ปัจจัยที่ส่งผลต่อการตระหนักและการใช้เทคโนโลยีความมั่นคงปลอดภัยทางไซเบอร์ตามประกาศคณะกรรมการการรักษาความปลอดภัยไซเบอร์แห่งชาติ: กรณีศึกษาโครงการเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา (Inter University Network)

Factors Affecting the Awareness and Adoption of Cybersecurity Technology according to the Announcement of the National Cyber Security Agency: A Case Study of the Inter University Network

นายณัฐกร ชาคโรทัย[1], รองศาสตราจารย์ ดร.ชัยวัฒน์ อุตตมากร[*]

นักศึกษา หลักสูตรปริญญาโทการบริหารนวัตกรรมและเทคโนโลยี มหาวิทยาลัยธรรมศาสตร์[1]

รองศาสตราจารย์ประจำหลักสูตรปริญญาโทการบริหารนวัตกรรมและเทคโนโลยี มหาวิทยาลัยธรรมศาสตร์[*]

Corresponding author's E-mail: ntkckrt@gmail.com

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาปัจจัยที่ส่งผลต่อการตระหนักและการใช้เทคโนโลยีความมั่นคงปลอดภัยทางไซเบอร์ในบริบทของโครงการเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา การวิจัยเป็นแบบเชิงปริมาณ โดยประชากรคือบุคลากรที่เกี่ยวข้องกับโครงการจำนวน 434 คน กำหนดขนาดกลุ่มตัวอย่างตามสูตรของ Yamane ได้จำนวน 208 คน เก็บรวบรวมข้อมูลด้วยแบบสอบถาม และมีข้อมูลที่ใช้ในการวิเคราะห์จำนวน 327 ชุด วิเคราะห์ข้อมูลด้วยสถิติเชิงพรรณนา การวิเคราะห์องค์ประกอบเชิงสำรวจ และแบบจำลองสมการโครงสร้าง

ผลการวิจัยพบว่า โมเดลมีความสอดคล้องกับข้อมูลเชิงประจักษ์ในระดับดี และปัจจัยด้านทัศนคติเป็นปัจจัยเดียวที่มีอิทธิพลอย่างมีนัยสำคัญต่อการตระหนักและการใช้เทคโนโลยีความมั่นคงปลอดภัยทางไซเบอร์ (β = 0.482, $p < .01$) โดยสามารถอธิบายความแปรปรวนของตัวแปรตามได้ร้อยละ 25 ซึ่งถือเป็นระดับที่ยอมรับได้ในงานวิจัยด้านพฤติกรรมองค์การและการยอมรับเทคโนโลยี

ข้อค้นพบชี้ให้เห็นว่าการพัฒนาทัศนคติของบุคลากรเป็นกลไกสำคัญในการส่งเสริมการตระหนักและการใช้เทคโนโลยีความมั่นคงปลอดภัยทางไซเบอร์ในองค์กร และสามารถนำไปใช้เป็นแนวทางในการพัฒนานโยบายหรือมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ในหน่วยงานที่เกี่ยวข้อง

คำสำคัญ: ความตระหนัก ความมั่นคงปลอดภัยทางไซเบอร์ การใช้เทคโนโลยี

Abstract

This study aims to examine the factors affecting cybersecurity awareness and technology adoption in the context of the Inter University Network (UniNet). A quantitative research design was employed. The population consisted of 434 personnel involved in the project. The sample size was determined using Yamane's formula, yielding a minimum sample of 208 participants. Data were collected through questionnaires, and 327 valid responses were used for analysis. The data were analyzed using descriptive statistics, Exploratory Factor Analysis (EFA), and Structural Equation Modeling (SEM).

The results indicated that the proposed model demonstrated a good fit with the empirical data. Attitude was the only factor that had a statistically significant effect on cybersecurity awareness and technology adoption (β = 0.482, $p < .01$). The model explained 25% of the variance in the dependent variable, which may be considered an acceptable level in behavioral and technology adoption research contexts, while the other factors showed no statistically significant effects.

The findings suggest that improving personnel attitudes is a key mechanism for enhancing cybersecurity awareness and technology adoption in organizations. These findings may also be used to support the development of policies and cybersecurity management measures in relevant organizations.

