ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากร ในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร
Cyber Security Awareness of Employees in One Private Company in Bangkok Area

เมธาพร ธรรมศิริ[1]
ศิรภัสสรศ์ วงศ์ทองดี[2]

บทคัดย่อ

การวิจัยเรื่อง “ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร” มีวัตถุประสงค์ (1) เพื่อศึกษาระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร และ (2) เพื่อเปรียบเทียบระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร จำแนกตามปัจจัยส่วนบุคคล โดยเป็นการวิจัยเชิงปริมาณ มีรูปแบบการวิจัยในเชิงสำรวจ ใช้แบบสอบถามเป็นเครื่องมือในการวิจัย ประชากรคือบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร กำหนดกลุ่มตัวอย่างจำนวน 170 คน

ผลการศึกษาพบว่า บุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร มีความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์อยู่ในระดับมาก โดยเมื่อจำแนกตามปัจจัยส่วนบุคคลพบว่าบุคลากรในบริษัทเอกชนแห่งนี้ที่มี เพศ อายุ และประสบการณ์การทำงาน (อายุงาน) ที่ต่างกันมีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ที่ไม่แตกต่างกัน และในส่วนบุคลากรที่มีระดับการศึกษาสูงสุด แผนกที่สังกัด และประสบการณ์เกี่ยวกับความมั่นคง

[1] นักศึกษาหลักสูตรรัฐประศาสนศาสตร์มหาบัณฑิต มหาวิทยาลัยธุรกิจบัณฑิตย์
[2] รองศาสตราจารย์ ดร. มหาวิทยาลัยธุรกิจบัณฑิตย์

ปลอดภัยทางไซเบอร์ ที่ต่างกัน มีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ที่แตกต่างกันอย่างมีนัยสำคัญทางสถิติ

คำสำคัญ: ความตระหนักรู้, ภัยคุกคามทางไซเบอร์, ความมั่นคงปลอดภัยทางไซเบอร์

Abstract

The purpose of the "Cyber Security Awareness of Employees in One Private Company in Bangkok Area" were to (1) study the level of cyber security awareness of employees in one private company in Bangkok area and (2) to compare their level of awareness regarding cyber security of employees in one private company in Bangkok area, classified by subjective factors. This research is a quantitative research with and exploratory research model, using questionnaires as a research tool. The population utilized in this research includes the employees in one private company in Bangkok area, with a determined sample group of 170 people.

The results of the research on cyber security awareness level revealed that employees in one private company in Bangkok area had a high level of cyber security awareness. Regarding the personal factors, it was found that employees in this private company with different genders, ages, and work experience had the same level of awareness against cyber security. Employees in this private company with different highest level of educations, departments, and cyber threat-related experiences had different levels of awareness against cyber security.

Keywords: Awareness, Cyber Threats, Cyber Security

บทนำ

ในปัจจุบันองค์กรภาครัฐและเอกชนมีการนำเอาเทคโนโลยีสารสนเทศมาใช้ในการปฏิบัติงานกันอย่างแพร่หลายเพื่ออำนวยความสะดวกและเพิ่มขีดความสามารถในการดำเนินกิจกรรมขององค์กรไม่ว่าจะเป็นการใช้งานเครื่องคอมพิวเตอร์ภายในสำนักงาน การใช้งานเครื่องคอมพิวเตอร์แม่ข่ายเพื่อการประมวลผล รวมไปถึงการเชื่อมต่อระบบคอมพิวเตอร์เข้ากับระบบเครือข่ายเพื่อสร้างการสื่อสารทั้งภายในและภายนอกองค์กร ซึ่งในองค์กรบางแห่งอาจจะมีการพึ่งพาระบบสารสนเทศเป็นแกนหลักเพื่อให้กิจกรรมขององค์กรสามารถดำเนินไปได้ โดยการที่องค์กรจำนวนมากหันมาใช้งานเทคโนโลยีสารสนเทศในการดำเนินงานกันมากขึ้น รวมถึงการทำงานจากที่บ้านได้รับความนิยมเพิ่มมากขึ้น ส่งผลให้องค์กรต่าง ๆ มีโอกาสที่จะตกเป็นเหยื่อจากการโจมตีทางไซเบอร์มากขึ้นตามไปด้วย ซึ่งการโจมตีทางไซเบอร์เป็นภัยคุกคามที่ส่งผลกระทบโดยตรงต่อความมั่นคงปลอดภัยระบบสารสนเทศขององค์กร มีโอกาสที่จะทำให้การดำเนินงานขององค์กรต้องหยุดชะงัก สร้างความเสียหายทางการเงิน ทำลายความน่าเชื่อถือและชื่อเสียงขององค์กร โดยในการศึกษาของบริษัท IBM พบว่าร้อยละ 95 ของการละเมิดทางไซเบอร์มีสาเหตุมาจากความผิดพลาดที่เกิดจากการกระทำของบุคคลซึ่งอาจจะเกิดขึ้นได้ในหลายลักษณะ เช่น บุคลากรบางคนตั้งค่ารหัสผ่านในการเข้าใช้งานระบบที่มีความสำคัญขององค์กรในลักษณะที่ง่ายต่อการคาดเดา หรือหลงเชื่ออีเมลหลอกลวง (Phishing Email) ทำให้ถูกหลอกเอาข้อมูลที่มีความสำคัญไป เป็นต้น

