกษาปัจจัยการตระหนักรู้ถึงความปลอดภัยที่มีต่อการรักษาความปลอดภัยของระบบ CBS
3. เพื่อศึกษาปัจจัยการฝึกอบรมและให้ความรู้ที่มีต่อการรักษาความปลอดภัยของระบบ CBS

สมมติฐานการวิจัย

1. ปัจจัยพฤติกรรมการใช้ระบบส่งผลต่อการรักษาความปลอดภัยระบบ CBS ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร
2. ปัจจัยการตระหนักรู้ถึงความปลอดภัยส่งผลต่อการรักษาความปลอดภัยระบบ CBS ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร
3. ปัจจัยการฝึกอบรมและให้ความรู้ส่งผลต่อการรักษาความปลอดภัยระบบ CBS ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร

การทบทวนวรรณกรรม

ในการศึกษาปัจจัยที่มีอิทธิพลต่อการรักษาความมั่นคงปลอดภัยระบบงานหลักธนาคาร (Core Banking System: CBS) ผู้วิจัยได้บูรณาการแนวคิดทฤษฎีพฤติกรรมศาสตร์ร่วมกับการบริหารจัดการเทคโนโลยีสารสนเทศ เพื่ออธิบายกลไกที่ส่งผลต่อประสิทธิภาพในการรักษาความปลอดภัยของบุคลากร ดังนี้

1. กลไกการประเมินภัยคุกคามและการตอบสนองตามทฤษฎี PMT และ SCT

ฐานคิดสำคัญประการแรกคือ ทฤษฎีแรงจูงใจในการป้องกัน (Protection Motivation Theory: PMT) โดย Rogers (1975) ซึ่งอธิบายว่าพนักงานจะเกิดพฤติกรรมการป้องกันก็ต่อเมื่อมีการ “ประเมินภัย

คุกคาม” (Threat Appraisal) ว่ามีความรุนแรงและมีโอกาสเกิดขึ้นจริง หากพนักงานขาดการตระหนักรู้ถึงความปลอดภัย (Security Awareness) จะส่งผลให้การประเมินนี้ต่ำลงและนำไปสู่ความประมาท สอดคล้องกับทฤษฎีการเรียนรู้ทางสังคม (Social Cognitive Theory: SCT) ของ Bandura (1986) ที่เน้นย้ำเรื่อง “ความเชื่อมั่นในความสามารถของตนเอง” (Self-Efficacy) ซึ่งในบริบทนี้คือความมั่นใจของพนักงานว่าตนมีทักษะเพียงพอในการจำแนกภัยคุกคาม เช่น Phishing หรือ Social Engineering ซึ่งทักษะดังกล่าวจำเป็นต้องได้รับการพัฒนาอย่างต่อเนื่องผ่านการฝึกอบรม

2. การปรับเปลี่ยนพฤติกรรมผ่านโมเดล COM-B

เพื่อให้เข้าใจถึงกลไกด้านพฤติกรรม ผู้วิจัยได้ประยุกต์ใช้โมเดล COM-B (Michie et al., 2011) ซึ่งระบุว่าพฤติกรรม (Behavior) จะเกิดขึ้นได้ต้องประกอบด้วย 3 องค์ประกอบ ได้แก่ 1) ชีตความสามารถ (Capability) ด้านความรู้และทักษะ 2) โอกาส (Opportunity) จากสภาพแวดล้อมและนโยบายองค์กร และ 3) แรงจูงใจ (Motivation) ดังนั้น การรักษาความปลอดภัยของระบบ CBS จึงเป็นผลลัพธ์ของทั้งระดับบุคคลและระดับองค์กรรวมกัน

3. บริบทของภัยคุกคามและมาตรฐานสากลในภาคการเงิน

รายงานจาก IBM Security (2023) และ Verizon (2024) ระบุว่าเหตุการณ์ข้อมูลรั่วไหลในสถาบันการเงินกว่า 70-80% มีสาเหตุจากปัจจัยด้านมนุษย์ เช่น รหัสผ่านที่ไม่ปลอดภัยหรือการตกเป็นเหยื่อของวิศวกรรมสังคม สอดคล้องกับมาตรฐาน ISO/IEC 27001 (2022) ที่กำหนดให้การควบคุมด้านบุคลากร (People Controls) และการฝึกอบรมอย่างต่อเนื่องเป็นองค์ประกอบสำคัญของการรักษาความลับและความถูกต้องของข้อมูล