Keywords: Awareness, Cybersecurity, Technology Adoption

บทนำ

ปัจจุบันภัยคุกคามทางไซเบอร์มีแนวโน้มเพิ่มขึ้นทั้งในด้านความถี่และความซับซ้อน ส่งผลกระทบต่อระบบสารสนเทศ เศรษฐกิจ และการให้บริการสาธารณะของหลายประเทศทั่วโลก โดยเฉพาะหน่วยงานที่จัดอยู่ในกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ซึ่งมีบทบาทสำคัญต่อการดำเนินชีวิตของประชาชนและความมั่นคงของประเทศ ประเทศไทยได้กำหนดกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ผ่านพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 [1] และประกาศของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ [2] ซึ่งกำหนดให้หน่วยงานของรัฐที่มีความพร้อมหรือหน่วยงานกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (Computer Emergency Response Team: CERT) เพื่อเฝ้าระวัง ตรวจจับ และรับมือกับภัยคุกคามทางไซเบอร์อย่างเป็นระบบ

โครงการเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา (Inter University Network) [3] เป็นโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่สำคัญของประเทศ ซึ่งทำหน้าที่เชื่อมโยงเครือข่ายข้อมูลและการสื่อสารระหว่างสถาบันอุดมศึกษา เพื่อสนับสนุนการเรียนการสอน การวิจัย และการแลกเปลี่ยนข้อมูลทางวิชาการทั้งในประเทศและต่างประเทศ ภายใต้การกำกับดูแลของสำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม ด้วยบทบาทดังกล่าว ระบบเครือข่าย UniNet จึงมีความสำคัญต่อการพัฒนาการศึกษาและการวิจัยของประเทศ และจำเป็นต้องมีมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ

เพื่อให้สอดคล้องกับนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ ได้มีการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา (Education Computer Emergency Response Team: Education CERT) เพื่อทำหน้าที่เฝ้าระวัง วิเคราะห์และประสานการรับมือกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงานในเครือข่าย อย่างไรก็ตาม การพัฒนาศักยภาพของหน่วยงานในการรับมือภัยคุกคามทางไซเบอร์จำเป็นต้องอาศัยทั้งเทคโนโลยี กระบวนการ และบุคลากรที่มีความตระหนักและมีทัศนคติที่เหมาะสมต่อการใช้เทคโนโลยีความมั่นคงปลอดภัยไซเบอร์

ดังนั้น การศึกษาปัจจัยที่ส่งผลต่อการตระหนักและการใช้เทคโนโลยีความมั่นคงปลอดภัยทางไซเบอร์ในบริบทของโครงการเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา จึงมีความสำคัญต่อการยกระดับการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของภาคการศึกษา งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาปัจจัยที่ส่งผลต่อการตระหนักและการใช้เทคโนโลยีความมั่นคงปลอดภัยไซเบอร์ตามแนวทางของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยใช้กลุ่มตัวอย่างเป็นบุคลากรที่เกี่ยวข้องกับการดำเนินงานในโครงการเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา และเพื่อเสนอแนะแนวทางในการพัฒนาการเฝ้าระวังและรับมือภัยคุกคามทางไซเบอร์สำหรับหน่วยงานที่เกี่ยวข้อง

ผลการศึกษาคาดว่าจะช่วยให้หน่วยงานที่เกี่ยวข้องสามารถนำข้อมูลไปใช้ในการวางแผนและพัฒนาการใช้เทคโนโลยีความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ ตลอดจนสนับสนุนการยกระดับความพร้อมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านการศึกษาในระยะยาว

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงปริมาณ (Quantitative Research) มีวัตถุประสงค์เพื่อศึกษาปัจจัยที่ส่งผลต่อการตระหนักและการใช้เทคโนโลยีความมั่นคงปลอดภัยทางไซเบอร์ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กรณีศึกษาโครงการเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา (Inter University Network)

ประชากรและกลุ่มตัวอย่าง

ประชากรในการวิจัยครั้งนี้ ได้แก่ บุคลากรที่มีส่วนเกี่ยวข้องกับการดำเนินงานในโครงการเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา (Inter University Network: UniNet) ภายใต้สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา จำนวนทั้งสิ้น 434 คน