จากข้อมูลดังกล่าวข้างต้นจะเห็นได้ว่าบุคลากรถือเป็นปัจจัยสำคัญที่ส่งผลต่อความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร แม้ว่าองค์กรจะมีการลงทุนจัดซื้ออุปกรณ์และเครื่องมือเพื่อใช้ในการรักษาความปลอดภัยทางไซเบอร์มากเท่าใดแต่ถ้าบุคลากรขาดความรู้และไม่ตระหนักถึงความสำคัญของการรักษาความปลอดภัยทางไซเบอร์ก็อาจส่งผลให้องค์กรตกอยู่ในความเสี่ยงที่จะถูกโจมตีได้โดยง่าย ดังนั้นผู้ศึกษาจึงได้ทำการศึกษาความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานครเพื่อใช้เป็นกรณีศึกษาในการพัฒนาแนวทางในการกำหนดนโยบายด้านความมั่นคงปลอดภัยทางไซเบอร์และออกแบบการฝึกอบรมเพื่อสร้างความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์

วัตถุประสงค์

1. เพื่อศึกษาระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร

2. เพื่อเปรียบเทียบระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร จำแนกตามปัจจัยส่วนบุคคล

แนวคิด ทฤษฎีและวรรณกรรมที่เกี่ยวข้อง

แนวคิดเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) สรุปได้ว่า ความมั่นคงปลอดภัยทางไซเบอร์หมายถึง วิธีการ มาตรการ หรือการดำเนินการใด ๆ เพื่อป้องกัน รับมือ บรรเทา และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีผลต่อปัจจัยการรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของอุปกรณ์และข้อมูลภายในระบบสารสนเทศ ซึ่งหากการรักษาความมั่นคงปลอดภัยทางไซเบอร์มีความอ่อนแออาจทำให้ผู้ประสงค์ร้ายสามารถสร้างความเสียหายต่อตัวผู้ใช้งานและข้อมูลส่วนบุคคลของผู้ใช้งานได้ (สพธอ., 2564) โดยสามารถพัฒนาขีดความสามารถในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้หลายวิธี เช่น การใช้รหัสผ่านที่ยากต่อการคาดเดา การติดตั้งใช้งานซอฟต์แวร์แอนตี้ไวรัส เป็นต้น (CISA, 2019)

แนวคิดเกี่ยวกับภัยคุกคามทางไซเบอร์ (Cyber Threat) สรุปได้ว่า ภัยคุกคามทางไซเบอร์หมายถึง เหตุการณ์หรือสถานการณ์ใด ๆ ซึ่งส่งผลเสียและอาจจะสร้างความเสียหายต่อปัจจัยทางด้านการรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศหรือข้อมูลของทั้งปัจเจกบุคคล องค์กร หรือประเทศชาติ ซึ่งภัยคุกคามทางไซเบอร์มีแหล่งที่มาจากอาชญากรไซเบอร์และผู้คุกคามที่มีรัฐหนุนหลังเป็นส่วนใหญ่ (Sailio et al., 2020) โดยประเภทของภัยคุกคามทางไซเบอร์ที่สำคัญ ๆ ได้แก่ มัลแวรีเรียกค่าไถ่ มัลแวร์ และภัยคุกคามที่เกี่ยวกับอีเมล เป็นต้น (ENISA, 2021)

แนวคิด ทฤษฎีที่เกี่ยวข้องกับความตระหนักรู้ (Awareness) โดย Bloom. (1997, p.213, อ้างถึงใน วาสนา อุทัยแสง, 2559, น.8) ให้ความหมายของความตระหนักรู้เอาไว้ว่า เป็นขั้นต่ำสุดของภาคอารมณ์และความรู้สึก (Affective Domain) ความตระหนักรู้มีความคล้ายกับความรู้เป็นอย่างมากในส่วนที่ความรู้และความตระหนักนั้นไม่ถือว่าเป็นสิ่งเร้า ความตระหนักรู้ไม่จำเป็นต้องเน้นปรากฏการณ์หรือสิ่งใดสิ่งหนึ่งและจะเกิดขึ้นก็ต่อเมื่อมีสิ่งเร้ามาเป็นตัวกระตุ้นให้เกิดความตระหนักรู้ โดยที่ Good (1973, p.54 อ้างถึงใน ดวงฤดี กิตติจารุดุลย์, 2557, น. 10-11) กล่าวเอาไว้ว่า การเกิดความตระหนักรู้เป็นผลลัพธ์จากกระบวนการทางปัญญา (Cognitive Process) ซึ่งหมายถึง หากบุคคลถูกกระตุ้นจากสิ่งเร้าหรือได้สัมผัสกับสิ่งเร้าจะทำให้เกิดความรู้ และเมื่อรับรู้แล้วลำดับถัดไปก็คือจะมีความเข้าใจในสิ่งนั้นจนเกิดความคิดรวบยอดที่นำไปสู่การเรียนบังเกิดเป็นความรู้ (Knowledge) ซึ่งนำไปสู่ความตระหนักรู้ (Awareness) ในท้ายที่สุด โดยทั้งความตระหนักรู้และความรู้จะผลักดันการแสดงออกของพฤติกรรมหรือการกระทำของบุคคลต่อสิ่งเร้านั้น ๆ

