แนวทางในการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร

นายอภิรักษ์ มิตรประสาร

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์ข้อมูลเพื่อนวัตกรรม
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2567

แนวทางในการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร

นายอภิรักษ์ มิตรประสาร

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์ข้อมูลเพื่อนวัตกรรม
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2567

ใบรับรองโครงร่างการค้นคว้าอิสระ

บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

เรื่อง แนวทางในการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร

โดย นายอภิรักษ์ มิตรประสาร

ได้รับอนุมัติให้นับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์ข้อมูลเพื่อนวัตกรรม

คณบดีคณะเทคโนโลยีสารสนเทศและ
..... นวัตกรรมดิจิทัล

(ผู้ช่วยศาสตราจารย์ ดร.สุนันฑา สดสี)

คณะกรรมการสอบการค้นคว้าอิสระ

..... ประธานกรรมการ
(รองศาสตราจารย์ ดร.สมชาย ปราการเจริญ)

..... อาจารย์ที่ปรึกษา
(รองศาสตราจารย์ ดร.นลินภัสร์ บำเพ็ญเพียร)

..... กรรมการ
(รองศาสตราจารย์ ดร.นลินภัสร์ บำเพ็ญเพียร)

..... กรรมการ
(อาจารย์ ดร.กาญจนา วิริยะพันธ์)

ชื่อ : นายอภิรักษ์ มิตรประสาร
ชื่อการค้นคว้าอิสระ : แนวทางในการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร
สาขาวิชา : วิทยาศาสตร์ข้อมูลเพื่อนวัตกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก : รองศาสตราจารย์ ดร.นลินภัสร์ บำเพ็ญเพียร
ปีการศึกษา : 2567

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาวิเคราะห์ปัจจัยที่ส่งผลให้ลดโอกาสเกิดภัยคุกคามทางไซเบอร์ และเพื่อนำเสนอแนวทางในการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร โดยใช้การศึกษาผ่านแบบสอบถามจากกลุ่มตัวอย่างประกอบด้วยบุคลากรในองค์กรต่าง ๆ จำนวน 411 คน การวิเคราะห์ปัจจัยที่มีผลต่อการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ทั้ง 7 ปัจจัยประกอบด้วย การรับรู้ภัยคุกคามทางไซเบอร์ พฤติกรรมการใช้งานระบบสารสนเทศ การฝึกอบรมและการให้ความรู้ด้านความปลอดภัยไซเบอร์ การสื่อสารภายในองค์กร วัฒนธรรมองค์กรที่สนับสนุนความปลอดภัยทางไซเบอร์ การใช้มาตรการป้องกันภัยคุกคามทางไซเบอร์ และการติดตามและตรวจสอบความปลอดภัยทางไซเบอร์ ผลการวิจัยแสดงให้เห็นว่ากลุ่มตัวอย่างเป็นทั้งชายและหญิง โดยส่วนใหญ่เป็นผู้ที่ทำงานในภาครัฐเป็นระยะเวลายาวนาน และการศึกษาสูง การวิเคราะห์ปัจจัยที่มีผลต่อการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ พบว่าแนวทางในการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กรที่สำคัญคือ การสื่อสารภายในองค์กรมีอิทธิพลมากที่สุด รองลงมาคือพฤติกรรมการใช้งานระบบสารสนเทศ โดยสรุปองค์กรควรมุ่งเน้นการพัฒนาด้านการสื่อสารภายใน การเสริมสร้างวัฒนธรรมองค์กรที่สนับสนุนความปลอดภัยไซเบอร์ เพื่อเพิ่มประสิทธิภาพของมาตรการรักษาความปลอดภัยทางไซเบอร์ให้ดียิ่งขึ้น

(มีจำนวนทั้งสิ้น 58 หน้า)

คำสำคัญ : ภัยคุกคามทางไซเบอร์ ความปลอดภัยไซเบอร์ ความตระหนักรู้ พฤติกรรมการใช้งานระบบสารสนเทศ

