บทปฏิทัศน์อย่างเป็นระบบว่าด้วยแนวทางการเตรียมพร้อมขององค์กร เพื่อยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์
A Systematic Review on Guidelines to Enhancing Organizational Preparation Readiness in Cybersecurity

ณัฐวี อุตกฤษฎ์ (Nattavee Utakrit)
และอนาวิล แก้วสอาด (Anawin Kaewsa-ard)

Received: January 30, 2023
Revised: February 19, 2023
Accepted: March 9, 2023

* ผู้นิพนธ์ประสานงาน: อนาวิล แก้วสอาด (Anawin Kaewsa-ard)

อีเมล: ianawin.tni@gmail.com

บทคัดย่อ

ปัจจุบันเทคโนโลยีสารสนเทศ และเครือข่ายอินเทอร์เน็ต มีการเปลี่ยนแปลง และพัฒนาอย่างรวดเร็ว ส่งผลให้การทำงานขององค์กรต่าง ๆ มีความเสี่ยงต่อภัยคุกคามในรูปแบบใหม่ หนึ่งในนั้นคือภัยคุกคามทางไซเบอร์ บทความวิชาการนี้ได้ศึกษาวรรณกรรมที่เกี่ยวข้อง พร้อมทั้งกรอบแนวคิด ทฤษฎี แบบจำลอง งานวิจัย และการศึกษาสถานการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ โดยนำเสนอแนวทางการเตรียมความพร้อมขององค์กรเพื่อยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ ผ่านการสังเคราะห์เชิงคุณภาพแบ่งออกเป็น 5 ประการ ได้แก่ 1. การประยุกต์ใช้กรอบงานด้านความปลอดภัยที่ได้รับการยอมรับ 2. การจัดตั้งผู้บริหารฝ่ายงานหรือคณะทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร 3. การจัดทำแผนงานด้านความมั่นคงปลอดภัยไซเบอร์ 4. การเสริมสร้างความตระหนักรู้ของบุคลากรด้านความปลอดภัยทางไซเบอร์ 5. การให้ความรู้ และทักษะเกี่ยวกับการใช้งานเทคโนโลยีในการรักษาความมั่นคงปลอดภัยไซเบอร์

คำสำคัญ: ความมั่นคงปลอดภัยไซเบอร์ แนวทางการเตรียมความพร้อมขององค์กร การยกระดับการรักษาความปลอดภัยไซเบอร์ การตระหนักรู้ของบุคลากร

Abstract

Nowadays, Information Technology and Internet networking have changed and developed rapidly. These changes can lead organizational workflows are in risks of the new types of threats. This literature study reviews conceptual frameworks, theories, models, research work and situations related to Cybersecurity. The paper discusses about guidelines to enhancing organizational readiness in Cybersecurity. Five elements of the guidelines include 1) Appling a recognized security framework 2) Appointing managers or corporate cybersecurity committee 3) Developing cybersecurity plan 4) Improving the awareness of personnel in cybersecurity 5) Providing knowledge and skills about using technology to maintain cyber security.

Keywords: Cybersecurity, Organizational Preparation Readiness Guideline, Enhancing Organizational Cybersecurity, Personal Awareness.

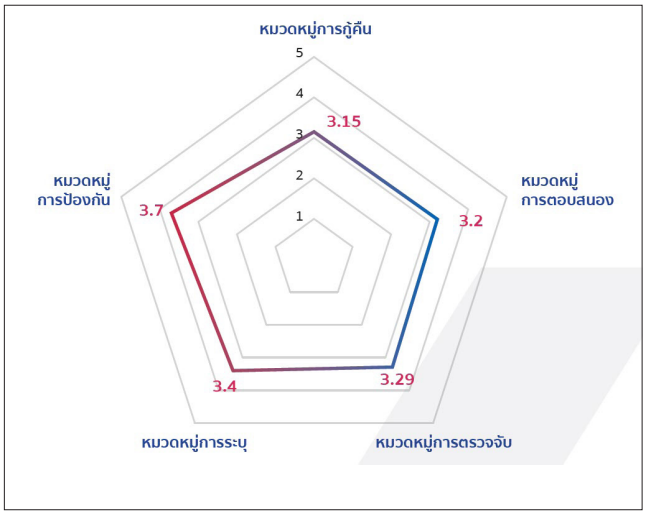
1. บทนำ

ปัจจุบันเทคโนโลยีสารสนเทศ และเครือข่ายอินเทอร์เน็ต เป็นเครื่องมือที่ได้เข้ามามีบทบาทสำคัญอย่างยิ่งต่อองค์กรทุกภาคส่วน ซึ่งล้วนแต่ใช้เครื่องมือดังกล่าวเพื่อช่วยให้ได้เปรียบในการแข่งขัน ไม่ว่าจะเป็น การใช้ระบบสารสนเทศเป็นแกนหลักในการสนับสนุนกิจกรรมขององค์กร การเปลี่ยนแปลงรูปกลยุทธ์รูปแบบการทำงาน เช่น รูปแบบ Work from Home โดยการเชื่อมต่อผ่านอินเทอร์เน็ตเพื่อเข้าถึงทรัพยากรขององค์กร เนื่องจากบริบทของเทคโนโลยีที่มีการพัฒนาอย่างต่อเนื่อง จึงส่งผลให้องค์กรต้องมีการปรับตัวการทำงานเพื่อให้ทันการเปลี่ยนแปลงทางเทคโนโลยีที่เกิดขึ้นอย่างรวดเร็ว (Disruptive Technology) [1] ทั้งนี้การเปลี่ยนแปลงที่สำคัญอีกประเด็นหนึ่งคือภัยคุกคามทางไซเบอร์ในรูปแบบใหม่ ๆ ที่ตรวจจับได้ยาก และมีผลกระทบรุนแรงต่อองค์กรมากขึ้น ภัยคุกคามทางไซเบอร์กำลังเป็นเรื่องท้าทายในยุคเศรษฐกิจดิจิทัล เพราะภัยคุกคามดังกล่าวเป็นความเสี่ยงต่อภาพลักษณ์และชื่อเสียงขององค์กรที่ได้สั่งสมมาเป็นเวลาหลายปี [2] ดังนั้นผู้บริหาร หรือคณะกรรมการบริหารในปัจจุบันจึงเริ่มให้ความสำคัญต่อการบริหารความเสี่ยง

* ภาควิชาการจัดการเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
* Department of Information Technology Management, Faculty of Information Technology and Digital Innovation, King Mongkut's University of Technology North Bangkok.