กลุ่มตัวอย่างกำหนดขนาดโดยใช้สูตรของ Yamane (1973) [11] ที่ระดับความคลาดเคลื่อน 0.05 ได้ขนาดตัวอย่างขั้นต่ำ 208 คน โดยใช้วิธีการคัดเลือกแบบเจาะจง (Purposive Sampling) จากบุคลากรที่มีบทบาทเกี่ยวข้องกับงานด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์โดยตรงในหน่วยงานที่อยู่ภายใต้โครงการ UniNet โดยกำหนดเกณฑ์การคัดเลือก ได้แก่ บุคลากรที่มีหน้าที่รับผิดชอบหรือปฏิบัติงานด้านดังกล่าว จึงใช้วิธีการคัดเลือกดังกล่าวเพื่อให้ได้กลุ่มตัวอย่างที่มีคุณสมบัติตรงตามวัตถุประสงค์ของการวิจัย ทั้งนี้ สามารถเก็บข้อมูลได้จำนวน 330 ชุด และหลังจากตรวจสอบความสมบูรณ์ของข้อมูลแล้ว เหลือข้อมูลที่ใช้ในการวิเคราะห์จำนวน 327 ชุด

เครื่องมือที่ใช้ในการวิจัย

เครื่องมือที่ใช้ในการวิจัยเป็นแบบสอบถาม (Questionnaire) ซึ่งพัฒนาขึ้นจากการสังเคราะห์วรรณกรรมและงานวิจัยที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์ และแนวคิดด้านพฤติกรรมการใช้เทคโนโลยีและความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ [8] [10] ตามแนวคิดที่ใช้ในการอธิบายพฤติกรรมการยอมรับและการใช้เทคโนโลยีในงานวิจัยด้านระบบสารสนเทศ โดยครอบคลุมตัวแปรสำคัญ ได้แก่ ประสบการณ์ด้านไซเบอร์ การรับรู้ข่าวสาร ความรู้ความเข้าใจ ความร่วมมือ ทัศนคติ พฤติกรรม และความตระหนัก

แบบสอบถามผ่านการตรวจสอบความตรงเชิงเนื้อหา (Content Validity) โดยผู้เชี่ยวชาญจำนวน 5 ท่าน โดยมีค่าดัชนีความสอดคล้องของข้อคำถาม (IOC) มากกว่า 0.5 ทุกข้อ ซึ่งเป็นไปตามเกณฑ์ที่ยอมรับได้ในการวิจัย และทดสอบความเชื่อมั่นของเครื่องมือด้วยค่าสัมประสิทธิ์ Cronbach’s Alpha เท่ากับ .977 ซึ่งอยู่ในระดับสูง แสดงว่าเครื่องมือมีความเหมาะสมและเชื่อถือได้สำหรับการนำไปใช้ในการวิจัย

การวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลแบ่งออกเป็น 2 ส่วน ได้แก่ (1) การวิเคราะห์สถิติเชิงพรรณนา (Descriptive Statistics) เพื่ออธิบายลักษณะทั่วไปของกลุ่มตัวอย่าง โดยใช้ค่าความถี่ ค่าร้อยละ ค่าเฉลี่ย และค่าส่วนเบี่ยงเบนมาตรฐาน และ (2) การวิเคราะห์สถิติเชิงอนุมาน (Inferential Statistics) โดยใช้การวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) เพื่อจัดกลุ่มองค์ประกอบของตัวแปร และการวิเคราะห์โมเดลสมการเชิงโครงสร้าง (Structural Equation Modeling: SEM) [5] [7] ร่วมกับการวิเคราะห์เส้นทาง (Path Analysis) เพื่อทดสอบความสัมพันธ์และอิทธิพลของปัจจัยที่ส่งผลต่อการตระหนักและการใช้เทคโนโลยีความมั่นคงปลอดภัยทางไซเบอร์

เนื่องจากการศึกษาครั้งนี้มีลักษณะมุ่งสำรวจและพัฒนาโครงสร้างปัจจัยในบริบทเฉพาะของโครงการ UniNet ผู้วิจัยจึงใช้การวิเคราะห์องค์ประกอบเชิงสำรวจ (EFA) ร่วมกับการวิเคราะห์โมเดลสมการเชิง