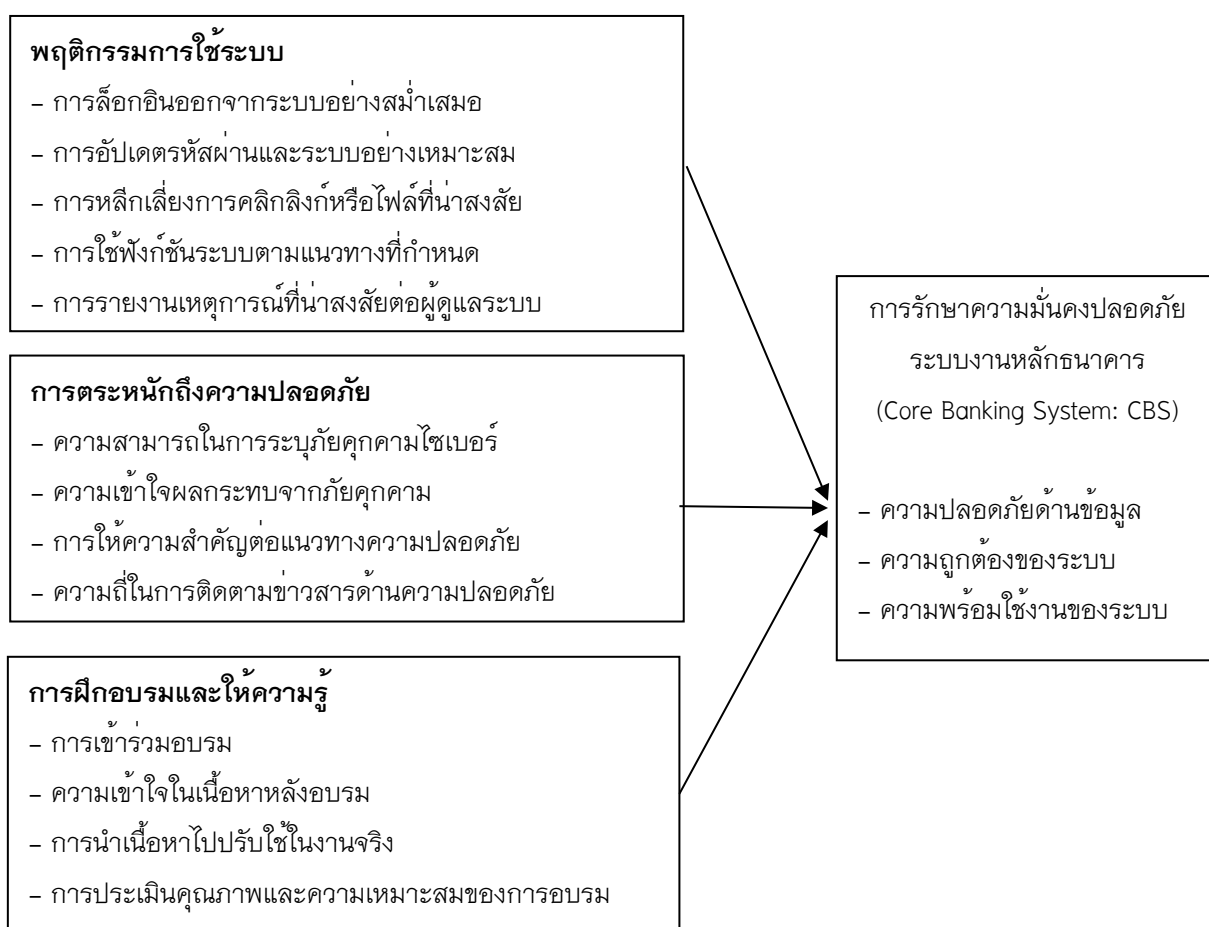
4. การสังเคราะห์และเชื่อมโยงงานวิจัยที่เกี่ยวข้อง

งานวิจัยของ Alsoud และ Al-Okaily (2022) ชี้ว่าเทคโนโลยีป้องกันจะไม่มีประสิทธิภาพหากผู้ใช้ขาดแรงจูงใจ ขณะที่ Angafor และคณะ (2020) พบว่าการฝึกอบรมแบบมีปฏิสัมพันธ์ช่วยยกระดับการนำไปใช้จริงได้ดีกว่าการอบรมแบบเดิม งานวิจัยก่อนหน้าส่วนใหญ่จึงมักศึกษาปัจจัยเหล่านี้แยกส่วน หรือมุ่งเน้นองค์กรเอกชนและธนาคารพาณิชย์เป็นหลัก

งานวิจัยนี้จึงมีบทบาทในการ ยืนยัน ความสำคัญของปัจจัยด้านมนุษย์ตามที่งานก่อนหน้าเสนอไว้ ขยายองค์ความรู้ ด้วยการบูรณาการกรอบแนวคิด PMT, SCT และ COM-B เข้าด้วยกันในโมเดลเดียว และแตกต่างจากงานก่อนหน้า โดยนำมาศึกษาในบริบทระบบ CBS ของสถาบันการเงินเฉพาะกิจของรัฐ ซึ่งยังมีหลักฐานเชิงประจักษ์จำกัด การสังเคราะห์ดังกล่าวช่วยอธิบายความสัมพันธ์เชิงระบบระหว่างพฤติกรรม การตระหนักรู้ และการฝึกอบรม ในฐานะกลไกสำคัญที่เกื้อหนุนกันในการลดความเสี่ยงทางไซเบอร์ของ ธ.ก.ส. อย่างเป็นรูปธรรม.

กรอบแนวคิดการวิจัย

งานวิจัยนี้ เป็นการวิจัยเชิงปริมาณ ผู้วิจัยกำหนดกรอบแนวคิดการวิจัยตามทฤษฎีแรงจูงใจในการป้องกัน (Protection Motivation Theory) การฝึกอบรมช่วยเพิ่มความเชื่อมั่นในความสามารถของบุคลากรในการป้องกันภัยคุกคาม (self-efficacy) และความเชื่อว่ามาตรการป้องกันมีประสิทธิภาพ (response efficacy) กลไกดังกล่าวอธิบายได้ว่าการฝึกอบรมมีผลเชิงบวกต่อความมั่นคงปลอดภัยของระบบ CBS โดยมีรายละเอียดดังนี้



ภาพที่ 1 กรอบแนวคิดการศึกษาค้นคว้าวิจัย

ระเบียบวิธีวิจัย

งานวิจัยนี้เป็นงานวิจัยเชิงปริมาณ มีวัตถุประสงค์เพื่อวิเคราะห์ปัจจัยที่มีอิทธิพลต่อการรักษาความมั่นคงปลอดภัยของระบบงานหลักธนาคาร (Core Banking System: CBS) ของธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร (ธ.ก.ส.) พื้นที่วิจัยครอบคลุมหน่วยงานของธนาคารเพื่อการเกษตรและสหกรณ์

การเกษตรทั่วประเทศ ประชากรที่ใช้ในการวิจัย คือ พนักงานของธนาคารเพื่อการเกษตรและสหกรณ์ การเกษตรในทุกสังกัด ได้แก่ ฝ่ายกิจการสาขาภาคต่าง ๆ และสำนักงานใหญ่ รวมทั้งสิ้นจำนวน 20,343 คน (ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร, 2568)