ระดับองค์กร การคุ้มครองข้อมูลส่วนบุคคล และการสร้างความตระหนักรู้ด้านไซเบอร์ให้กับองค์กร [3], [4]

นับตั้งแต่มีการบังคับใช้ พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ตามมาตราที่ 49 ให้มีการจัดตั้งหน่วยงานโครงสร้างพื้นฐานสำคัญด้านสารสนเทศ (Critical Information Infrastructure: CII) ประกอบด้วย ด้านความมั่นคงของรัฐ ด้านการบริการภาครัฐที่สำคัญ ด้านการเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศ และโทรคมนาคม ด้านการขนส่งและโลจิสติกส์ ด้านพลังงานและสาธารณูปโภค ด้านสาธารณสุข และอื่น ๆ ตามที่ตามที่คณะกรรมการประกาศเพิ่มเติม ทำให้หน่วยงานภาครัฐ และภาคเอกชนต่างให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยไซเบอร์ในองค์กรอย่างยั่งยืน [5], [6] ทั้งนี้จากผลการศึกษา และการประเมินความพร้อมในการรับมือความเสี่ยงต่อภัยคุกคามทางไซเบอร์ระดับกลุ่มหน่วยงาน CII ระดับหน่วยงานภาครัฐ ซึ่งจัดทำโดยสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ปี พ.ศ. 2564 พบว่าหน่วยงาน CII มีคะแนนเฉลี่ยรวม 3.35 คะแนน จากคะแนนเต็ม 5 คะแนน โดยการประเมินผลจาก NIST Cyber Security Framework (NIST CSF) ประกอบด้วยด้านการระบุ (Identify) 3.4 คะแนน ด้านการป้องกัน (Protect) 3.7 คะแนน ด้านการตรวจจับ (Detect) 3.29 คะแนน ด้านการตอบสนอง (Response) 3.2 คะแนน และด้านการกู้คืน (Recovery) 3.15 คะแนน รายละเอียดตามภาพที่ 1 โดยหน่วยงาน CII ที่มีคะแนนสูงสุด 3 อันดับแรก คือ หน่วยงานด้านการเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม และด้านการขนส่งและโลจิสติกส์ ส่วนหน่วยงานที่มีคะแนนเฉลี่ยต่ำสุด 3 อันดับสุดท้าย คือ ด้านสาธารณสุข ด้านความมั่นคงของรัฐ และด้านการบริการภาครัฐที่สำคัญ [7] จากผลการประเมินขีดความสามารถในการรับมือสถานการณ์ทางไซเบอร์จะเห็นได้ว่าหน่วยงาน CII 3 อันดับสุดท้ายจะต้องมีการยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างเร่งด่วน เพื่อเป็นการเตรียมความพร้อมในการรับมือความเสี่ยงต่อภัยคุกคามทางไซเบอร์ก่อนที่จะส่งผลเสียร้ายแรงต่อองค์กร และหากเกิดเหตุการณ์ทางไซเบอร์ขึ้น องค์กรควรจะมีความสามารถในการตอบสนองต่อการโจมตีได้อย่างรวดเร็ว เพราะต่อจากนี้ทั้งในปัจจุบัน และอนาคตองค์กรมีความจำเป็นต้องทำให้ระบบสารสนเทศสามารถทนทานต่อภัยคุกคามทางไซเบอร์รูปแบบใหม่ ๆ อยู่ตลอดเวลา รวมถึงการปรับปรุงนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์และให้ความตระหนักรู้กับบุคลากรภายในองค์กรอย่างต่อเนื่อง



ภาพที่ 1 *ผลการประเมินขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของ CII ประเทศไทย จาก สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)*

2. ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

2.1 นิยามศัพท์ (Definition)

ณฐพร และ ณัฐวี [8] ได้อธิบายถึงความเหมือนและความแตกต่างของคำว่า ความมั่นคงปลอดภัยสารสนเทศ (Information Security: IS) และการประกันความมั่นคงปลอดภัยสารสนเทศ (Information Assurance: IA) ไว้ว่า IS และ IA ต่างก็ให้ความสำคัญไปที่การปกป้องโครงสร้างพื้นฐานสารสนเทศขององค์กร ทั้งนี้คำจำกัดความทั้งสองนั้นมีความเชื่อมโยงในการรับมือกับภัยคุกคามที่มีแนวโน้มส่งผลต่อความเป็นส่วนตัว การบุกรุกระบบสารสนเทศ และกลยุทธ์ที่ใช้ในการรับมือกับภัยคุกคามดังกล่าว

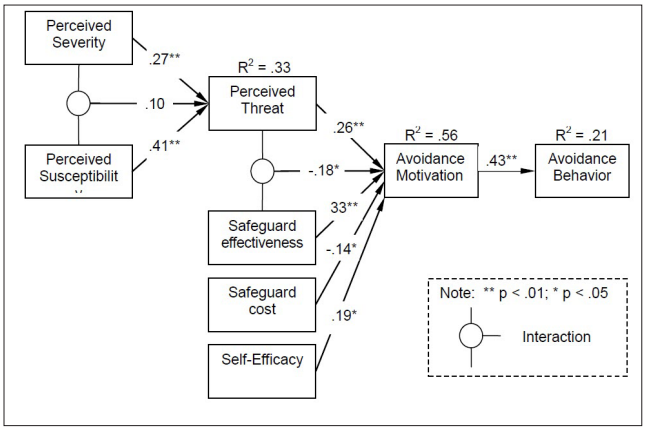
บทความดังกล่าวได้อธิบายความหมายของ IA ไว้ว่าเป็นวิธีการในการจัดการเกี่ยวกับการใช้งานสารสนเทศ การกำกับดูแล (Governance) และการบริหารความเสี่ยง (Enterprise Risk Management) ตลอดจนการวางกลยุทธ์และแผนงบประมาณเพื่อขับเคลื่อนธุรกิจขององค์กรให้มีความมั่นคงปลอดภัย ส่วน IS เป็นแนวปฏิบัติจะเน้นไปที่การพัฒนา หรือยกระดับเครื่องมือ เทคโนโลยี