โครงสร้าง (SEM) บนชุดข้อมูลเดียวกัน เพื่อทดสอบความเหมาะสมของโมเดลเบื้องต้น ทั้งนี้ การตรวจสอบความเที่ยงตรงของโมเดลกับกลุ่มตัวอย่างอิสระ (cross-validation) ควรได้รับการพัฒนาเพิ่มเติมในการศึกษาครั้งต่อไป [7]

ผลการวิจัย

การศึกษาปัจจัยที่ส่งผลต่อการตระหนักและการใช้เทคโนโลยีความมั่นคงปลอดภัยทางไซเบอร์ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กรณีศึกษาโครงการเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา (Inter University Network) ได้นำเสนอผลการวิจัยตามวัตถุประสงค์ของการศึกษา ได้แก่ (1) การวิเคราะห์ข้อมูลทั่วไปของกลุ่มตัวอย่าง (2) การวิเคราะห์องค์ประกอบเชิงสำรวจ และ (3) การทดสอบสมมติฐานด้วยโมเดลสมการเชิงโครงสร้าง

1. ข้อมูลทั่วไปของกลุ่มตัวอย่าง

กลุ่มตัวอย่างที่ใช้ในการวิจัยจำนวน 327 คน เป็นบุคลากรที่มีส่วนเกี่ยวข้องกับการดำเนินงานในโครงการเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา โดยผลการวิเคราะห์ข้อมูลทั่วไปแสดงดังตารางที่ 1

ตารางที่ 1 ข้อมูลทั่วไปของกลุ่มตัวอย่าง (n = 327)

ตัวแปร	จำนวน	ร้อยละ
เพศ		
ชาย	188	57.50
หญิง	139	42.50
อายุ		
21-30 ปี	145	44.30
31-40 ปี	133	40.70
41-50 ปี	34	10.40
51-60 ปี	15	4.60
ระดับการศึกษา		
ปริญญาตรีหรือเทียบเท่า	264	80.70
ปริญญาโท	61	18.70
ปริญญาเอก	2	0.60
ประสบการณ์ทำงาน		
ต่ำกว่า 3 ปี	82	25.10
3-5 ปี	170	52.00
6-10 ปี	41	12.50
มากกว่า 10 ปี	34	10.40

ผลการวิเคราะห์พบว่า กลุ่มตัวอย่างส่วนใหญ่เป็นเพศชาย (57.50%) มีอายุระหว่าง 21–30 ปี (44.30%) มีระดับการศึกษาปริญญาตรีหรือเทียบเท่า (80.70%) และมีประสบการณ์ทำงาน 3–5 ปี (52.00%)

2. ผลการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA)

การวิเคราะห์องค์ประกอบเชิงสำรวจใช้วิธี Principal Component Analysis (PCA) และการหมุนแกนแบบ Varimax เพื่อตรวจสอบโครงสร้างของตัวแปรแฝง ผลการทดสอบความเหมาะสมของข้อมูลพบว่าค่า Kaiser–Meyer–Olkin (KMO) อยู่ในช่วง .508 – .840 และค่า Bartlett's Test of Sphericity มีนัยสำคัญทางสถิติ ($p < .001$) แสดงว่าข้อมูลมีความเหมาะสมสำหรับการวิเคราะห์องค์ประกอบ [5] ซึ่งผลการวิเคราะห์พบว่าสามารถจำแนกองค์ประกอบได้ 6 ปัจจัยหลัก ได้แก่

1) ประสบการณ์ความมั่นคงปลอดภัยทางไซเบอร์
2) การรับรู้ข่าวสาร
3) ความรู้ความเข้าใจ
4) ความร่วมมือ
5) ทัศนคติ
6) พฤติกรรม

โดยในปัจจัยด้านความรู้ความเข้าใจ พบว่าองค์ประกอบ มาตรฐานด้านไซเบอร์ และ กฎหมายด้านไซเบอร์มีความสัมพันธ์กันสูงและถูกรวมเป็นองค์ประกอบเดียวกัน

3. ผลการวิเคราะห์โมเดลสมการเชิงโครงสร้าง (Structural Equation Modeling: SEM)