กลุ่มตัวอย่างที่ใช้ในการวิจัย คือ พนักงานธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร โดยคำนวณขนาดกลุ่มตัวอย่างด้วยสูตรของ Taro Yamane ที่ระดับความเชื่อมั่น 95% ได้ขนาดกลุ่มตัวอย่างที่เหมาะสมเท่ากับ 392.25 คน เพื่อป้องกันความคลาดเคลื่อนจากการตอบแบบสอบถามไม่สมบูรณ์ ผู้วิจัย จึงกำหนดขนาดกลุ่มตัวอย่างและเก็บข้อมูลจริงจำนวน 400 คน ซึ่งเพียงพอต่อการวิเคราะห์ทางสถิติ โดยเฉพาะการวิเคราะห์การถดถอยพหุคูณที่ต้องการขนาดตัวอย่างที่เหมาะสมเพื่อเพิ่มความแม่นยำของค่าประมาณ

ผู้วิจัยเลือกใช้วิธีการคัดเลือกกลุ่มตัวอย่างแบบเจาะจง (Purposive Sampling) โดยกำหนดเกณฑ์ให้เป็นพนักงานที่ปฏิบัติงานเกี่ยวข้องหรือมีการใช้งานระบบ CBS ทั้งในส่วนสาขาและสำนักงานใหญ่ เพื่อให้ได้ข้อมูลจากผู้ที่มีประสบการณ์ตรงกับระบบงานหลักธนาคาร ทั้งนี้ แม้ว่าวิธีดังกล่าวอาจมีข้อจำกัดด้านการอ้างอิงผลไปยังประชากรทั้งหมด (generalizability) เนื่องจากไม่ใช้การสุ่มแบบความน่าจะเป็น แต่การเลือกแบบเจาะจงมีเหตุผลเชิงวิชาการในกรณีที่ผู้วิจัยต้องการข้อมูลจากกลุ่มที่มีคุณลักษณะเฉพาะและเกี่ยวข้องโดยตรงกับตัวแปรที่ศึกษา ซึ่งช่วยเพิ่มความตรงประเด็น (relevance) และคุณภาพของข้อมูลที่ใช้วิเคราะห์

เครื่องมือที่ใช้ในการวิจัย ได้แก่ แบบสอบถาม (Questionnaire) ซึ่งพัฒนาขึ้นตามกรอบแนวคิดและวัตถุประสงค์ของการวิจัย โดยอาศัยการวิเคราะห์และสังเคราะห์แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องกับพฤติกรรมการใช้ระบบ การตระหนักรู้ด้านความมั่นคงปลอดภัย และการฝึกอบรมและให้ความรู้ด้านความมั่นคงปลอดภัย แบบสอบถามแบ่งออกเป็น 5 ส่วน ได้แก่ ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม ส่วนที่ 2 พฤติกรรมการใช้ระบบ ส่วนที่ 3 การตระหนักถึงความปลอดภัย ส่วนที่ 4 การฝึกอบรมและให้ความรู้ และส่วนที่ 5 การรักษาความมั่นคงปลอดภัย โดยข้อคำถามในส่วนที่ 2-4 เชื่อมโยงกับกรอบทฤษฎี PMT และ TPB ส่วนข้อคำถามในส่วนที่ 5 อ้างอิงแนวทางมาตรฐาน ISO/IEC 27001 ลักษณะคำถามเป็นแบบมาตราส่วนประมาณค่า 5 ระดับ ตามแบบ Likert Scale

แบบสอบถามได้รับการตรวจสอบความเที่ยงตรงเชิงเนื้อหา (Content Validity) จากผู้ทรงคุณวุฒิ 3 ท่าน โดยพิจารณาค่า IOC ซึ่งอยู่ระหว่าง 0.67–1.00 แสดงถึงความสอดคล้องของข้อคำถามกับวัตถุประสงค์การวิจัย และทดสอบความเชื่อมั่น (Reliability) ด้วยค่าสัมประสิทธิ์แอลฟาของครอนบัคจากการทดลองใช้กับพนักงาน 30 คน พบว่ามีค่าอยู่ระหว่าง 0.88–0.93 สูงกว่าเกณฑ์ 0.70 แสดงถึงความเชื่อมั่นในระดับสูง

การเก็บรวบรวมข้อมูลดำเนินการผ่านแบบสอบถามออนไลน์ด้วยแพลตฟอร์ม Microsoft Forms พร้อมทั้งศึกษาข้อมูลทุติยภูมิจากเอกสารวิชาการและเอกสารของธนาคาร ข้อมูลเชิงปริมาณที่ได้ถูกวิเคราะห์ด้วยโปรแกรมสำเร็จรูปทางสถิติ โดยใช้สถิติเชิงพรรณนา ได้แก่ ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน

ความถี่ และร้อยละ เพื่ออธิบายลักษณะข้อมูล และใช้สถิติเชิงอนุมาน ได้แก่ การวิเคราะห์การถดถอยพหุคูณ (Multiple Regression Analysis)

เหตุผลเชิงวิชาการในการเลือกใช้ในการถดถอยพหุคูณ เนื่องจากงานวิจัยนี้มีตัวแปรอิสระมากกว่าหนึ่งตัว ได้แก่ พฤติกรรมการใช้ระบบ การตระหนักถึงความปลอดภัย และการฝึกอบรมและให้ความรู้ และต้องการวิเคราะห์อิทธิพลของแต่ละตัวแปรต่อการรักษาความมั่นคงปลอดภัยของระบบ CBS พร้อมกันในโมเดลเดียว การวิเคราะห์การถดถอยพหุคูณจึงเหมาะสมในการประเมินขนาดอิทธิพลสัมพัทธ์ (relative effect) ของแต่ละปัจจัย ควบคุมผลกระทบระหว่างตัวแปร และตรวจสอบความสามารถของโมเดลในการอธิบายความแปรปรวนของตัวแปรตาม (R^2) อย่างเป็นระบบ โดยกำหนดระดับนัยสำคัญทางสถิติที่ 0.05