สมมติฐานของการวิจัย

บุคลากรที่มีปัจจัยส่วนบุคคลที่ต่างกัน ได้แก่ เพศ อายุ ระดับการศึกษาสูงสุด แผนกที่สังกัด ประสบการณ์การทำงาน (อายุงาน) และประสบการณ์เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ มีความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ในระดับที่แตกต่างกัน

ขอบเขตของการวิจัย

ในการศึกษาครั้งนี้ ได้กำหนดขอบเขตของการวิจัยในประเด็นต่าง ๆ ดังนี้

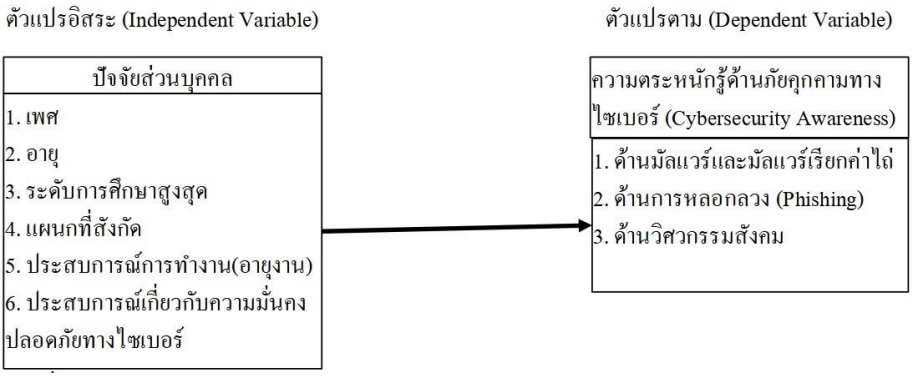
1. ขอบเขตด้านประชากรและพื้นที่ ประชากรที่ใช้ในการวิจัยนี้ คือ บุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร จำนวน 228 คน โดยกำหนดขนาดตัวอย่างจำนวนทั้งสิ้น 170 คน

2. ขอบเขตด้านเนื้อหา ศึกษาระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร

3. ขอบเขตด้านระยะเวลา วิจัยโดยรวบรวมข้อมูลระหว่างเดือนมกราคม - กุมภาพันธ์ พ.ศ. 2565

กรอบแนวคิดในการวิจัย

จากการศึกษาแนวคิดและทฤษฎี รวมถึงงานวิจัยที่เกี่ยวข้อง ผู้ศึกษาได้กำหนดแนวความคิดไว้ดังนี้



ภาพที่ 1 กรอบแนวคิดการวิจัย

วิธีการวิจัย

ประชากรที่ใช้ในการวิจัยครั้งนี้คือ บุคลากรจากทุกแผนกของบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร ยกเว้นผู้บริหารระดับสูง จำนวน 228 คน โดยใช้สูตรการหาขนาดตัวอย่างตามหลักการของยามาเน่ (Taro Yamane, 1973) โดยกำหนดระดับความเชื่อมั่นที่ 95% และความคลาดเคลื่อนที่ 5% พบว่าได้ขนาดประชากรจำนวน 146 คน เก็บจริง 142 คน จึงเพียงพอในการใช้เป็นตัวแทนการวิจัย และสุ่มตัวอย่างแบบชั้นภูมิ (Proportional Stratified Random Sampling) และสุ่มอย่าง่ายเพื่อให้ได้จำนวนกลุ่มตัวอย่างตามสัดส่วนของขนาดกลุ่มประชากร ผู้วิจัยได้ศึกษาค้นคว้าจากทฤษฎีนักวิชาการ และนักปฏิบัติที่ได้เขียนไว้เพื่อนำมาเป็นข้อมูลในการสร้างแบบสอบถาม ซึ่งผู้วิจัยได้เสนอแบบสอบถามที่สร้างขึ้นต่อ

อาจารย์ที่ปรึกษา เพื่อตรวจสอบความครบถ้วนของเนื้อหา (Content Validity) ของแบบสอบถามในเรื่องที่จะศึกษา และมีการตรวจสอบความเชื่อมั่น (Reliability) โดยใช้สถิติค่าสัมประสิทธิ์อัลฟาของครอนบาช (Cronbach's Alpha Coefficient) ของคำถามแต่ละด้าน โดยแบบสอบถามแบ่งเป็น 3 ตอน คือ

ตอนที่ 1 เป็นแบบสอบถามเกี่ยวกับปัจจัยส่วนบุคคลของกลุ่มตัวอย่าง ได้แก่ เพศ อายุ ระดับการศึกษาสูงสุด แผนกที่สังกัด ประสบการณ์การทำงาน (อายุงาน) และประสบการณ์เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ จำนวน 6 ข้อ

ตอนที่ 2 เป็นแบบสอบถามเกี่ยวกับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Cyber Security) มีทั้งหมด 3 ด้าน ได้แก่ ด้านที่ 1 ความตระหนักรู้เกี่ยวกับมัลแวร์และมัลแวร์เรียกค่าไถ่ (Malware/Ransomware Awareness) ด้านที่ 2 ความตระหนักรู้เกี่ยวกับการหลอกลวง (Phishing) ด้านที่ 3 ความตระหนักรู้เกี่ยวกับวิศวกรรมสังคม (Social Engineering) จำนวนรวมทั้งหมด 15 ข้อ โดยใช้มาตรส่วนประเมินค่าคะแนน (Rating Scale) ตามแบบของ Likert Scale มีทางเลือกตอบได้ 5 ระดับ โดยมีเกณฑ์การให้คะแนนดังนี้ ระดับ 1 = เห็นด้วยน้อยที่สุด ระดับที่ 2 = เห็นด้วยน้อย ระดับที่ 3 = เห็นด้วยปานกลาง ระดับที่ 4 = เห็นด้วยมาก และระดับที่ 5 = เห็นด้วยมากที่สุด