ระบบสารสนเทศ แอปพลิเคชัน และกระบวนการ รวมถึงการให้ความตระหนักรู้กับคนภายในองค์กร เพื่อให้เกิดความมั่นคงปลอดภัยแบบบูรณาการ แต่ทั้งนี้ IA และ IS ควรจะมีการประยุกต์ใช้เข้ากับบริบทขององค์กรไม่ว่าจะเป็นองค์กรขนาดเล็ก กลาง หรือใหญ่ ตลอดจนการกำหนดบทบาทหน้าที่ความรับผิดชอบของคนในองค์กรเพื่อสร้างมาตรการควบคุมในการปกป้องสารสนเทศจากความเสี่ยงที่ส่งผลต่อสารสนเทศ

2.2 ทฤษฎีการหลีกเลี่ยงภัยคุกคามทางเทคโนโลยี (Technology Threat Avoidance Theory: TTAT)

ทฤษฎีการหลีกเลี่ยงภัยคุกคามเทคโนโลยีสารสนเทศเป็นทฤษฎีที่ใช้อธิบายถึงกระบวนการ และปัจจัยของพฤติกรรมการหลีกเลี่ยงภัยคุกคามของภัยคุกคามทางเทคโนโลยีสารสนเทศกับผู้ใช้งาน (Users) โดย ต้องการแสดงให้เห็นถึงกระบวนการทางปัญญาของมนุษย์ ภายใต้อิทธิพลของภัยคุกคามและการระบุตัวแปรพื้นฐานในการประเมินขีดความสามารถการรับมือจากภัยคุกคามดังกล่าว

H. Liang, และ Y. Xue. [9] ได้เริ่มต้นจากการพัฒนาทฤษฎี TTAT ให้อยู่ในรูปแบบของแบบจำลองกระบวนการ (Process Theory) แต่ทั้งนี้เนื่องจากทฤษฎีกระบวนการไม่ได้แสดงให้เห็นถึงปัจจัยที่ส่งผลต่อกระบวนการหลีกเลี่ยงภัยคุกคามดังกล่าว เพื่อทำความเข้าใจพฤติกรรมการหลีกเลี่ยงของผู้ใช้งานระบบสารสนเทศ ผู้วิจัยจึงได้มีการบูรณาการทฤษฎีแรงจูงใจเพื่อป้องกันโรค (Protection Motivation Theory: PMT) (Ref PMT) และงานวิจัยที่เกี่ยวข้องกับการวิเคราะห์ความเสี่ยง (Risk Analysis Research) [10], [11], [12] ร่วมด้วย เพื่อให้ทฤษฎี TTAT สามารถระบุปัจจัยที่ส่งผลต่อความสัมพันธ์ต่อการหลีกเลี่ยงภัยคุกคามมากยิ่งขึ้น และในปี 2010 H. Liang, และ Y. Xue [13] ได้ทำการพัฒนาแบบจำลองพฤติกรรมการหลีกเลี่ยงสปายแวร์โดยใช้ทฤษฎี TTAT กับกลุ่มตัวอย่างนักศึกษาระดับปริญญาตรี สาขาบริหารธุรกิจ ประเทศสหรัฐอเมริกา จำนวน 152 คน ซึ่งเป็นกลุ่มผู้ใช้งานคอมพิวเตอร์ทั่วไป (Non-IT User) และทดสอบสมมติฐานทางสถิติด้วยแบบจำลองสมการโครงสร้างพบว่าแบบจำลองดังกล่าวรายละเอียดตามภาพที่ 2 สามารถอธิบายความตั้งใจในการหลีกเลี่ยงสปายแวร์ของกลุ่มตัวอย่างได้ที่ร้อยละ 56 และพฤติกรรมในการหลีกเลี่ยงสปายแวร์ที่ร้อยละ 21 สามารถอธิบายได้ว่าในกรณีที่ผู้ใช้งานคอมพิวเตอร์ทั่วไปสามารถตระหนักได้ถึงภัยคุกคามที่เกิดขึ้นกับตนเอง จะมีความตั้งใจในการหลีกเลี่ยงภัยคุกคาม แต่อย่างไรก็ตามหากผู้ใช้งานไม่ทราบถึงวิธีการรับมือกับภัยคุกคามดังกล่าวจากผลสำรวจพบว่ากลุ่มตัวอย่างดังกล่าวเลือกที่จะเพิกเฉยต่อภัยคุกคามที่เกิดขึ้น [13]



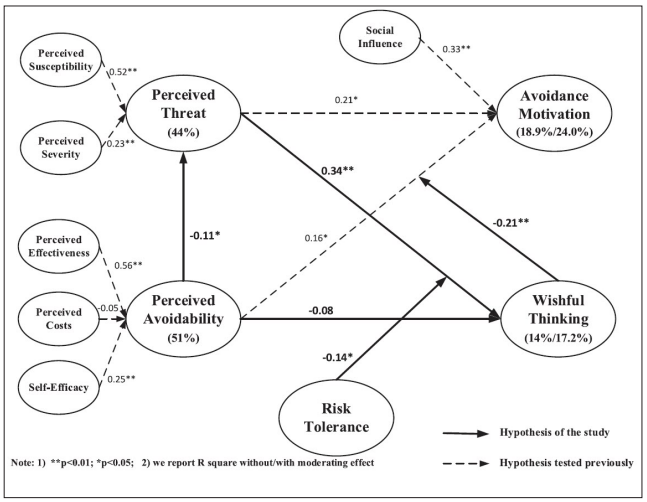
ภาพที่ 2 *Spyware Avoidance Behavior Hypothesis Testing with Structural Equation Modeling*