ผลการวิจัย

ผลการวิเคราะห์ข้อมูลจากกลุ่มตัวอย่างพนักงาน ธ.ก.ส. จำนวน 400 คน พบว่า ข้อมูลลักษณะประชากรศาสตร์ของกลุ่มตัวอย่าง ผู้ตอบแบบสอบถามส่วนใหญ่เป็นเพศหญิง (ร้อยละ 59.8) มีอายุระหว่าง 41–50 ปี (ร้อยละ 35) และมีอายุการทำงานระหว่าง 11–15 ปี (ร้อยละ 33.3) ส่วนใหญ่จบการศึกษาระดับปริญญาตรี (ร้อยละ 66.8) และมีรายได้ต่อเดือนระหว่าง 35,001–55,000 บาท (ร้อยละ 38.5)

วัตถุประสงค์ที่ 1. ผลการวิจัยพบว่า พฤติกรรมการใช้ระบบโดยรวมอยู่ในระดับมากที่สุด แสดงให้เห็นว่าพนักงาน ธ.ก.ส. มีพฤติกรรมการใช้ระบบที่ปลอดภัยอย่างสม่ำเสมอ ดังตารางที่ 1

ตารางที่ 1 ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานของปัจจัยพฤติกรรมการใช้ระบบ

ปัจจัยย่อยด้านพฤติกรรมการใช้ระบบ	ค่าเฉลี่ย (Mean)	ส่วนเบี่ยงเบน มาตรฐาน (S.D.)	ระดับ ความ คิดเห็น
ด้านการล็อกเอาต์ (Log out) ออกจากระบบอย่างสม่ำเสมอ	4.67	0.59	มากที่สุด
ด้านการอัปเดตรหัสผ่านและระบบอย่างเหมาะสม	4.80	0.46	มากที่สุด
ด้านการหลีกเลี่ยงการคลิกลิงก์หรือไฟล์ที่น่าสงสัย	4.86	0.39	มากที่สุด
ด้านการใช้ฟังก์ชันระบบตามแนวทางที่กำหนด	4.86	0.39	มากที่สุด
ด้านการรายงานเหตุการณ์ที่น่าสงสัยต่อผู้ดูแลระบบ	4.81	0.45	มากที่สุด
รวม	4.80	0.40	มากที่สุด

จากตารางที่ 1 พบว่า พฤติกรรมการใช้ระบบโดยรวมอยู่ในระดับมากที่สุด ($\bar{X} = 4.80$, S.D. = 0.40) แสดงให้เห็นว่าพนักงาน ธ.ก.ส. มีพฤติกรรมการใช้ระบบที่ปลอดภัยอย่างสม่ำเสมอ เมื่อพิจารณารายมิติ

พบว่า ด้านการหลีกเลี่ยงการคลิกลิงก์หรือไฟล์ที่น่าสงสัยและด้านการใช้ฟังก์ชันระบบตามแนวทางที่กำหนดมีค่าเฉลี่ยสูงสุด ($\bar{X} = 4.86$) สะท้อนถึงวัฒนธรรมการปฏิบัติตามระเบียบที่เข้มแข็งขององค์กร ในขณะที่มิติด้านการล็อกเอาต์ (Log out) ออกจากระบบอย่างสม่ำเสมอมีค่าเฉลี่ยต่ำที่สุด ($\bar{X} = 4.67$) แม้จะยังอยู่ในระดับมากที่สุดก็ตาม

วัตถุประสงค์ที่ 2. ผลการวิจัยพบว่า การตระหนักถึงความปลอดภัยโดยรวมอยู่ในระดับมากที่สุด แสดงว่าพนักงานมีความตระหนักรู้ถึงความสำคัญของความมั่นคงปลอดภัยในระดับสูง ดังตารางที่ 2

ตารางที่ 2 ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานของปัจจัยการตระหนักถึงความปลอดภัย

ปัจจัยย่อยด้านการตระหนักถึงความปลอดภัย	ค่าเฉลี่ย (Mean)	ส่วนเบี่ยงเบน มาตรฐาน (S.D.)	ระดับ ความ คิดเห็น
ด้านความสามารถในการระบุภัยคุกคามไซเบอร์	4.55	0.68	มากที่สุด
ด้านความเข้าใจผลกระทบจากภัยคุกคาม	4.81	0.44	มากที่สุด
ด้านการให้ความสำคัญต่อแนวทางความปลอดภัย	4.87	0.39	มากที่สุด
ด้านความถี่ในการติดตามข่าวสารด้านความปลอดภัย	4.73	0.51	มากที่สุด
รวม	4.74	0.44	มากที่สุด

จากตารางที่ 2 พบว่า การตระหนักถึงความปลอดภัยโดยรวมอยู่ในระดับมากที่สุด ($\bar{X} = 4.74$, S.D. = 0.44) แสดงว่าพนักงานมีความตระหนักรู้ถึงความสำคัญของความมั่นคงปลอดภัยในระดับสูง เมื่อพิจารณารายมิติ พบว่า ด้านการให้ความสำคัญต่อแนวทางความปลอดภัยมีค่าเฉลี่ยสูงสุด ($\bar{X} = 4.87$) ในขณะที่ด้านความสามารถในการระบุภัยคุกคามไซเบอร์มีค่าเฉลี่ยต่ำที่สุดในกลุ่ม ($\bar{X} = 4.55$) แม้จะยังอยู่ในระดับมากที่สุดก็ตาม

วัตถุประสงค์ที่ 3. ผลการวิจัยพบว่า การฝึกอบรมและให้ความรู้โดยรวมอยู่ในระดับมากที่สุด ($\bar{X} = 4.45$, S.D. = 0.77) แสดงว่าพนักงานมีความพึงพอใจและเห็นประโยชน์ของการฝึกอบรมที่ธนาคารจัดให้ ส่วนการรักษาความมั่นคงปลอดภัยของระบบ CBS ตามการรับรู้ของผู้ใช้งานโดยรวม พบว่าอยู่ในระดับมากที่สุด แสดงว่าพนักงานมีความเชื่อมั่นต่อความปลอดภัยของระบบ CBS ในระดับสูง ดังตารางที่ 3 และ 4

ตารางที่ 3 ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานของปัจจัยการฝึกอบรมและให้ความรู้