ตอนที่ 3 เป็นแบบสอบถามเพื่อรับฟังข้อเสนอแนะเพิ่มเติม

การวิจัยครั้งนี้ใช้การวิเคราะห์ข้อมูลโดยโปรแกรมทางสถิติสำเร็จรูป และระดับความเชื่อมั่นที่ระดับ 0.05 เป็นเกณฑ์ในการยอมรับหรือปฏิเสธสมมติฐานในการวิจัย ใช้สถิติในการวิเคราะห์ข้อมูลคือ สถิติเชิงพรรณนา (Descriptive Statistics) ได้แก่ ค่าความถี่ (Frequency) ค่าร้อยละ (Percentage) ค่าเฉลี่ย (Mean) และค่าส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) สถิติเชิงอนุมาน (Inferential Statistics) ได้แก่ค่า t-Test และ F-Test (ANOVA)

ผลการวิจัย

ผลการวิเคราะห์ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม พบว่า กลุ่มตัวอย่างเป็นเพศหญิง จำนวน 75 คน คิดเป็นร้อยละ 52.8 และเป็นเพศชาย จำนวน 67 คน คิดเป็นร้อยละ 47.2 อายุ กลุ่มตัวอย่างส่วนใหญ่มีอายุ 25-35 ปี จำนวน 76 คน คิดเป็นร้อยละ 53.5 อายุ 36-45 ปี จำนวน 30 คน คิดเป็นร้อยละ 21.1 อายุต่ำกว่า 25 ปี จำนวน 21 คน คิดเป็นร้อยละ 14.8 และอายุ 46-55 ปี จำนวน 15 คน คิดเป็นร้อยละ 10.6 ตามลำดับ สำหรับศึกษาครั้งนี้ไม่มีกลุ่มตัวอย่างที่มีอายุตั้งแต่ 56 ปีขึ้นไป ระดับการศึกษาสูงสุด พบว่ากลุ่มตัวอย่างส่วนใหญ่จบการศึกษาสูงสุดในระดับปริญญาตรี จำนวน 94 คน คิดเป็นร้อยละ 66.2 ระดับต่ำกว่าปริญญาตรี จำนวน 41 คน คิดเป็นร้อยละ 28.9 และปริญญาโท จำนวน 7 คน คิดเป็นร้อยละ 4.9 ตามลำดับ สำหรับการศึกษาครั้งนี้ไม่มีกลุ่มตัวอย่างที่มีระดับการศึกษาสูงกว่าปริญญาโท แผนกที่สังกัด พบว่ากลุ่มตัวอย่างส่วนใหญ่สังกัดในแผนกประกันคุณภาพ (QA) จำนวน 23 คน คิดเป็นร้อยละ 16.2 รองลงมาได้แก่แผนกวิศวกรรมเครื่องกล (Plant Engineer) จำนวน 20 คน คิดเป็นร้อยละ 14.1 แผนกบรรจุ (Packing) จำนวน 18 คน คิดเป็นร้อยละ 12.7 แผนกผลิต (MFG) จำนวน 14 คน คิดเป็นร้อยละ 9.9 แผนกขนส่ง (Transfore) จำนวน 13 คน คิดเป็นร้อยละ 9.2 แผนกบริการลูกค้า (CSC) จำนวน 13 คน คิดเป็นร้อยละ 9.2 แผนกจัดซื้อ (PU) จำนวน 12 คน คิดเป็นร้อยละ 8.5 แผนกออกแบบเคเบิล (CDD) จำนวน 9 คน คิดเป็นร้อยละ 6.3 แผนกทรัพยากรบุคคล (HR) จำนวน 8 คน คิดเป็นร้อยละ 5.6 แผนกบัญชี (Accounting) จำนวน 8 คน คิดเป็นร้อยละ 5.6 และแผนกกระบวนการ (Process) จำนวน 4 คน คิดเป็นร้อยละ 2.8 ตามลำดับ ประสบการณ์การทำงาน (อายุงาน) พบว่ากลุ่มตัวอย่างส่วนใหญ่มีประสบการณ์การทำงาน (อายุงาน) ในระดับ 1-3 ปี จำนวน 55 คน คิดเป็นร้อยละ 38.7 ระดับ 4-6 ปี จำนวน 43 คน คิดเป็นร้อยละ 30.3 ระดับต่ำกว่า 1 ปี จำนวน 18 คน คิดเป็นร้อยละ 12.7 ระดับมากกว่า 10 ปี จำนวน 14 คน คิดเป็นร้อยละ 9.9 และระดับ 7-9 ปี จำนวน 12 คน คิดเป็นร้อยละ 8.5 ตามลำดับ ประสบการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ พบว่ากลุ่มตัวอย่างส่วนใหญ่เคยมีประสบการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ จำนวน 78 คน คิดเป็นร้อยละ 54.9 โดยแบ่งเป็น เคยถูก