_____ อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก

Name : Mr. Apiruck Mitprasan
Independent Study Title : Guidelines for Reducing the Risk of Cyber Threats in an Organization
Major Field : Data Science for Innovation
King Mongkut's University of Technology North Bangkok
Independent Study Advisor : Associate Professor Dr. Nalinpat Bhumpenpein
Academic Year : 2024

ABSTRACT

This research aims to analyze the factors that contribute to reducing the likelihood of cybersecurity threats and to propose practical approaches for minimizing such threats within organizations. The study employed a questionnaire survey with a sample of 411 personnel from various organizations. The analysis focused on seven key factors influencing the reduction of cybersecurity threats: cybersecurity threat awareness, information system usage behavior, cybersecurity training and awareness, internal organizational communication, a cybersecurity-supportive organizational culture, implementation of cybersecurity measures, and cybersecurity monitoring and auditing.The findings revealed that the respondents were both male and female, primarily long-term government employees with high levels of education. The analysis indicated that the most influential factor in reducing cybersecurity threats was internal organizational communication, followed by information system usage behavior. In conclusion, organizations should prioritize improving internal communication and fostering a culture that supports cybersecurity in order to enhance the effectiveness of cybersecurity measures.

(Total 58 Pages)

Keywords: Cybersecurity Threats, Cybersecurity, Awareness, Information System Usage Behavior

_____ Advisor

กิตติกรรมประกาศ

กิตติกรรมประกาศนี้ ข้าพเจ้าขอกราบขอบพระคุณอาจารย์ที่ปรึกษาการค้นคว้าอิสระ รองศาสตราจารย์ ดร.นลินภัสร์ บำเพ็ญเพียร ผู้ให้คำแนะนำ องค์ความรู้ และข้อเสนอแนะที่มีคุณค่าอย่างยิ่งตลอดกระบวนการทำสารนิพนธ์ฉบับนี้ นอกจากนี้ ข้าพเจ้าขอขอบพระคุณคณะกรรมการสอบทุกท่านที่ให้คำแนะนำอันเป็นประโยชน์ ซึ่งช่วยให้ข้าพเจ้าสามารถปรับปรุงและพัฒนาผลงานให้มีคุณภาพมากยิ่งขึ้น

ข้าพเจ้าขอขอบคุณ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ที่ให้การสนับสนุนข้อมูลและทรัพยากรที่จำเป็นสำหรับการศึกษา รวมถึงขอขอบคุณเพื่อนนักศึกษา และผู้มีส่วนเกี่ยวข้องทุกท่าน ที่ให้กำลังใจและแลกเปลี่ยนความคิดเห็นอันเป็นประโยชน์ตลอดการทำวิจัย สุดท้ายนี้ข้าพเจ้าขอขอบคุณครอบครัวที่ให้กำลังใจและสนับสนุนข้าพเจ้าในทุกด้านมาโดยตลอด การค้นคว้าอิสระฉบับนี้สำเร็จลงได้ด้วยแรงสนับสนุนจากทุกฝ่าย ข้าพเจ้าขอกราบขอบพระคุณจากใจจริง

อภิรักษ์ มิตรประสาร

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญรูปภาพ

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันในยุคดิจิทัลที่เทคโนโลยีและอินเทอร์เน็ตมีบทบาทสำคัญในชีวิตประจำวันของผู้คนทั่วโลก ความปลอดภัยทางไซเบอร์กลายเป็นเรื่องที่มีความสำคัญอย่างยิ่ง เนื่องจากการเพิ่มขึ้นของภัยคุกคามทางไซเบอร์ที่ซับซ้อนและมากขึ้นเรื่อย ๆ องค์กรและบุคคลทั่วไปต้องเผชิญกับความเสี่ยงในการถูกโจมตีทางไซเบอร์ ซึ่งอาจก่อให้เกิดความเสียหายทั้งทางการเงินและความเสียหายต่อชื่อเสียง ภัยคุกคามทางไซเบอร์สามารถเกิดขึ้นได้ในหลายรูปแบบ เช่น การโจมตีแบบฟิชชิ่ง (Phishing) การโจมตีด้วยมัลแวร์ (Malware) การโจมตีแบบแรนซัมแวร์ (Ransomware) และการโจมตีแบบ DDoS (Distributed Denial of Service) เป็นต้น การโจมตีเหล่านี้มักมีเป้าหมายเพื่อขโมยข้อมูลสำคัญ เรียกค่าไถ่ หรือทำลายระบบคอมพิวเตอร์ ทำให้การรักษาความปลอดภัยทางไซเบอร์เป็นเรื่องที่องค์กรและบุคคลทั่วไปไม่สามารถมองข้ามได้ [1]