ปัจจัยย่อยด้านการฝึกอบรมและให้ความรู้	ค่าเฉลี่ย (Mean)	ส่วนเบี่ยงเบน มาตรฐาน (S.D.)	ระดับ ความ คิดเห็น
ด้านการเข้าร่วมอบรม	4.30	0.89	มากที่สุด
ด้านความเข้าใจในเนื้อหาหลังอบรม	4.50	0.79	มาก
ด้านการนำเนื้อหาไปปรับใช้ในงานจริง	4.55	0.77	มาก
ด้านการประเมินคุณภาพและความเหมาะสมของการอบรม	4.46	0.84	มาก
รวม	4.45	0.77	มากที่สุด

จากตารางที่ 3 พบว่า การฝึกอบรมและให้ความรู้โดยรวมอยู่ในระดับมากที่สุด ($\bar{X} = 4.45$, S.D. = 0.77) แสดงว่าพนักงานมีความพึงพอใจและเห็นประโยชน์ของการฝึกอบรมที่ธนาคารจัดให้ เมื่อพิจารณารายพบว่า ด้านการนำเนื้อหาไปปรับใช้ในงานจริงมีค่าเฉลี่ยสูงสุด ($\bar{X} = 4.55$) ในขณะที่ด้านการเข้าร่วมอบรมมีค่าเฉลี่ยต่ำที่สุด ($\bar{X} = 4.30$)

ตารางที่ 4 ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานของการรักษาความมั่นคงปลอดภัยของระบบ CBS

ปัจจัยย่อยด้านการรักษาความมั่นคงปลอดภัย	ค่าเฉลี่ย (Mean)	ส่วนเบี่ยงเบน มาตรฐาน (S.D.)	ระดับ ความ คิดเห็น
ด้านความปลอดภัยของข้อมูล (Confidentiality)	4.73	0.56	มากที่สุด
ด้านความถูกต้องของระบบ (Integrity)	4.69	0.57	มากที่สุด
ด้านความพร้อมใช้งานของระบบ (Availability)	4.55	0.72	มากที่สุด
รวม	4.66	0.57	มากที่สุด

จากตารางที่ 4 พบว่า การรักษาความมั่นคงปลอดภัยของระบบ CBS ตามการรับรู้ของผู้ใช้งานโดยรวม พบว่าอยู่ในระดับมากที่สุด ($\bar{X} = 4.66$, S.D. = 0.57) แสดงว่าพนักงานมีความเชื่อมั่นต่อความปลอดภัย

ของระบบ CBS ในระดับสูง เมื่อพิจารณาราย พบว่าด้านความปลอดภัยของข้อมูล (Confidentiality) มีค่าเฉลี่ยสูงสุด ($\bar{X} = 4.73$)

ผลการศึกษาสถิติเชิงอนุมาน

การวิเคราะห์ข้อมูลเพื่อทดสอบสมมติฐานการวิจัยที่ตั้งไว้ โดยใช้การวิเคราะห์การถดถอยเชิงพหุคูณ (Multiple Regression Analysis) เพื่อศึกษาอิทธิพลของปัจจัยพฤติกรรมการใช้ระบบ ปัจจัยการตระหนักถึงความปลอดภัย และปัจจัยการฝึกอบรมและให้ความรู้ ที่มีต่อการรักษาความมั่นคงปลอดภัยของระบบ CBS สรุปรายละเอียด ดังตารางที่ 5

ตารางที่ 5 ผลการวิเคราะห์สรุปโมเดลถดถอยเชิงพหุคูณ (Model Summary)

Model	R	R ²	Adjusted R ²	Std. Error of the Estimate	Durbin-Watson
1	0.777	0.603	0.600	0.3573	1.900

จากตารางที่ 5 ค่า $R = 0.777$ แสดงถึงความสัมพันธ์รวมในระดับสูง ค่า $R^2 = 0.603$ หมายความว่าตัวแปรอิสระทั้งสามสามารถอธิบายความแปรปรวนของการรักษาความมั่นคงปลอดภัยของระบบ CBS ได้ร้อยละ 60.3 ค่า Adjusted $R^2 = 0.600$ ปรับค่าความแม่นยำให้เหมาะสมกับจำนวนตัวแปร ค่า Durbin-Watson = 1.900 ใกล้ 2 แสดงว่าไม่มีปัญหา Autocorrelation

ตารางที่ 6 ผลการวิเคราะห์ความมีนัยสำคัญของโมเดลถดถอย (ANOVA)

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	76.945	3	25.648	200.856	.000**
Residual	50.568	396	0.128		
Total	127.513	399			

จากตารางที่ 6 ค่า $F = 200.856$, Sig. = .000 < 0.05 แสดงว่าโมเดลโดยรวมมีนัยสำคัญทางสถิติ

ตารางที่ 7 ค่าสัมประสิทธิ์การถดถอยเชิงพหุคูณ (Coefficients)

ตัวแปรอิสระ	B	Std. Error	Beta	t	p_value	VIF
(Constant)	0.299	0.220	–	1.358	0.175	–
พฤติกรรมการใช้ระบบ	0.283	0.073	0.200	3.864	.000**	2.681
การตระหนักถึงความปลอดภัย	0.336	0.076	0.260	4.431	.000**	3.434
การฝึกอบรมและให้ความรู้	0.316	0.030	0.433	10.590	.000**	1.670
R = .777 ^a R ² = 0.603 Adjusted R ² = 0.600						

** p ≤ .001

จากตารางที่ 7 R² = 0.603 หรือกล่าวได้ว่าปัจจัยทั้งสามร่วมกันสามารถอธิบายความแปรปรวนในการรักษาความปลอดภัยของระบบ CBS ได้ถึงประมาณร้อยละ 60. โดยการฝึกอบรมและให้ความรู้ มีค่า Beta สูงสุด (0.433) แสดงว่ามีอิทธิพลมากที่สุด รองลงมาคือ การตระหนักถึงความปลอดภัย (0.260) และพฤติกรรมการใช้ระบบ (0.200) ตามลำดับ Sig. ของทุกตัวแปร < 0.05 จึงมีนัยสำคัญทางสถิติ ค่า VIF < 10 แสดงว่าไม่มีปัญหา Multicollinearity