โจมตีทางไซเบอร์ เช่น คอมพิวเตอร์ติดไวรัสหรือได้รับอีเมลหลอกลวง จำนวน 51 คน คิดเป็นร้อยละ 35.9 เคยได้รับคำเตือนให้ระวังภัยทางไซเบอร์ผ่านสื่อต่าง ๆ เป็นประจำ จำนวน 46 คน คิดเป็นร้อยละ 32.4 และเคยได้รับการอบรมเสริมสร้างความตระหนักรู้ทางไซเบอร์อย่างสม่ำเสมอ จำนวน 16 คน คิดเป็นร้อยละ 16 ตามลำดับ

ผลการวิเคราะห์ระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร พบว่า ในภาพรวมกลุ่มตัวอย่างมีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์อยู่ในระดับมาก มีค่าเฉลี่ยเท่ากับ 3.85 และมีค่าส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.61 เมื่อพิจารณาเป็นรายด้านพบว่า ด้านความตระหนักรู้เกี่ยวกับมัลแวร์และมัลแวร์เรียกค่าไถ่ (Malware/Ransomware Awareness) เป็นด้านที่มีค่าเฉลี่ยสูงสุดอยู่ในระดับ 3.91 รองลงมา คือด้านความตระหนักรู้เกี่ยวกับวิศวกรรมสังคม (Social Engineering Awareness) มีค่าเฉลี่ยเท่ากับ 3.85 และด้านความตระหนักรู้เกี่ยวกับการหลอกลวง (Phishing Awareness) มีค่าเฉลี่ยเท่ากับ 3.81 ตามลำดับ

ผลการทดสอบสมมติฐาน

ผลการทดสอบสมมติฐานบุคลากรที่มีปัจจัยส่วนบุคคลที่ต่างกัน ได้แก่ เพศ อายุ ระดับการศึกษาสูงสุด แผนกที่สังกัด ประสบการณ์การทำงาน (อายุงาน) และประสบการณ์เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ มีความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ในระดับที่แตกต่างกัน โดยใช้สถิติในการวิเคราะห์คือ t-Test และค่า F-test ที่ระดับความเชื่อมั่น 95% มีดังต่อไปนี้

1. ผลการทดสอบสมมติฐานระหว่างเพศกับระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ พบว่า ค่า Sig. ของตัวแปรทุกคู่ที่ทดสอบมีค่ามากกว่า 0.05 ดังนั้นจึงสรุปได้ว่าบุคลากรของบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานครที่มีเพศต่างกันมีความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ในระดับที่ไม่แตกต่างกัน

2. ผลการทดสอบสมมติฐานระหว่างอายุกับระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ พบว่า ค่า Sig. ของตัวแปรทุกคู่ที่ทดสอบมีค่ามากกว่า 0.05 ดังนั้นจึงสรุปได้ว่า

บุคลากรของบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานครที่มีอายุต่างกันมีความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ในระดับที่ไม่แตกต่างกัน

3. ผลการทดสอบสมมติฐานระหว่างระดับการศึกษาสูงสุดกับระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ พบว่า ค่า Sig. ของตัวแปรทุกคู่ที่ทดสอบมีค่าน้อยกว่า 0.05 ดังนั้นจึงสรุปได้ว่า บุคลากรของบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานครที่มีระดับการศึกษาสูงสุดต่างกันมีความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ในระดับที่แตกต่างกัน

4. ผลการทดสอบสมมติฐานระหว่างแผนกที่สังกัดกับระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ พบว่า ค่า Sig. ของตัวแปรทุกคู่ที่ทดสอบมีค่าน้อยกว่า 0.05 ดังนั้นจึงสรุปได้ว่า บุคลากรของบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานครที่สังกัดแผนกต่างกันมีความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ในระดับที่แตกต่างกัน

5. ผลการทดสอบสมมติฐานระหว่างประสบการณ์การทำงาน (อายุงาน) กับระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ พบว่า ค่า Sig. ของตัวแปรทุกคู่ที่ทดสอบมีค่ามากกว่า 0.05 ดังนั้นจึงสรุปได้ว่า บุคลากรของบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานครที่มีประสบการณ์การทำงาน (อายุงาน) ต่างกันมีความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ในระดับที่ไม่แตกต่างกัน

6. ผลการทดสอบสมมติฐานระหว่างประสบการณ์เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์กับระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ ในหัวข้อ เคยได้รับการอบรมเสริมสร้างความตระหนักรู้ทางไซเบอร์อย่างสม่ำเสมอ พบว่า ค่า Sig. ของ 2 ตัวแปร ได้แก่ ตัวแปรด้านความตระหนักรู้เกี่ยวกับมัลแวร์และมัลแวร์เรียกค่าไถ่ (Malware/Ransomware Awareness) และตัวแปรด้านความตระหนักรู้เกี่ยวกับการหลอกลวง (Phishing Awareness) มีค่าน้อยกว่า 0.05 ดังนั้นจึงสรุปได้ว่า บุคลากรของบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานครที่มีประสบการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ ในหัวข้อเคยได้รับการอบรมเสริมสร้างความตระหนักรู้ทางไซเบอร์อย่างสม่ำเสมอ มีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ในด้านความตระหนักรู้เกี่ยวกับมัลแวร์และมัลแวร์เรียกค่าไถ่ (Malware/Ransomware Awareness) และด้านความตระหนักรู้เกี่ยวกับการ