งานวิจัยของ D. Q. Chen., และ H. Liang. [14] ได้ทำการศึกษาพฤติกรรมการหลีกเลี่ยงภัยคุกคามที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ร่วมกับแนวความคิดการมองโลกในแง่ดี (Wishful Thinking) ในระดับผู้ใช้งานคอมพิวเตอร์ เกี่ยวกับการตั้งค่าความปลอดภัยให้กับเครือข่าย โดยใช้ทฤษฎี TTAT รายละเอียดพบว่าการมองโลกในแง่ดีนั้น ส่งผลต่อพฤติกรรมความปลอดภัยของผู้ใช้งาน โดยเฉพาะอย่างยิ่งเมื่อผู้ใช้งานรู้สึกว่าความเสี่ยงที่เกิดขึ้นจากภัยคุกคามนั้น มีโอกาสที่จะเกิดขึ้นกับตัวเองต่ำ จะส่งผลให้การเตรียมความพร้อมในการรับมือกับภัยคุกคามลดลงเช่นเดียวกัน จากผลการวิเคราะห์ข้อมูลจากแบบจำลองสมการโครงสร้างรายละเอียดตามภาพที่ 3 ทำให้ผู้วิจัยสรุปได้ว่า การสร้างพฤติกรรมความปลอดภัยด้านเทคโนโลยีสารสนเทศในระดับบุคคลจะต้องมีการให้ความรู้เกี่ยวกับแนวทางการป้องกันภัยคุกคามทางไซเบอร์ และการสร้างความตระหนักรู้ถึงการเตรียมความพร้อมเพื่อรับมือกับภัยคุกคามดังกล่าวที่มีโอกาสเกิดขึ้น ทั้งนี้เพื่อเป็นการสร้างความเชื่อมั่นให้กับผู้ใช้งานว่าภัยคุกคามนั้นสามารถหลีกเลี่ยงหรือรับมือได้ด้วยตนเองในกรณีที่ผู้ใช้งานมีความรู้และทักษะที่เพียงพอ [14]

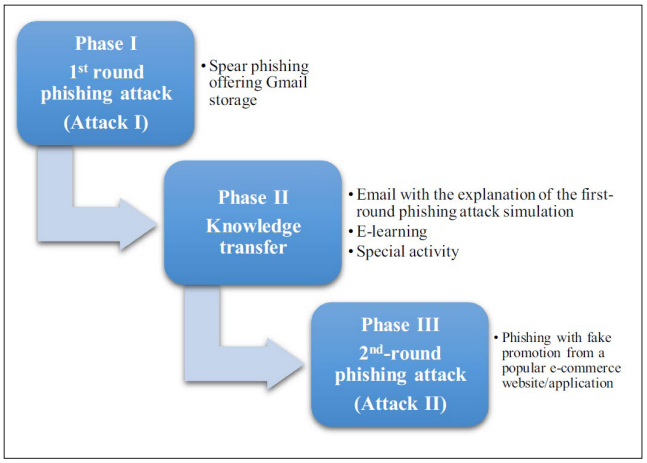
2.3 การสร้างสถานการณ์ทางไซเบอร์เพื่อสร้างความตระหนักรู้ (Scenario Based Learning)

งานวิจัยของเทอดพงษ์ และคณะ [15] ได้ทำการศึกษาความตระหนักรู้ด้านไซเบอร์ของพนักงานไทย หน่วยงานด้านการเงิน การธนาคาร จำนวน 20,134 คน การวิจัยครั้งนี้

แบ่งออกเป็น 3 ขั้นตอน ประกอบไปด้วยขั้นตอนที่ 1 การโจมตีด้วย Phishing Mail ขั้นตอนที่ 2 การให้ความรู้ผ่านระบบ E-Learning และจัดกิจกรรมให้ความตระหนักรู้ Phishing Mail และขั้นตอนที่ 3 สร้างสถานการณ์ทางไซเบอร์ด้วย Fake Promotion Campaign ผ่านการโจมตีด้วย Phishing Mail รายละเอียดตามภาพที่ 4



ภาพที่ 3 *Wishful Thinking Hypothesis Testing with Structural Equation Modeling*



ภาพที่ 4 *กระบวนการสร้างความตระหนักรู้ด้านไซเบอร์*

จากผลการวิจัยพบว่าความตระหนักรู้ของกลุ่มตัวอย่างพนักงานไทยเพิ่มขึ้นอย่างมีนัยสำคัญทางสถิติ (P-Values <0.05) โดยจำนวนของพนักงานไทยที่เปิด Phishing Mail ลดลงถึง 71.5% ทั้งนี้ยังพบว่าพนักงานไทยเพศผู้หญิงมีความตระหนักรู้มากกว่าพนักงานไทยเพศชาย และกลุ่มคนทำงาน Gen X Gen Y และ Baby Boomers มีความตระหนักรู้ที่ไม่แตกต่างกัน ดังนั้นการให้ความตระหนักรู้ด้านไซเบอร์กับพนักงานภายในองค์กรในทุกช่วงอายุ และบทบาทหน้าที่ ส่งผลต่อการสร้างความตระหนักรู้ด้านไซเบอร์อย่างยั่งยืนต่อองค์กร [15]

3. กรอบแนวคิดการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับสากล

3.1 กรอบแนวคิด NIST

NIST ได้ออก NIST Cyber Security Framework Version 1.0 ในปี พ.ศ. 2557 และได้มีการปรับปรุงเป็น Version 1.1 ในปี พ.ศ. 2561 [16] โดยมีวัตถุประสงค์เพื่อให้หน่วยงานโครงสร้างพื้นฐานสารสนเทศที่สำคัญได้นำ 5 กระบวนการหลักของ NIST Framework Core Structure นำมาใช้ประโยชน์ในการปรับปรุงความปลอดภัย ความเสี่ยงพื้นฐาน สำหรับเจ้าของผู้ประกอบการ หรือผู้สร้างโครงสร้างพื้นฐานสำคัญในองค์กรไปประยุกต์ใช้ตามบริบทของหน่วยงาน โดยไม่ได้บังคับตามกฎหมายแต่อย่างใด แต่ต้องการส่งเสริมให้องค์กรปรับกระบวนการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ให้เข้าสู่สถานะที่เรียกว่า Cyber Resilience [17] ซึ่งจากคำนิยามศัพท์ในเอกสาร President Policy Practice: Critical Infrastructure Security and Resilience [18] หมายถึง ความสามารถในการเตรียมตัวและการปรับตัวต่อการเปลี่ยนแปลง รวมถึงขีดความสามารถในการทนทานต่อการบุกรุก โจมตี รวมทั้งภัยธรรมชาติและภัยที่มนุษย์ได้ก่อขึ้นทั้งในรูปแบบตั้งใจ (Intention) หรือไม่ได้ตั้งใจ (Lack of Awareness) องค์ประกอบ Framework Core Function แบ่งย่อยออกเป็นกรอบงานหลัก 5 ฟังก์ชัน รายละเอียดตามภาพที่ 5 ซึ่งเป็นกิจกรรมงานหลักด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งประกอบไปด้วย