สรุปได้ว่า ปัจจัยด้านมนุษย์ทั้งสามสามารถอธิบายความมั่นคงปลอดภัยของระบบ CBS ได้อย่างมีนัยสำคัญ โดยเฉพาะการฝึกอบรมซึ่งเป็นกลไกหลักในการเสริมสร้างทักษะและความมั่นใจของพนักงาน ผลลัพธ์นี้ชี้ให้เห็นว่าแนวทางบริหารความปลอดภัยที่เน้นเทคโนโลยีเพียงอย่างเดียวอาจไม่เพียงพอ หากไม่พัฒนาองค์ประกอบด้านมนุษย์ควบคู่กัน

ผลการทดสอบสมมติฐาน

สมมติฐานที่ 1 (H₁) ปัจจัยพฤติกรรมการใช้ระบบส่งผลต่อการรักษาความปลอดภัยระบบ CBS ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร ผลการทดสอบปัจจัยพฤติกรรมการใช้ระบบมีอิทธิพลเชิงบวกต่อการรักษาความมั่นคงปลอดภัยของระบบ CBS อย่างมีนัยสำคัญทางสถิติ โดยมีค่าสัมประสิทธิ์มาตรฐาน (Beta) เท่ากับ 0.200 ซึ่งหมายความว่า หากพนักงานมีพฤติกรรมการใช้ระบบที่เหมาะสมและปลอดภัยมากขึ้น จะส่งผลให้ระดับการรักษาความมั่นคงปลอดภัยของระบบ CBS สูงขึ้นตามไปด้วย และจากตารางที่ 4.9 พบว่าปัจจัยพฤติกรรมการใช้ระบบมีค่า p-value (Sig.) เท่ากับ .000 ซึ่งน้อยกว่าระดับนัยสำคัญทางสถิติที่ 0.05 ดังนั้นจึง ยอมรับสมมติฐานที่ 1

สมมติฐานที่ 2 (H₂) ปัจจัยการตระหนักถึงความปลอดภัยส่งผลต่อการรักษาความปลอดภัยระบบ CBS ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร ผลการทดสอบปัจจัยการตระหนักถึงความปลอดภัยมีอิทธิพลเชิงบวกต่อการรักษาความมั่นคงปลอดภัยของระบบ CBS อย่างมีนัยสำคัญทางสถิติ โดยมีค่าสัมประสิทธิ์มาตรฐาน (Beta) เท่ากับ 0.260 ซึ่งหมายความว่า เมื่อพนักงานมีการตระหนักรู้ถึงภัยคุกคาม

และให้ความสำคัญกับแนวทางความปลอดภัยมากขึ้น จะส่งผลให้ระดับการรักษาความมั่นคงปลอดภัยของระบบ CBS สูงขึ้น และจากตารางที่ 4.9 พบว่าปัจจัยการตระหนักถึงความปลอดภัยมีค่า p -value (Sig.) เท่ากับ .000 ซึ่งน้อยกว่าระดับนัยสำคัญทางสถิติที่ 0.05 ดังนั้นจึง ยอมรับสมมติฐานที่ 2

สมมติฐานที่ 3 (H_3) ปัจจัยการฝึกอบรมและให้ความรู้ส่งผลต่อการรักษาความมั่นคงปลอดภัยระบบ CBS ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร ผลการทดสอบปัจจัยการฝึกอบรมและให้ความรู้มีอิทธิพลเชิงบวกต่อการรักษาความมั่นคงปลอดภัยของระบบ CBS อย่างมีนัยสำคัญทางสถิติ โดยมีค่าสัมประสิทธิ์มาตรฐาน (Beta) เท่ากับ 0.433 ซึ่งเป็นค่าที่สูงที่สุดในบรรดาตัวแปรอิสระทั้งสามตัว แสดงให้เห็นว่าการฝึกอบรมเป็นปัจจัยที่มีอิทธิพลมากที่สุด กล่าวคือ การที่พนักงานได้รับความรู้ความเข้าใจและสามารถนำทักษะจากการฝึกอบรมไปปรับใช้ได้จริง จะส่งผลให้ระดับการรักษาความมั่นคงปลอดภัยของระบบ CBS เพิ่มขึ้นอย่างชัดเจน และจากตารางที่ 4.9 พบว่าปัจจัยการฝึกอบรมและให้ความรู้มีค่า p -value (Sig.) เท่ากับ .000 ซึ่งน้อยกว่าระดับนัยสำคัญทางสถิติที่ 0.05 ดังนั้นจึง ยอมรับสมมติฐานที่ 3

อภิปรายผลการวิจัย

ผลการวิจัยโดยภาพรวมไม่เพียงยืนยันบทบาทของ “ปัจจัยด้านมนุษย์” ต่อการรักษาความมั่นคงปลอดภัยของระบบงานหลักธนาคาร (CBS) เท่านั้น แต่ยังช่วยยกระดับความเข้าใจเชิงทฤษฎีเกี่ยวกับ Human Factor ในบริบทของระบบสารสนเทศทางการเงินที่มีความสำคัญเชิงโครงสร้างระดับองค์กร โดยเฉพาะในสถาบันการเงินเฉพาะกิจของรัฐ ผลลัพธ์ที่พบว่าปัจจัยด้านการฝึกอบรมและให้ความรู้มีอิทธิพลสูงสุด รองลงมาคือการตระหนักถึงความปลอดภัย และพฤติกรรมการใช้ระบบ สะท้อนให้เห็นว่า “ความมั่นคงปลอดภัย” ในระบบ CBS มิใช่เพียงผลรวมของพฤติกรรมรายบุคคล แต่เป็นผลลัพธ์ของกลไกเชิงระบบที่เชื่อมโยงการเรียนรู้ แรงจูงใจ และสภาพแวดล้อมองค์กรเข้าด้วยกัน