หลอกลวง (Phishing Awareness) ที่ต่างกัน แต่มีระดับความตระหนักรู้ด้านความตระหนักรู้เกี่ยวกับวิศวกรรมสังคม (Social Engineering Awareness) ที่ไม่แตกต่างกัน หัวข้อ เคยถูกโจมตีทางไซเบอร์ เช่น คอมพิวเตอร์ติดไวรัสหรือได้รับอีเมลหลอกลวง พบว่า ค่า Sig. ของ 1 ตัวแปร คือ ตัวแปรด้านความตระหนักรู้เกี่ยวกับวิศวกรรมสังคม (Social Engineering Awareness) มีค่าน้อยกว่า 0.05 ดังนั้นจึงสรุปได้ว่า บุคลากรของบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานครที่มีประสบการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ ในหัวข้อ เคยถูกโจมตีทางไซเบอร์ เช่น คอมพิวเตอร์ติดไวรัสหรือได้รับอีเมลหลอกลวง มีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ในด้านความตระหนักรู้เกี่ยวกับวิศวกรรมสังคม (Social Engineering Awareness) ที่ต่างกัน แต่มีระดับความตระหนักรู้ด้านความตระหนักรู้เกี่ยวกับมัลแวร์และมัลแวร์เรียกค่าไถ่ (Malware/Ransomware Awareness) และด้านความตระหนักรู้เกี่ยวกับการหลอกลวง (Phishing Awareness) ที่ไม่แตกต่างกัน หัวข้อ เคยได้รับคำเตือนให้ระวังภัยทางไซเบอร์ผ่านสื่อต่าง ๆ เป็นประจำ พบว่า ค่า Sig. ของ 2 ตัวแปร ได้แก่ ตัวแปรด้านความตระหนักรู้เกี่ยวกับการหลอกลวง (Phishing Awareness) และตัวแปรด้านความตระหนักรู้เกี่ยวกับวิศวกรรมสังคม (Social Engineering Awareness) มีค่าน้อยกว่า 0.05 ดังนั้นจึงสรุปได้ว่า บุคลากรของบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานครที่มีประสบการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ ในหัวข้อ เคยได้รับคำเตือนให้ระวังภัยทางไซเบอร์ผ่านสื่อต่าง ๆ เป็นประจำ มีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ในด้านความตระหนักรู้เกี่ยวกับการหลอกลวง (Phishing Awareness) และด้านความตระหนักรู้เกี่ยวกับวิศวกรรมสังคม (Social Engineering Awareness) ที่ต่างกัน แต่มีระดับความตระหนักรู้ด้านความตระหนักรู้เกี่ยวกับมัลแวร์และมัลแวร์เรียกค่าไถ่ (Malware/Ransomware Awareness) ที่ไม่แตกต่างกัน หัวข้อ ไม่เคยมีประสบการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ พบว่า ค่า Sig. ของ 2 ตัวแปร ได้แก่ ตัวแปรด้านความตระหนักรู้เกี่ยวกับการหลอกลวง (Phishing Awareness) และตัวแปรด้านความตระหนักรู้เกี่ยวกับวิศวกรรมสังคม (Social Engineering Awareness) มีค่าน้อยกว่า 0.05 ดังนั้นจึงสรุปได้ว่า บุคลากรของบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานครที่มี

ประสบการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ ในหัวข้อ ไม่เคยมีประสบการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ มีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ในด้านความตระหนักรู้เกี่ยวกับการหลอกลวง (Phishing Awareness) และด้านความตระหนักรู้เกี่ยวกับวิศวกรรมสังคม (Social Engineering Awareness) ที่ต่างกัน แต่มีระดับความตระหนักรู้ด้านความตระหนักรู้เกี่ยวกับมัลแวร์และมัลแวร์เรียกค่าไถ่ (Malware/Ransomware Awareness) ที่ไม่แตกต่างกัน

อภิปรายผล

จากผลการวิจัยในส่วนของระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานครที่พบว่า กลุ่มตัวอย่างมีความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ในภาพรวมอยู่ในระดับมาก สอดคล้องกับ สุธาเทพ รุณเรศ (2561) ได้วิจัยเรื่อง ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร พบว่า ในภาพรวมกลุ่มตัวอย่างมีความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์ในระดับมากเช่นเดียวกัน ทั้งนี้เป็นเพราะบริษัทเอกชนแห่งนี้ได้รับการรับรองมาตรฐานที่สำคัญหลายรายการซึ่งมีส่วนที่เกี่ยวข้องกับการบริหารจัดการระบบสารสนเทศเพื่อตอบสนองต่อความต้องการด้านมาตรฐานของคู่ค้า อีกทั้งมีกระบวนการให้ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์แก่บุคลากรเป็นระยะ ๆ ทำให้บุคลากรมีความรู้ความเข้าใจในการใช้งานเทคโนโลยีสารสนเทศเป็นอย่างดี แต่หากพิจารณาเป็นรายด้านจะพบว่า กลุ่มตัวอย่างมีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์เกี่ยวกับการหลอกลวง (Phishing Awareness) ต่ำที่สุดจากทั้งหมด 3 ด้าน ซึ่งมีสาเหตุเพราะในการโจมตีด้วยวิธีการหลอกลวง (Phishing) เป็นการโจมตีซึ่งแสวงประโยชน์จากสถาวะจิตใจและพฤติกรรมของมนุษย์ (ENISA, 2021) จึงทำให้ยากแก่การป้องกัน