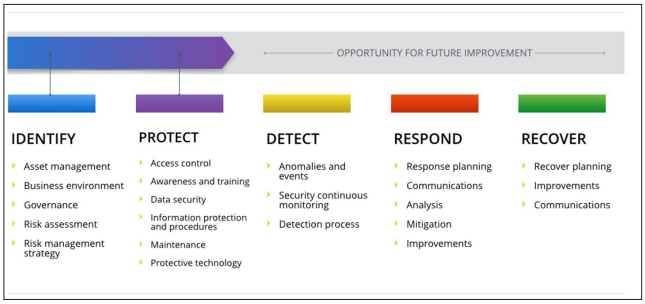
1) การระบุ (Identify) เป็นขั้นตอนแรกในการศึกษาทำความเข้าใจบริบท ทรัพยากร และกิจกรรม หรืองานสำคัญเพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มีต่อระบบสารสนเทศ

2) การป้องกัน (Protect) เป็นการจัดทำ และดำเนินการตามมาตรการควบคุมสำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยมีวัตถุประสงค์เพื่อควบคุมผลกระทบของเหตุการณ์ทางไซเบอร์ สร้างความตระหนักรู้ด้านไซเบอร์ การควบคุมการเข้าถึงระบบสารสนเทศ และมาตรการสร้างความปลอดภัยต่อผู้ใช้งาน กระบวนการ และเทคโนโลยีสารสนเทศ

3) การตรวจจับ (Detect) เป็นการตรวจหาเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น ครอบคลุมถึงกระบวนการเฝ้าระวัง หรือการติดตามอย่างต่อเนื่อง

4) การตอบสนอง (Respond) เป็นการจัดทำ และดำเนินกิจกรรมตามแผนงานเพื่อตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ ครอบคลุมถึงการกำหนดช่องทางการติดต่อสื่อสารเมื่อเกิดเหตุการณ์ การวิเคราะห์สถานการณ์ทางไซเบอร์ และการลดผลกระทบที่เกิดขึ้นต่อระบบสารสนเทศขององค์กร

5) การคืนสภาพ (Recover) เป็นการกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อให้กิจกรรมขององค์กรสามารถดำเนินได้อย่างต่อเนื่อง และฟื้นฟูระบบสารสนเทศหรือฟังก์ชันงานหลักขององค์กรให้กลับคืนสู่สภาพเดิม

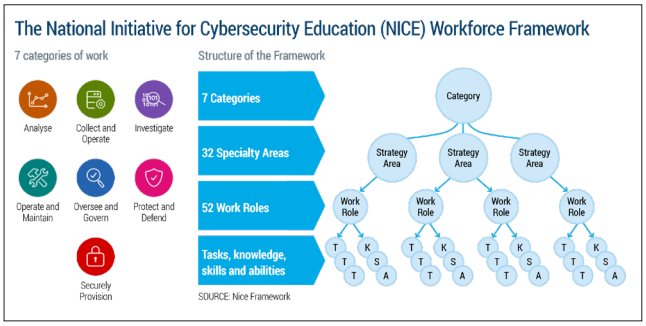


ภาพที่ 5 *NIST Framework Core Structure*
จาก https://www.nist.gov/cyberframework

3.2 โครงสร้างกรอบแนวคิดของ NICE Framework

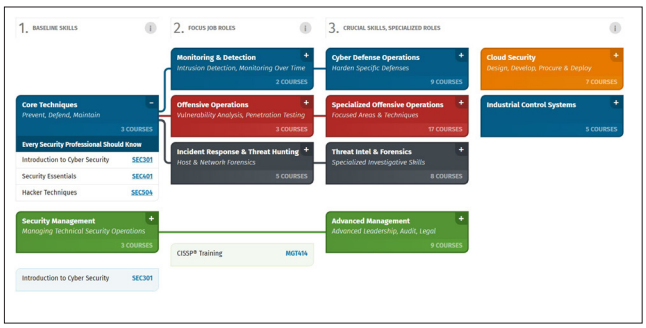
เนื่องจากงานด้านความมั่นคงปลอดภัยไซเบอร์มีความหลากหลาย ทั้งโครงสร้างองค์กร บทบาท หน้าที่ ความรับผิดชอบ ความรู้ทักษะที่จำเป็นต่อการปฏิบัติงาน ซึ่งครอบคลุมถึงการบริหารจัดการ และด้านเทคนิค เพื่อเป็นการเสริมสร้างและยกระดับขีดความสามารถของบุคลากรด้านไซเบอร์ โครงการ National Initiative for Cybersecurity Education (NICE) จึงได้ถูกก่อตั้งขึ้นโดยประธานาธิบดี Barack Obama โดยวัตถุประสงค์ของโครงการนี้เพื่อสร้างความตระหนักรู้ การให้การศึกษา ฝึกอบรม และพัฒนาบุคลากรให้สามารถรับมือกับภัยคุกคามด้านไซเบอร์ที่กระทบต่อความมั่นคงของประเทศได้อย่างมีประสิทธิภาพ นอกจากนี้ทาง NICE ได้ร่วมมือกับหน่วยงานภาครัฐและเอกชนต่าง ๆ ของประเทศสหรัฐฯ กำหนดกรอบดำเนินงานการบริหารบุคลากรด้านไซเบอร์ที่เรียกว่า National Cybersecurity Workforce Framework ซึ่งสามารถนำไปประยุกต์ใช้ทั้งหน่วยงานภาครัฐ และเอกชนในทุกอุตสาหกรรม [19]

ในโครงสร้างของ National Cybersecurity Working Force Framework ได้มีการแบ่งความชำนาญพิเศษ (Specialty Area) เป็นหัวข้อ 52 บทบาทหน้าที่การทำงาน (Work Roles) และจัดความชำนาญพิเศษที่มีความเกี่ยวข้องกันให้อยู่ในกลุ่มหน้าที่เดียวกันซึ่ง NICE ได้จัดแบ่งกลุ่มหน้าที่ของงานด้านความมั่นคงปลอดภัยไซเบอร์ออกเป็น 7 กลุ่มหน้าที่ ประกอบด้วย กลุ่มงานเตรียมความพร้อมด้านความปลอดภัย (Securely Provision) กลุ่มงานปฏิบัติการ และบำรุงรักษา (Operate and Maintain) กลุ่มงานป้องกัน และต้านทาน (Protect and Defend) กลุ่มตรวจสอบ (Investigate) กลุ่มงานเก็บรวบรวม และปฏิบัติการ (Collect and Operate) กลุ่มงานวิเคราะห์ (Analyze) และกลุ่มงานด้านการกำกับดูแลและพัฒนากรอบแนวทาง (Oversight and Development) รายละเอียดตามภาพที่ 6 [20], [21], [22]