ในมิติของทฤษฎี ผลการวิจัยขยายกรอบแนวคิดของ Protection Motivation Theory (PMT) จากเดิมที่มุ่งอธิบายแรงจูงใจในการป้องกันภัยในระดับบุคคล ไปสู่การอธิบายในระดับ “ระบบองค์กร” กล่าวคือการประเมินภัยคุกคาม (Threat Appraisal) และการประเมินการรับมือ (Coping Appraisal) มิได้เกิดขึ้นอย่างโดดเดี่ยวภายในตัวบุคคล แต่ถูกกำหนดและหล่อหลอมผ่านโครงสร้างการฝึกอบรม นโยบาย และวัฒนธรรมองค์กรที่เป็นระบบสนับสนุน เมื่อการฝึกอบรมสามารถเพิ่ม Self-Efficacy และ Response Efficacy ได้อย่างมีนัยสำคัญ จึงส่งผลโดยตรงต่อความมั่นคงปลอดภัยของระบบ CBS ทั้งระบบ ไม่ใช่เพียงพฤติกรรมเฉพาะบุคคลรายใดรายหนึ่ง

ผลจากวัตถุประสงค์ที่ 1 ที่พบว่าพฤติกรรมการใช้ระบบมีอิทธิพลต่ำที่สุด ($\beta = .200$) ชี้ให้เห็นประเด็นเชิงทฤษฎีที่สำคัญว่า พฤติกรรมเป็น “ปลายทาง” ของกระบวนการทางจิตวิทยาและโครงสร้างองค์กร มากกว่าจะเป็นตัวแปรต้นตั้งต้นโดยลำพัง สอดคล้องกับ Theory of Planned Behavior (TPB) ที่อธิบายว่าพฤติกรรมเป็นผลของความตั้งใจซึ่งได้รับอิทธิพลจากทัศนคติและบรรทัดฐานทางสังคม อย่างไรก็ตาม งานวิจัยนี้ขยายความเข้าใจเพิ่มเติมว่า ในบริบท CBS ซึ่งเป็นระบบที่มีความเสี่ยงสูง พฤติกรรมพื้นฐาน เช่น

การล็อกเอาต์ อาจถูกกำหนดโดย “การออกแบบระบบ” และ “กลไกกำกับขององค์กร” ควบคู่กับแรงจูงใจส่วนบุคคล จึงสะท้อนความจำเป็นของการผสานแนวคิดด้าน Behavioral Design เข้ากับการบริหารความมั่นคงปลอดภัย

ในส่วนของวัตถุประสงค์ที่ 2 แม้ว่าการตระหนักถึงความปลอดภัย ($\beta = .260$) จะมีบทบาทสำคัญในฐานะตัวจุดชนวนทางความคิดตามกรอบ PMT แต่ผลเชิงพรรณนาที่พบช่องว่างระหว่างระดับการให้ความสำคัญกับแนวทางความปลอดภัยที่สูง กับความสามารถในการระบุภัยคุกคามที่ต่ำกว่า สะท้อนข้อค้นพบเชิงทฤษฎีที่สำคัญว่า “การรับรู้ภัยคุกคาม” เพียงอย่างเดียวไม่เพียงพอในการสร้างพฤติกรรมป้องกันที่มีประสิทธิภาพ หากไม่มีกลไกเสริมด้านทักษะและการฝึกปฏิบัติจริง ผลลัพธ์นี้จึงช่วยขยาย PMT โดยชี้ให้เห็นความจำเป็นของการบูรณาการ Threat Appraisal เข้ากับการพัฒนาศักยภาพเชิงปฏิบัติในระดับองค์กร

ผลจากวัตถุประสงค์ที่ 3 ที่พบว่า การฝึกอบรมและให้ความรู้มีอิทธิพลสูงสุด ($\beta = .433$) มีนัยเชิงทฤษฎีอย่างชัดเจนว่า Coping Appraisal โดยเฉพาะ Self-Efficacy เป็นกลไกขับเคลื่อนสำคัญในบริบทระบบการเงินที่ซับซ้อน งานวิจัยนี้จึงช่วยยืนยันและขยายแนวคิดของ PMT ว่า การเพิ่มความสามารถเชิงปฏิบัติและความเชื่อมั่นในระดับบุคลากร สามารถส่งผลเชิงโครงสร้างต่อความมั่นคงปลอดภัยของระบบ CBS โดยรวม นอกจากนี้ยังสอดคล้องกับแนวคิด COM-B ที่ระบุว่าพฤติกรรมจะเกิดขึ้นได้เมื่อมี Capability ควบคู่กับ Opportunity และ Motivation ซึ่งในบริบทนี้ “การฝึกอบรมเชิงปฏิบัติ” ทำหน้าที่เป็นกลไกเชื่อมโยงทั้งสามองค์ประกอบเข้าด้วยกัน

โดยสรุป งานวิจัยนี้มีคุณูปการเชิงทฤษฎีในการยกระดับความเข้าใจเรื่อง Human Factor ในระบบ CBS จากมุมมองที่เน้นพฤติกรรมรายบุคคล ไปสู่กรอบการวิเคราะห์เชิงระบบที่บูรณาการ PMT, TPB และ COM-B เข้าด้วยกัน ผลการศึกษาชี้ชัดว่า ความมั่นคงปลอดภัยของระบบงานหลักธนาคารเป็นผลลัพธ์ของโครงสร้างการเรียนรู้ แรงจูงใจ และการออกแบบเชิงองค์กรที่สนับสนุนพฤติกรรมที่ปลอดภัยอย่างต่อเนื่อง จึงเป็นการขยายกรอบแนวคิดด้านความมั่นคงปลอดภัยไซเบอร์จาก “เทคโนโลยีเป็นศูนย์กลาง” ไปสู่ “มนุษย์และระบบองค์กรเป็นศูนย์กลาง” อย่างเป็นรูปธรรม