ผลการวิจัยในส่วนของปัจจัยส่วนบุคคลที่พบว่า บุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานครที่มี เพศ อายุ และประสบการณ์การทำงาน (อายุงาน) ที่ต่างกันมีระดับ

ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ที่ไม่แตกต่างกันนั้นเนื่องมาจากในปัจจุบันประชาชนไม่ว่าจะเป็นเพศใด มีอายุหรือประสบการณ์การทำงาน (อายุงาน) เท่าใดก็สามารถเข้าถึงและใช้งานอินเตอร์เน็ตได้อย่างเท่าเทียมกันซึ่งเป็นปัจจัยหนึ่งที่ส่งผลให้เกิดความตระหนักรู้ตามที่ กุลวดี ราชภักดี (2545, น.38) กล่าวเอาไว้ว่า ความตระหนัก หมายถึง การที่บุคคลเกิดความรู้สึก นึกคิด ความคิดเห็นหรือประสบการณแล้วเกิดความเข้าใจแล้วประเมินสถานการณที่เกี่ยวกับตนเองได้จากสภาวะจิตที่ยอมรับและเกิดแสดงพฤติกรรมตอบสนองต่อเหตุการณ์ ดังนั้นเพศ อายุ และประสบการณ์การทำงาน (อายุงาน) จึงไม่ใช่ข้อจำกัดที่จะทำให้โอกาสในการเรียนรู้หรือการสร้างความคุ้นเคยเกี่ยวกับความปลอดภัยในการใช้งานอินเตอร์เน็ตของผู้ตอบแบบสอบถามเกิดความแตกต่างกันได้ และในส่วนของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานครที่มีระดับการศึกษาสูงสุด แผนกที่สังกัด และประสบการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ ที่แตกต่างกันมีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ที่แตกต่างกัน แยกอธิบายได้ว่า ในส่วนของระดับการศึกษาสูงสุดนั้น ถือว่าเป็นองค์ประกอบสำคัญในกระบวนการที่ทำให้เกิดความตระหนักรู้ตามที่ Good (1973, p.54 อ้างถึงใน ดวงฤดี กิตติจารุดุลย์, 2557, น. 10-11) กล่าวเอาไว้ว่าการเกิดความตระหนักรู้เป็นผลลัพธ์จากกระบวนการทางปัญญา (Cognitive Process) ซึ่งหมายถึงหากบุคคลถูกกระตุ้นจากสิ่งเร้าที่ช่วยกระตุ้นบุคคลทำให้เกิดความรู้จนมีความเข้าใจในสิ่งนั้นนำไปสู่การเรียนบังเกิดเป็นความรู้ (Knowledge) และนำไปสู่ความตระหนักรู้ (Awareness) ดังนั้น ระดับการศึกษาสูงสุดของบุคลากรที่ต่างกันจึงทำให้เกิดความแตกต่างของความสามารถทางด้านการเรียนรู้และความตระหนักรู้ดังจะเห็นได้จากการที่บุคลากรที่มีระดับการศึกษาสูงสุดในระดับปริญญาโทมีค่าเฉลี่ยความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์สูงกว่าระดับต่ำกว่าปริญญาตรีและระดับปริญญาตรีในทุกด้าน ในส่วนของแผนกที่สังกัดเนื่องมาจากบุคลากรในแต่ละแผนกมีระดับการศึกษาที่ต่างกัน รวมทั้งธรรมชาติของการปฏิบัติงานในบางแผนกที่มีโอกาสได้ใช้งานระบบสารสนเทศมากกว่าแผนกอื่น ๆ ทำให้เกิดความคุ้นชิน อีกทั้งในแต่ละแผนกมีโอกาสในการเข้ารับการอบรมเสริมสร้างความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์แตกต่างกัน จึงทำให้บางแผนกมีโอกาสในการเรียนรู้มากกว่า ใน

ส่วนของประสบการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ จะเห็นได้ว่าการที่กลุ่มตัวอย่างได้มีประสบการณ์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์โดยตรงถือว่าเป็นสิ่งเร้าที่เป็นตัวกระตุ้นทำให้เกิดความตระหนักรู้ ดังที่ วาสนา อุทัยแสง (2559, น.8) กล่าวเอาไว้ว่า ความตระหนักรู้เป็นความคิดเห็น ความรู้สึก ความสำนึกถึงความสำคัญ บุคคลจะเกิดความสำนักหรือความตระหนักรู้หากบุคคลนั้นมีการรับรู้หรือเคยรับรู้มาก่อนและได้รับสิ่งเร้ามาเป็นตัวกระตุ้น ดังนั้นบุคลากรที่เคยมีประสบการ์ตรงจึงมีระดับความตระหนักรู้มากกว่า