การทดสอบความสอดคล้องของโมเดลสมการเชิงโครงสร้างกับข้อมูลเชิงประจักษ์ พบว่าโมเดลมีค่าดัชนีความสอดคล้องอยู่ในเกณฑ์ที่ยอมรับได้ ดังตารางที่ 2 [5] [7]

ตารางที่ 2 ค่าดัชนีความสอดคล้องของโมเดล

ดัชนี	เกณฑ์มาตรฐาน	ค่าที่ได้
CMIN/df	< 5	1.528
GFI	> 0.90	0.965
CFI	> 0.90	0.988
RMSEA	< 0.10	0.040

เมื่อพิจารณาค่าดัชนีความสอดคล้องหลายรายการร่วมกัน ได้แก่ *CMIN/df, GFI, CFI* และ *RMSEA* พบว่าโมเดลมีความเหมาะสมในภาพรวม สะท้อนว่าโครงสร้างเชิงทฤษฎีที่พัฒนาขึ้นสามารถอธิบายข้อมูลเชิงประจักษ์ในบริบทขององค์กรเครือข่ายการศึกษาได้ในระดับน่าพอใจ

4. ผลการทดสอบสมมติฐาน

การวิเคราะห์เส้นทาง (Path Analysis) เพื่อตรวจสอบอิทธิพลของปัจจัยที่ส่งผลต่อการตระหนักและการใช้เทคโนโลยีความมั่นคงปลอดภัยทางไซเบอร์ พบว่าปัจจัยด้านทัศนคติเป็นปัจจัยเดียวที่มีอิทธิพลอย่างมีนัยสำคัญทางสถิติ

ตารางที่ 3 ผลการทดสอบสมมติฐาน

สมมติฐาน	ปัจจัย	β	p-value	ผล
H1	ประสบการณ์ด้านไซเบอร์	.099	p = .421	ปฏิเสธ
H2	การรับรู้ข่าวสาร	.108	p = .881	ปฏิเสธ
H3	ความรู้ความเข้าใจ	-.046	p = .665	ปฏิเสธ
H4	ความร่วมมือ	.148	p = .191	ปฏิเสธ
H5	**ทัศนคติ**	**.482**	**p < .01**	**ยอมรับ**
H6	พฤติกรรม	.115	p = .958	ปฏิเสธ

ผลการวิเคราะห์พบว่า ปัจจัยด้านทัศนคติ (*Attitude)* มีอิทธิพลต่อการตระหนักและการใช้เทคโนโลยีความมั่นคงปลอดภัยทางไซเบอร์อย่างมีนัยสำคัญทางสถิติที่ระดับ *.01 (β = 0.482)* และสามารถอธิบายความแปรปรวนของตัวแปรตามได้ร้อยละ *25 (R^2 = .250)*

อภิปรายผลและสรุปผล

ผลการวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษาปัจจัยที่ส่งผลต่อการตระหนักและการใช้เทคโนโลยีความมั่นคงปลอดภัยทางไซเบอร์ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในบริบทของโครงการเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา (Inter University Network) โดยใช้การวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) และการวิเคราะห์โมเดลสมการเชิงโครงสร้าง (Structural Equation Modeling: SEM)

ผลการวิเคราะห์พบว่า โมเดลการวิจัยมีความสอดคล้องกับข้อมูลเชิงประจักษ์ โดยมีค่าดัชนีความสอดคล้องของโมเดลอยู่ในเกณฑ์ที่ยอมรับได้ ได้แก่ CMIN/df = 1.528, GFI = .965, CFI = .988 และ RMSEA = .040 แสดงให้เห็นว่าโครงสร้างของตัวแปรและความสัมพันธ์ระหว่างปัจจัยในโมเดลมีความเหมาะสมกับบริบทของการศึกษา

ผลการทดสอบสมมติฐานพบว่า ปัจจัยด้านทัศนคติ (Attitude) เป็นปัจจัยเพียงปัจจัยเดียวที่มีอิทธิพลต่อการตระหนักและการใช้เทคโนโลยีความมั่นคงปลอดภัยทางไซเบอร์อย่างมีนัยสำคัญทางสถิติ (β = .482, p ≤ .01) โดยสามารถอธิบายความแปรปรวนของตัวแปรตามได้ร้อยละ 25 (R^2 = .250) ผลดังกล่าวชี้ให้เห็นว่าทัศนคติของบุคลากรเป็นกลไกสำคัญต่อการสร้างความตระหนักและการนำเทคโนโลยีด้านความปลอดภัยไซเบอร์ไปใช้ในองค์กร