การสร้างความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์จึงเป็นสิ่งสำคัญที่สามารถช่วยลดความเสี่ยงและป้องกันการโจมตีได้ ผู้ใช้คอมพิวเตอร์และอินเทอร์เน็ตที่มีความรู้และตระหนักรู้ในเรื่องความปลอดภัยทางไซเบอร์จะสามารถระบุและตอบโต้ภัยคุกคามได้อย่างมีประสิทธิภาพ ทั้งนี้ การให้ความรู้และการฝึกอบรมเกี่ยวกับภัยคุกคามทางไซเบอร์ให้กับพนักงานในองค์กรและบุคคลทั่วไปเป็นวิธีหนึ่งที่สามารถช่วยเสริมสร้างความตระหนักรู้และเพิ่มความปลอดภัยทางไซเบอร์ได้ บุคลากรมีบทบาทสำคัญในการรักษาความปลอดภัยทางไซเบอร์ เนื่องจากพนักงานในองค์กรเป็นเป้าหมายที่สำคัญของการโจมตีทางไซเบอร์ หากพนักงานไม่มีความรู้และทักษะในการระวังภัยคุกคาม พวกเขาอาจเผลอเปิดทางให้กับผู้โจมตี เช่น การคลิกเปิดอีเมลฟิชชิ่งที่มีมัลแวร์ฝังอยู่ การเข้าไปยังเว็บไซต์ที่ไม่เหมาะสม การเปิดไฟล์ที่ไม่มีการตรวจสอบ และการใช้รหัสผ่านที่ไม่ปลอดภัย เป็นต้น ดังนั้นการให้ความรู้และการฝึกอบรมแก่บุคลากรในองค์กรเป็นสิ่งที่จำเป็นในการเสริมสร้างความมั่นคงและปลอดภัยของระบบสารสนเทศในองค์กร การลงทุนในด้านการฝึกอบรมและพัฒนาทักษะของบุคลากรจะช่วยเพิ่มความสามารถในการรับมือกับภัยคุกคามทางไซเบอร์ นอกจากนี้ การสร้างวัฒนธรรมองค์กรที่เน้นความปลอดภัยทางไซเบอร์จะช่วยเสริมสร้างความรับผิดชอบและการตระหนักรู้ของพนักงาน ทำให้องค์กรสามารถรับมือกับภัยคุกคามได้อย่างมีประสิทธิภาพและปลอดภัยยิ่งขึ้น การกระทำความผิดเกี่ยวกับระบบและข้อมูลคอมพิวเตอร์เป็นเรื่องสำคัญที่อาจส่งผลกระทบที่รุนแรงต่อองค์กรและบุคคล การเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต การละเมิดความเป็นส่วนตัว หรือการแอบดูดข้อมูลสามารถทำให้องค์กรโดนลงโทษทางกฎหมายและเสียชื่อเสียงได้ นอกจากนี้ การโจมตีด้วยมัลแวร์และการทำลาย

ข้อมูลสามารถทำให้ระบบคอมพิวเตอร์ขัดข้องและทำให้งานขององค์กรหยุดชะงักได้ ดังนั้น การป้องกันและการเตรียมความพร้อมเพื่อป้องกันการกระทำความผิดเช่นนี้เป็นสิ่งจำเป็นสำหรับองค์กรในยุคดิจิทัลที่มีภัยคุกคามทางไซเบอร์เพิ่มมากขึ้นอย่างต่อเนื่อง [2]