ข้อเสนอแนะ

ข้อเสนอแนะจากการวิจัยครั้งนี้ จากการวิจัยควรปรับนโยบายด้านความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรโดยกำหนดนโยบายให้มีความสอดคล้องกับพฤติกรรมการใช้งานสื่อสังคมออนไลน์ (Social Media) ของบุคลากร เช่น การออกคำแนะนำในการใช้งานสื่อสังคมออนไลน์อย่างปลอดภัย รวมถึงกำหนดมาตรฐานการตั้งค่ารหัสผ่าน (Password) ให้มีความเข้มแข็งยากต่อการคาดเดา เช่น รหัสผ่านควรมีความยาวมากกว่า 8 อักษร และต้องมีตัวอักษรภาษาอังกฤษทั้งตัวเล็กและตัวใหญ่รวมอยู่ด้วย นอกจากนั้นควรมีการกำหนดมาตรฐานการเข้าใช้งานเว็บไซต์ของบุคลากรให้มีความปลอดภัยมากยิ่งขึ้น เช่น การกำหนดกฎห้ามเข้าใช้งานเว็บไซต์ที่ไม่ได้ทำงานบนโปรโตคอล HTTPS เป็นต้น

องค์กรควรออกแบบการฝึกอบรมเพื่อสร้างความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Cyber Security Awareness Training) เพื่อสร้างความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ให้กับบุคลากร โดยเน้นให้มีเนื้อหาที่เกี่ยวข้องกับภัยคุกคามที่เกิดจากการหลอกลวง (Phishing) เนื่องจากบุคลากรมีระดับความตระหนักรู้ในด้านนี้ต่ำที่สุดจากทั้งสามด้านโดยเฉพาะหัวข้อที่เกี่ยวข้องกับความปลอดภัยในการใช้งานเว็บไซต์บนอินเตอร์เน็ต เช่น วิธีการในการสังเกตว่าเว็บไซต์ใดเป็นเว็บไซต์หลอกลวง การให้ความรู้เกี่ยวกับความแตกต่างระหว่างโปรโตคอล HTTP และ HTTPS นอกจากนั้นควรให้ความสำคัญกับการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์และการฝึกอบรมบุคลากรที่สังกัดอยู่ในแผนกประกันคุณภาพ (QA) รวมถึงบุคลากรที่มีระดับการศึกษาสูงสุดต่ำกว่าปริญญาตรี

เนื่องจากบุคลากรในกลุ่มนี้มีระดับความตระหนักรู้ต่ำที่สุดเมื่อเทียบกับบุคลากรกลุ่มอื่น ๆ ภายในบริษัท นอกจากนั้นควรเพิ่มช่องทางและความถี่ในการแจ้งเตือนข่าวสารที่เกี่ยวกับภัยคุกคามทางไซเบอร์ให้กับบุคลากรอย่างสม่ำเสมอเนื่องจากเป็นวิธีการที่สามารถสร้างความตระหนักรู้ได้อย่างมีนัยสำคัญ

ข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป

การวิจัยครั้งนี้เป็นการศึกษาวิจัยเชิงปริมาณ ข้อมูลที่ได้จากผู้ตอบแบบสอบถามจึงเป็นข้อมูลเบื้องต้น ดังนั้นเพื่อให้ได้ข้อมูลเชิงลึกมาใช้ในการวิเคราะห์ปัจจัยที่เกี่ยวข้องอาจเพิ่มเติมวิธีการวิจัยเชิงคุณภาพ (Qualitative Research) ด้วยการสัมภาษณ์กลุ่ม (Focus Group Interview) หรือการสัมภาษณ์เจาะลึก (In-depth Interview) จะทำให้ทราบแนวคิดและระดับความรู้ของบุคลากรในองค์กรมากขึ้น

บรรณานุกรม

ดวงฤดี กิตติจารุดุลย์ (2557) ปัจจัยที่มีอิทธิพลต่อทัศนคติและความตระหนักด้านการบริหารจัดการความเสี่ยง กรณีศึกษา: บริษัทนำเข้าส่งออกแห่งหนึ่ง. กรุงเทพมหานคร: บัณฑิตศึกษา มหาวิทยาลัยเนชั่น

วาสนา อุทัยแสง. (2559). การตระหนักรับรู้การบริหารความเสี่ยง และการนำการบริหารความเสี่ยงไปปฏิบัติของบุคลากรมหาวิทยาลัยมหาสารคาม. กองแผนงาน: สำนักงานอธิการบดี

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัล. (2564). *CS*101 ความมั่นคงปลอดภัยไซเบอร์เบื้องต้น. สืบค้น 3 มกราคม 2565, จาก https://www.etda.or.th/th/Useful-Resource/Knowledge-Sharing/Articles/Cyber Security-101.aspx?feed=cb66f430-5546-4dd8-b279-3827e88d154b#_ftn5

สุธาเทพ รุณเรศ. (2561). ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร. กรุงเทพมหานคร: มหาวิทยาลัยธรรมศาสตร์

Cyber Security and Infrastructure Security Agency. (2019). *What is Cyber Security?*. Retrieved Jan 3, 2022, from https://www.cisa.gov/uscert/ncas/tips/ST04-001

European Union Agency for Cyber Security. (2021). *ENISA THREAT LANDSCAPE 2021* (Research report). Europe: European Union Agency for Cyber Security

Sailio, M.; Latvala, O. & Szanto, A. (2020). Cyber Threat Actors for the Factory of the Future. *Applied Sciences*, 10(12), 4334.

Yamane, Taro. (1973). *Statistics: An Introductory Analysis*. 3rded. New York: Harper and Row Publications.