แม้ว่าค่าอำนาจการอธิบายความแปรปรวนของตัวแปรตาม (R^2 = .250) จะอยู่ในระดับปานกลาง แต่ถือว่าอยู่ในเกณฑ์ที่ยอมรับได้สำหรับงานวิจัยด้านพฤติกรรมศาสตร์และการยอมรับเทคโนโลยี เนื่องจากพฤติกรรมของบุคคลมักได้รับอิทธิพลจากหลายปัจจัย ทั้งด้านองค์กร วัฒนธรรม ทรัพยากร และบริบทแวดล้อม ซึ่งอาจไม่ได้รวมอยู่ในโมเดลการศึกษาครั้งนี้ทั้งหมด

ผลที่พบว่าปัจจัยด้านทัศนคติมีอิทธิพลสูงสุด สอดคล้องกับแนวคิด Technology Acceptance Model (Davis, 1989) [4] ที่เสนอว่าทัศนคติของผู้ใช้เป็นกลไกสำคัญก่อนการยอมรับและการใช้งานเทคโนโลยีจริง แสดงให้เห็นว่าแม้องค์กรจะมีนโยบาย เครื่องมือ หรือองค์ความรู้ด้านไซเบอร์แล้ว หากบุคลากรยังไม่เห็นคุณค่า หรือไม่เชื่อมั่นต่อเทคโนโลยีดังกล่าว การนำไปใช้จริงอาจยังไม่เกิดขึ้นอย่างมีประสิทธิผล

สำหรับปัจจัยด้านประสบการณ์ การรับรู้ข่าวสาร ความรู้ความเข้าใจ ความร่วมมือ และพฤติกรรมที่ไม่พบอิทธิพลอย่างมีนัยสำคัญ อาจสะท้อนว่าปัจจัยดังกล่าวมีผลทางอ้อม หรือมีผลผ่านการก่อรูปเป็นทัศนคติของบุคลากรมากกว่าผลทางตรง ซึ่งเป็นประเด็นที่ควรได้รับการศึกษาต่อยอดในอนาคต [6]

โดยสรุป งานวิจัยนี้ชี้ให้เห็นว่าการส่งเสริมทัศนคติที่ดีต่อเทคโนโลยีความมั่นคงปลอดภัยไซเบอร์เป็นปัจจัยสำคัญในการยกระดับการตระหนักและการใช้เทคโนโลยีด้านความปลอดภัยไซเบอร์ในหน่วยงานที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญด้านการศึกษา

ข้อจำกัดของการวิจัย

1. การศึกษานี้เก็บข้อมูลจากกลุ่มตัวอย่างในบริบทของโครงการ UniNet ซึ่งเป็นองค์กรเฉพาะด้าน จึงควรใช้ความระมัดระวังในการอ้างอิงผลไปยังองค์กรประเภทอื่น

2. การวิเคราะห์องค์ประกอบเชิงสำรวจและโมเดลสมการโครงสร้างดำเนินการบนชุดข้อมูลเดียวกัน ซึ่งเหมาะสมกับการศึกษาเชิงสำรวจแต่ควรมีการตรวจสอบซ้ำกับกลุ่มตัวอย่างอิสระในอนาคต

3. โมเดลการศึกษานี้มุ่งเน้นการทดสอบอิทธิพลทางตรงของปัจจัยหลัก จึงยังไม่ได้ครอบคลุมความสัมพันธ์เชิงส่งผ่านหรือเชิงกำกับในรายละเอียด