ภาพที่ 6 *NICE Framework Structure*
จาก https://niccs.cisa.gov/

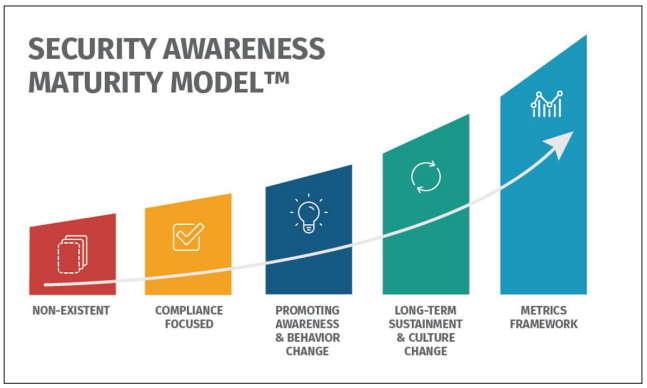
3.3 การประยุกต์ใช้ NICE Framework ร่วมกับการพัฒนาหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์



ภาพที่ 7 *SANS Cyber Security Skills Roadmap*
จาก https://bit.ly/3xeVyU2

SANS ได้นำ NICE Framework ไปพัฒนาเป็นหลักสูตรด้านไซเบอร์ทั้งเชิงรุก และเชิงรับ รายละเอียดตามภาพที่ 7 โดยแบ่งหลักสูตรต่าง ๆ ออกเป็น 3 ระดับ ประกอบด้วย ระดับที่ 1 ความมั่นคงปลอดภัยไซเบอร์เบื้องต้น (Baseline Skills) ระดับที่ 2 การปฏิบัติงานด้านไซเบอร์เชิงรุก และรับ (Focus Job Roles) และระดับที่ 3 ระดับเชี่ยวชาญ และงานเฉพาะด้าน (Crucial Skills and Specialize Roles) [23]

3.4 แบบจำลองวุฒิภาวะในการยกระดับความตระหนักรู้ด้านไซเบอร์ของ SANS



ภาพที่ 8 แบบจำลองวุฒิภาวะการสร้างความตระหนักรู้ด้านไซเบอร์ของ *SANS จาก https://bit.ly/3HSBUlS*

SANS ได้ทำการพัฒนาแบบจำลองวุฒิภาวะ รายละเอียดตามภาพที่ 8 เพื่อใช้เป็นเครื่องมือในการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร และบริหารจัดการความเสี่ยงในส่วนของบุคคลากร (Human Risk and Insider Threat) ทั้งในส่วนของกลุ่มผู้ใช้งานทั่วไป และกลุ่มผู้ปฏิบัติงานด้าน IT [24] โดยแบบจำลองดังกล่าวมีด้วยกัน *5* ระดับดังนี้

1) ระดับที่ 1 ไม่มีกรอบแนวทางการสร้างความตระหนักรู้ด้านไซเบอร์ขององค์กร

2) ระดับที่ 2 มีกรอบแนวทางทางสร้างความตระหนักรู้ด้านไซเบอร์เพื่อปฏิบัตินโยบาย แนวปฏิบัติ กฎระเบียบ หรือข้อบังคับต่าง ๆ

3) ระดับที่ 3 มีกรอบแนวทางการสร้างความตระหนักรู้ด้านไซเบอร์เพื่อสนับสนุนการทำงานตามบทบาทหน้าที่ของพนักงานภายในองค์กร

4) ระดับที่ 4 กรอบแนวทางการสร้างความตระหนักรู้ด้านไซเบอร์ได้รับการสนับสนุนจากผู้บริหารระดับสูง และเป็นส่วนหนึ่งของแผนงานประจำปี

5) ระดับที่ 5 องค์กรสามารถกำหนดมาตรวัดเพื่อใช้ประเมินความตระหนักรู้ด้านไซเบอร์ขององค์กร และยกระดับกรอบในแนวทางการรับมือกับภัยคุกคามทางไซเบอร์ได้ตามสถานการณ์ปัจจุบัน

4. ผลการสำรวจความตระหนักรู้ด้านไซเบอร์ของพนักงานไทยช่วงอายุ 22-60 ปี

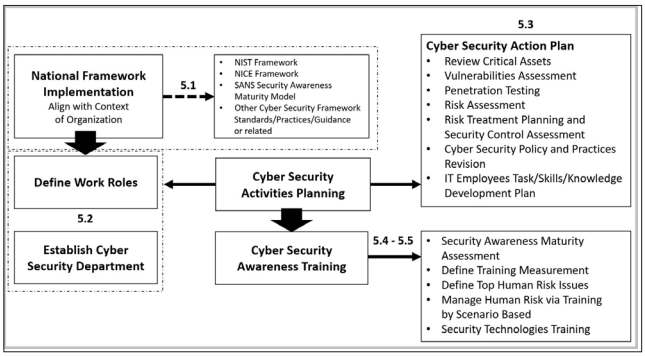
ผู้เขียนบทความได้ทำการสำรวจเพื่อศึกษาระดับความตระหนักรู้ด้านไซเบอร์ของพนักงานไทยที่ต้องปฏิบัติงาน Work from Home ช่วงอายุ 22-60 ปี จำนวน 459 คน เป็นเพศชาย จำนวน 260 คน เพศหญิง จำนวน 188 คน เพศทางเลือกจำนวน 7 คน และไม่ระบุเพศ จำนวน 4 คน ซึ่งมีระดับการศึกษาตั้งแต่ต่ำกว่าระดับปริญญาตรี ไปจนถึงระดับปริญญาเอก ผ่านเครื่องมือแบบสอบถามออนไลน์ด้วยวิธีการสุ่มตัวอย่าง โดยไม่ใช้ความน่าจะเป็น จากสื่อสังคมออนไลน์ การฝึกอบรมหลักสูตรความตระหนักรู้ด้านไซเบอร์ของหน่วยงานภาครัฐ และกลุ่มอาสาสมัครจากหน่วยงานภาครัฐ และเอกชน โดยใช้มาตรวัดลิเคิร์ท 7 ระดับ