ข้อเสนอแนะ

จากผลการวิจัย ผู้วิจัยมีข้อเสนอแนะ ดังนี้

1. ข้อเสนอแนะในการนำผลการวิจัยไปใช้ประโยชน์

ด้านพฤติกรรมการใช้ระบบ ซึ่งสะท้อนผลลัพธ์ของการฝึกอบรมและการตระหนักรู้ ธ.ก.ส. ควรใช้มาตรการทางเทคนิคควบคู่กับการรณรงค์ เช่น การตั้งค่าล็อกหน้าจออัตโนมัติเมื่อไม่มีการใช้งาน และการสื่อสารเตือนพนักงานอย่างสม่ำเสมอ พร้อมทั้งส่งเสริมให้ผู้บริหารเป็นแบบอย่างที่ดี เพื่อให้พฤติกรรมด้านความปลอดภัยกลายเป็นส่วนหนึ่งของวัฒนธรรมองค์กร

ด้านการตระหนักถึงความปลอดภัย แม้พนักงานจะมีทัศนคติเชิงบวกต่อความสำคัญของความปลอดภัยในระดับสูง แต่ยังคงขาดทักษะเชิงปฏิบัติ ธ.ก.ส. จึงควรส่งเสริมการสื่อสารด้านความปลอดภัยอย่างต่อเนื่องผ่านสื่อภายในองค์กร และสร้างช่องทางการรายงานเหตุการณ์ที่เข้าถึงง่ายและไม่ก่อให้เกิดความกังวลต่อการถูกตำหนิ เพื่อปลูกฝังวัฒนธรรมความปลอดภัยที่เข้มแข็งและยั่งยืน

ด้านการฝึกอบรมและให้ความรู้ ซึ่งเป็นปัจจัยที่มีอิทธิพลสูงที่สุด ธ.ก.ส. ควรพัฒนาการฝึกอบรมจากรูปแบบเชิงทฤษฎีไปสู่การฝึกอบรมเชิงปฏิบัติที่เน้นการจำลองสถานการณ์จริง เช่น การทดสอบอีเมลหลอกลวง เพื่อเสริมสร้างทักษะในการระบุและรับมือกับภัยคุกคามไซเบอร์ รวมถึงควรจัดทำหลักสูตรฝึกอบรมเฉพาะทางให้เหมาะสมกับบทบาทหน้าที่และระดับความเสี่ยงของพนักงานแต่ละกลุ่ม เพื่อเพิ่มประสิทธิภาพของการเรียนรู้และการนำไปใช้จริง

2. ข้อเสนอแนะในการทำวิจัยครั้งต่อไป

การวิจัยในอนาคตควรบูรณาการกรอบแนวคิดทางทฤษฎีเพิ่มเติมนอกเหนือจากทฤษฎีแรงจูงใจในการป้องกัน (PMT) และทฤษฎีพฤติกรรมตามแผน (TPB) เพื่อให้เกิดความเข้าใจพฤติกรรมด้านความมั่นคงปลอดภัยของระบบสารสนเทศในมิติที่ลึกซึ้งและครอบคลุมมากยิ่งขึ้น โดยเฉพาะการศึกษาบทบาทของบรรทัดฐานกลุ่มอ้างอิง (Subjective Norms) เพื่ออธิบายอิทธิพลของแรงกดดันทางสังคมจากเพื่อนร่วมงานและผู้บังคับบัญชาต่อความตั้งใจในการปฏิบัติตามนโยบายความปลอดภัย

นอกจากนี้ ควรนำทฤษฎีการข่มขู่ยับยั้ง (General Deterrence Theory: GDT) มาประยุกต์ใช้เพื่อศึกษาผลของการรับรู้ถึงบทลงโทษต่อการยับยั้งพฤติกรรมที่ไม่ปลอดภัยของพนักงาน ควบคู่กับการพัฒนาเครื่องมือวัดวัฒนธรรมความปลอดภัยในระดับองค์กร แทนการวัดเพียงการตระหนักรู้ในระดับบุคคล ซึ่งจะช่วยให้สามารถอธิบายและกำหนดกลยุทธ์ด้านความมั่นคงปลอดภัยขององค์กรได้อย่างเป็นระบบและมีประสิทธิภาพยิ่งขึ้น

เอกสารอ้างอิง

- กิตติศักดิ์ จันทรนิเวศน์. (2565). ปัจจัยที่ส่งผลต่อความตั้งใจในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรในบริษัทกลุ่ม Oil and Gas. [วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ]. มหาวิทยาลัยธรรมศาสตร์.
- ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร. (2568). รายงานประจำปี 2567 ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร. เข้าถึงได้จาก <https://www.baac.or.th>
- ธนาคารแห่งประเทศไทย. (2566). การกำกับดูแลสถาบันการเงินเฉพาะกิจ. สืบค้นจาก <https://www.bot.or.th/th/supervision/financial-institutions/sfi.html>
- นริส อุไรพันธ์. (2565). ปัจจัยที่ส่งผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ของธุรกิจพาณิชย์อิเล็กทรอนิกส์สำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทย. [วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ]. มหาวิทยาลัยศรีปทุม.

- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211.
- Alsaad, A., & Al-Okaily, M. (2022). Acceptance of protection technology in a time of fear: the case of Covid-19 exposure detection apps. *Information Technology & People*, 35(3), 1116–1142.
- Angafor, G. N., Yevseyeva, I., & He, Y. (2020). Game-based information security/privacy education and training: A systematic literature mapping. *Security and Privacy*, 3(6), e126.
- Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Englewood Cliffs: Prentice-Hall.
- Cronbach, L. J. (1970). *Essentials of psychological testing* (3rd ed.). New York, NY: Harper & Row.
- IBM Security. (2023). *IBM Security X-Force Threat Intelligence Index 2023*. New York: IBM Corporation.
- ISO/IEC 27001. (2022). *Information security management systems — Requirements*. Geneva: International Organization for Standardization.
- Keepnet Labs. (2025). *Top phishing statistics and trends you must know*. Retrieved from <https://keepnetlabs.com/blog/top-phishing-statistics-and-trends-you-must-know>
- Michie, S., van Stralen, M. M., & West, R. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Science*, 6(42), 1–11.
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114.
- Verizon. (2024). *2024 Data Breach Investigations Report*. Retrieved from <https://www.verizon.com/business/resources/T646/reports/2024-dbir-data-breach-investigations-report.pdf>
- Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th ed.). Boston: Cengage Learning.