ข้อเสนอแนะ

1. ข้อเสนอแนะด้านวิชาการ

การศึกษาครั้งต่อไปควรขยายขอบเขตการวิจัยไปยังกลุ่มตัวอย่างที่หลากหลายมากขึ้น เช่น หน่วยงานภาครัฐ หน่วยงานเอกชน หรือสถาบันการศึกษาประเภทอื่น เพื่อเปรียบเทียบปัจจัยที่ส่งผลต่อการตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ในบริบทที่แตกต่างกัน นอกจากนี้ ควรมีการประยุกต์ใช้กรอบแนวคิดหรือทฤษฎีเพิ่มเติม เช่น Technology Acceptance Model (TAM) [4] หรือทฤษฎีการรับรู้ความเสี่ยง (Risk Perception Theory) เพื่อวิเคราะห์ปัจจัยที่มีอิทธิพลต่อการยอมรับและการใช้เทคโนโลยีความมั่นคงปลอดภัยไซเบอร์ได้อย่างครอบคลุมมากยิ่งขึ้น รวมทั้งควรพัฒนาโมเดลเปรียบเทียบทางเลือก (alternative models) และศึกษาบทบาทของตัวแปรส่งผ่าน (mediator) หรือตัวแปรกำกับ (moderator) [7] เพื่ออธิบาย

กลไกการยอมรับเทคโนโลยีความมั่นคงปลอดภัยไซเบอร์ได้ชัดเจนยิ่งขึ้น ตลอดจนการศึกษาวิจัยเชิงคุณภาพ เช่น การสัมภาษณ์เชิงลึกกับผู้เชี่ยวชาญ เพื่อให้ได้ข้อมูลเชิงลึกที่สามารถนำไปใช้พัฒนานโยบายหรือแนวทางการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ในองค์กรได้อย่างมีประสิทธิภาพ

2. ข้อเสนอแนะด้านบริหาร

หน่วยงานที่เกี่ยวข้องกับโครงสร้างพื้นฐานด้านการศึกษา เช่น มหาวิทยาลัยหรือหน่วยงานกำกับดูแลด้านเทคโนโลยีสารสนเทศ ควรให้ความสำคัญกับการพัฒนาทัศนคติของบุคลากรต่อการใช้เทคโนโลยีความมั่นคงปลอดภัยไซเบอร์ โดยส่งเสริมการฝึกอบรม การสร้างความเข้าใจเกี่ยวกับบทบาทของเทคโนโลยีด้านความปลอดภัยไซเบอร์ และการสร้างวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้บุคลากรเห็นถึงความสำคัญของการป้องกันภัยคุกคามทางไซเบอร์และสามารถนำเทคโนโลยีด้านความปลอดภัยมาใช้ได้อย่างมีประสิทธิภาพ

นอกจากนี้ องค์กรควรสนับสนุนการพัฒนาศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ (Security Operations Center: SOC) และกลไกการเฝ้าระวังภัยคุกคามทางไซเบอร์ เช่น CERT หรือ Sectoral CERT [9] เพื่อเพิ่มประสิทธิภาพในการตรวจจับและตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ในระบบเครือข่ายการศึกษา

กิตติกรรมประกาศ

ผู้วิจัยขอขอบพระคุณ รองศาสตราจารย์ ดร.ชัยวัฒน์ อุตตมากร อาจารย์ที่ปรึกษา ตลอดจนคณะกรรมการสอบวิทยานิพนธ์ ที่ได้กรุณาให้คำแนะนำอันทรงคุณค่าต่อการศึกษาครั้งนี้ รวมทั้งขอขอบคุณโครงการเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา (UniNet) และผู้ตอบแบบสอบถามทุกท่านที่ให้ความอนุเคราะห์ข้อมูลเพื่อการวิจัย

เอกสารอ้างอิง

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2562). *พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562*.

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2564). *ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะ หน้าที่ และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ*.

สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา. (2567). *โครงการเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา (UniNet).* กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม.

Davis, F. D. (1989). *Perceived usefulness, perceived ease of use, and user acceptance of information technology*. MIS Quarterly, 13(3), 319–340.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis (8th ed.)*. Cengage Learning.

Ifinedo, P. (2012). *Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory*. Computers & Security, 31(1), 83–95.

Kline, R. B. (2016). *Principles and practice of structural equation modeling (4th ed.)*. Guilford Press.

Kruger, H. A., & Kearney, W. D. (2006). *A prototype for assessing information security awareness*. Computers & Security, 25(4), 289–296.

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity (Version 1.1)*.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). *The human aspects of information security questionnaire (HAIS-Q): Two further validation studies*. Computers & Security, 66, 40–51.

Yamane, T. (1973). *Statistics: An introductory analysis (3rd ed.)*. Harper & Row.