จากผลการสำรวจพบว่า พนักงานไทยกลุ่มตัวอย่างช่วงอายุ 22-60 ปี มีความตระหนักรู้ด้านไซเบอร์ในเบื้องต้นเพียงพอสำหรับการทำงาน Work from Home แต่อย่างไรก็ตาม พบว่ากลุ่มตัวอย่างดังกล่าวยังไม่คุ้นชินกับเทคโนโลยีที่ใช้ในการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น การใช้เครือข่ายเสมือน (Virtual Private Network) การใช้ระบบจัดการรหัสผ่าน (Password Manager) การยืนยันตัวตนเข้าใช้งานแบบหลายขั้นตอน (Multifactor Authentication) รวมถึงการใช้งานเครื่องมือป้องกันมัลแวร์ (Anti-Malware)

5. แนวทางการเตรียมความพร้อมกับสถานการณ์ทางไซเบอร์ในอนาคต

จากผลการศึกษากรอบแนวคิดระดับสากลจะเห็นได้ว่ากรอบแนวคิดทั้ง NIST Cybersecurity Framework NICE Framework และ SANS มีความเชื่อมโยงไปที่การบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ขององค์กรให้มีประสิทธิภาพ ครอบคลุมทั้งระดับผู้ใช้งาน (User) การกำกับดูแลกิจการ (Governance) การใช้งานเทคโนโลยีสารสนเทศให้เกิดความปลอดภัย ทั้งนี้เพื่อยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กรในยุคดิจิทัล บทปฏิทัศน์ฉบับนี้จึงเป็นการรวบรวมและสังเคราะห์ข้อมูลที่เกี่ยวข้องอย่างเป็นระบบ [25]

ซึ่งประกอบด้วยวรรณกรรมที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ กรอบแนวคิด ทฤษฎี แบบจำลอง งานวิจัย และการศึกษาสถานการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ เพื่อนำเสนอแนวทางการเตรียมพร้อมขององค์กรเพื่อยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีรายละเอียดตามหัวข้อที่ 5.1-5.5 และการนำเสนอในรูปแบบกรอบการดำเนินงานตามภาพที่ 9



ภาพที่ 9 กรอบแนวทางการเตรียมความพร้อมเพื่อรับมือกับสถานการณ์ทางไซเบอร์

5.1 ควรมีการนำกรอบงานที่ได้รับการยอมรับ เช่น NIST Framework NICE Framework SANS Security Awareness Model หรือมาตรฐานอื่น ๆ ที่เกี่ยวข้องนำมาปรับใช้ร่วมกับบริบทขององค์กร เพื่อยกระดับขีดความสามารถการรักษาความมั่นคงปลอดภัยไซเบอร์

5.2 องค์กรควรมีการจัดตั้งผู้บริหารฝ่ายงาน หรือคณะทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กรอย่างเป็นทางการ ตลอดจนการกำหนดบทบาทหน้าที่ความรับผิดชอบเพื่อสนับสนุนภารกิจ และกิจกรรมต่าง ๆ ขององค์กร ตามแนวทางของ NIST Framework และ NICE Framework

5.3 องค์กรควรมีการจัดทำแผนงานด้านความมั่นคงปลอดภัยไซเบอร์ประจำปี เช่น การปรับปรุงนโยบาย แนวปฏิบัติ และกรอบการดำเนินงานการประเมินความเสี่ยง การหาช่องโหว่และทดสอบเจาะระบบ การตรวจประเมินมาตรฐานด้านไซเบอร์ พร้อมจัดสรรงบประมาณให้เพียงพอสำหรับการพัฒนาบุคลากรสายงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

5.4 องค์กรควรมีการเสริมสร้างความตระหนักรู้โดยการจัดฝึกอบรม ให้กับบุคลากรภายในองค์กร ตั้งแต่เจ้าหน้าที่ระดับปฏิบัติการ หัวหน้างาน และผู้บริหารแต่ละฝ่ายงาน ตลอดจนผู้บริหารระดับสูง และประเมินระดับความตระหนักรู้ด้วยกรอบงานที่ได้รับการยอมรับ เช่น SANS Security Awareness Model เพื่อเป็นการเตรียมความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ที่จะเกิดขึ้นในอนาคต

5.5 องค์กรควรมีการให้ความรู้และทักษะเกี่ยวกับการใช้งานเทคโนโลยีในการรักษาความมั่นคงปลอดภัยไซเบอร์กับผู้ใช้งานทั่วไปภายในองค์กร (Non-IT User) เช่น การใช้งานโปรแกรมป้องกันมัลแวร์ การใช้งานเครือข่ายเสมือน (VPN: Virtual Private Network) การพิสูจน์ทราบตัวตนหลายขั้นตอน (MFA: Multifactor Authentication) การใช้งานแอปพลิเคชั่นเพื่อการจัดการบัญชีเข้าใช้งาน (Password Manager) หรืออื่น ๆ ที่เกี่ยวข้องตามบริบทขององค์กร

6. สรุป

ประเทศไทยได้ก้าวเข้าสู่เทคโนโลยีดิจิทัลอย่างเต็มตัว ซึ่งทำให้เกิดการเปลี่ยนแปลงในเชิงบวกในการยกระดับความคุณภาพชีวิตให้กับคนในประเทศ รวมถึงการขับเคลื่อนเศรษฐกิจดิจิทัลจากองค์กรทุกภาคส่วน แต่อย่างไรก็ตาม ก็มีโอกาสที่จะส่งผลในทางลบได้เช่นกัน เมื่อไม่สามารถนำเทคโนโลยีมาใช้งานได้อย่างคุ้มค่า หรือเกิดปัญหาต่าง ๆ ขึ้นจากการนำเทคโนโลยีมาใช้อย่างไม่ถูกต้อง หรือขาดความปลอดภัยในการใช้งาน ดังนั้นองค์กรควรสร้างความมั่นคงปลอดภัยไซเบอร์ โดยการเตรียมพร้อมขององค์กรเพื่อยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ ควรประกอบไปด้วย 5 ประการ ได้แก่ 1) การประยุกต์ใช้กรอบงาน หรือมาตรฐานที่ได้รับการยอมรับร่วมกับบริบทการทำงานขององค์กรนั้น ๆ 2) การจัดตั้งผู้บริหารฝ่ายงาน หรือคณะทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร 3) การจัดทำแผนงานด้านความมั่นคงปลอดภัยไซเบอร์ 4) การเสริมสร้างความตระหนักรู้ให้แก่บุคลากรขององค์กรด้านความมั่นคงปลอดภัยไซเบอร์ และ 5) การให้ความรู้ และทักษะเกี่ยวกับการใช้งานเทคโนโลยีในการรักษาความมั่นคงปลอดภัยไซเบอร์กับผู้ใช้งานทั่วไปภายในองค์กร

7. ข้อเสนอแนะเพิ่มเติม

ควรมีการศึกษา จัดทำรายละเอียด และกระบวนการตรวจสอบประเมินผล ในการปฏิบัติตามแนวทางการเตรียมความพร้อมภายใต้กรอบแนวคิดดังกล่าวนี้เพื่อส่งผลในทางปฏิบัติ

อย่างมีประสิทธิภาพ รวมถึงการวางแผนพัฒนาบุคลากรด้านไซเบอร์ขององค์กรให้เกิดความรู้ ทักษะความสามารถในการวิเคราะห์วางกลยุทธ์ จัดทำแผนงาน และจัดการความเสี่ยงได้อย่างแท้จริง

8. เอกสารอ้างอิง

[1] T. Sirikunakronkun. *Cyber Security: Work from Home Model.* An Independent Study Submitted in Partial Fulfillment of the requirement for the Joint Advanced Course, Joint War College, National Defense Studies Institute, 2020.

[2] A. Prateapusanond, and T. Kalyanamitra. "Thai Military Development Guideline on Cyber Security". *National Defense Studies Institute Journal,* Vol. 8, No. 3, pp. 11-23, September-December, 2017.

[3] A. Kaewsa-ard, and N. Utakrit. "Cyber Security Risk Management Guidance for Enterprise". *National Defense Studies Institute Journal,* Vol. 12, No. 1, pp. 6-20, January-April, 2017.

[4] P. Wuttidittachotti, K. Chanloi, and S. Kijtongpool. *CYBER SECURITY Don't ever let somebody use your personal information.* Bangkok: Amarin Printing and Publishing Public Company Limited, 2022.

[5] Office of the Council of State, *Cybersecurity Act, B.E. 2562 (2019).* Available online at https://bit.ly/41Gz7oG, accessed on 3 March 2023.

[6] Thai Government Gazette, *Notifications of National Cyber Security Committee B.E.2564 (2021).* Available online at https://bit.ly/3J6jNKP, accessed on 3 March 2023.

[7] National Cyber Security Agency (NCSA). *The Result of the Cybersecurity Readiness Assessment Survey for Critical Information Infrastructure (CII), Regulators and Government Agencies.* Bangkok: National Cyber Security Agency (NCSA), 2022.

[8] N. Utakrit, and N. Utakrit. "Similarity and Dissimilarity between Information Security and Assurance". *Information Technology Journal,* Vol. 17, No. 2, pp. 46-56, July-December, 2021.

[9] H. Liang, and Y. Xue. "Avoidance of Information Technology Threats: A Theoretical Perspective". *MIS Quarterly,* Vol. 33, No. 1, pp. 71–90, 2009.

[10] D. E. Stern, C. W. Lamb, and D. L. MacLachlan. "Perceived Risk: A Synthesis". *European Journal of Marketing,* Vol. 11, No. 4, pp. 312-319, 1977. https://doi.org/10.1108/EUM0000000005017

[11] D. Littler, and D. Melanthiou. "Consumer perceptions of risk and uncertainty and the implications for behavior towards innovative retail services: The case of Internet Banking". *Journal of Retailing and Consumer Services,* Vol. 13, No. 6, pp. 431-443, November, 2006.

[12] M. Lee. "Factors influencing the adoption of Internet banking: An integration of TAM and TPB with perceived risk and perceived benefit". *Electronic Commerce Research and Applications,* Vol. 8, No. 3, pp. 130-141, May, 2009.

[13] H. Liang, and Y. Xue. "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective". *Journal of the Association for Information Systems,* Vol. 11, No. 7, pp. 394-413, July, 2010.

[14] D. Q. Chen, and H. Liang. "Wishful Thinking and IT Threat Avoidance: An Extension to the Technology Threat Avoidance Theory". *IEEE Transactions on Engineering Management,* Vol. 66, No. 4, pp. 552-567, November, 2019.

[15] T. Daengsi, P.Pornpongtechavanich, and P. Wuttidittachotti. "Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks". *Education and Information Technologies,* Vol. 27, No. 4, pp. 4729-4752, May, 2022.

[16] NIST, *Cyber Security Framework Version 1.1 Framework for Improving Critical Infrastructure Cybersecurity.* Available Online at https://www.nist.gov/cyberframework, accessed on 29 October 2022.

[17] S. Malisuwan. *Cyber Security Strategy A Guideline and Recommendation.* Available Online at https://bit.ly/3lF2KpT, accessed on 29 October 2022.

[18] THE WHITE HOUSE Office of the Press Secretary, *President Policy Practice: Critical Infrastructure Security and Resilience (PPD-21).* Available online at https://bit.ly/3k9c05w, accessed on 29 October 2022.

[19] P. Hom-anek. *Strategy to Cyber Security 4.0.* Bangkok: WACHARIN P.P. PRINTING CO., LTD., 2017.

[20] National Initiative for Cybersecurity Careers and Studies (NICSS), *Workforce Framework for Cybersecurity (NICE Framework).* Available online at https://niccs.cisa.gov/workforce-development/nice-framework, accessed on 29 October 2022.

[21] National Initiative for Cybersecurity Education (NICE) Applied Cybersecurity Division Information Technology Laboratory, *NIST Special Publication 800-181 Workforce Framework for Cybersecurity.* Available Online at https://bit.ly/3IbDsYm, accessed on 29 October 2022.

[22] United States Government Accountability Office (GAO), *Report to Congressional Committee: Cyber Security Workforce (2019).* Available Online at https://www.gao.gov/products/gao-19-144, accessed on 29 October 2022.

[23] SANS, *Cyber Security Skills Roadmap.* Available online at https://bit.ly/3xeVyU2,accessed on 29 October 2022.

[24] SANS, *Security Awareness Maturity Model.* Available online at https://www.sans.org/cybersecurity-leadership/, accessed on 29 October 2022.

[25] Health Technical Office, "Recommendation for Author." *Journal of Health Science,* Vol. 11, No. 4, July-August, 2002.