ผู้วิจัยจึงเล็งเห็นว่า แนวทางในการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กรเป็นส่วนสำคัญที่ช่วยให้เข้าใจถึงภัยคุกคามทางไซเบอร์ในมุมมองที่ลึกซึ้งขึ้น ผู้วิจัยมองเห็นว่าการเพิ่มความรู้และการตระหนักรู้ในการรักษาความปลอดภัยทางไซเบอร์ของบุคลากรเป็นเรื่องสำคัญ เนื่องจากบุคลากรเป็นปัจจัยสำคัญที่มีส่วนร่วมในการป้องกันและตอบสนองต่อการโจมตีทางไซเบอร์ การศึกษาและการฝึกอบรมเป็นวิธีที่ดีในการสร้างพลังป้องกันที่แข็งแกร่ง ซึ่งส่งผลต่อการป้องกันข้อมูลและระบบคอมพิวเตอร์ขององค์กรให้มีประสิทธิภาพมากยิ่งขึ้น

1.2 วัตถุประสงค์ของการวิจัย

1.2.1 เพื่อวิเคราะห์ปัจจัยที่ส่งผลให้ลดโอกาสเกิดภัยคุกคามทางไซเบอร์

1.2.2 เพื่อนำเสนอแนวทางในการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร

1.3 ขอบเขตของการวิจัย

การวิจัยนี้ผู้วิจัยได้กาหนดขอบเขตการวิจัยแบ่งออกเป็น 2 ด้าน คือ ขอบเขตด้านประชากรและกลุ่มตัวอย่าง และขอบเขตด้านเนื้อหาการวิจัย ดังนี้

1.3.1 ขอบเขตด้านประชากรและกลุ่มตัวอย่าง

ประชากร คือ ผู้ใช้งานระบบและข้อมูลคอมพิวเตอร์ผ่านเครือข่ายอินเทอร์เน็ตในเขตพื้นที่กรุงเทพมหานครและปริมณฑล โดยการสำรวจจากประชากรในเขตพื้นที่กรุงเทพมหานครและปริมณฑลตามหลักฐาน การทะเบียนราษฎรที่มีจานวนประชากรมากถึง 10,944,863 คนหรือประมาณร้อยละ 16.44 ของประชากรทั่วประเทศ (ราชกิจจานุเบกษา วันที่ 30 มกราคม 2563) และมีสถิติในการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือน พ.ศ. 2561 ซึ่งใช้งานผ่านอุปกรณ์อิเล็กทรอนิกส์ที่เชื่อมต่อกับเครือข่ายอินเทอร์เน็ตคิดเป็นร้อยละ 30.67 ของการใช้งานถือได้ว่าประชากรในเขตพื้นที่กรุงเทพมหานครและปริมณฑลเป็นประชาชนส่วนใหญ่ของประเทศไทยที่มีการใช้ระบบและข้อมูลคอมพิวเตอร์

กลุ่มตัวอย่าง คือ ผู้ใช้งานระบบและข้อมูลคอมพิวเตอร์ผ่านเครือข่ายอินเทอร์เน็ต ซึ่งผู้วิจัยได้ทำ การสำรวจข้อมูลผ่านทางแบบสอบถาม (Questionnaire) จำนวน 400 คน โดยการหาขนาดกลุ่มตัวอย่างจากตารางสำเร็จของทาโร่ ยามาเน่ ที่ระดับความคลาดเคลื่อนร้อยละ 5 หรือระดับความเชื่อมั่นร้อยละ 95

1.3.2 ขอบเขตด้านเนื้อหาการวิจัย

การวิจัยนี้เป็นศึกษาความตระหนักรู้ด้านภัยคุมคามทางไซเบอร์ ปัจจุบันเนื่องจากภัยคุกคามทางไซเบอร์มีความซับซ้อนและรุนแรงมากขึ้น การเข้าใจและการรับมือกับภัยคุกคามทางไซเบอร์เป็นสิ่งจำเป็นที่องค์กรและบุคคลทั่วไปต้องมี เพื่อลดความเสี่ยงและปกป้องข้อมูลสำคัญจากการโจมตีต่าง ๆ ทั้งการศึกษาวิธีการป้องกัน การสร้างความตระหนักรู้ในบุคลากร และการพัฒนานโยบายความปลอดภัยที่เข้มแข็ง เพื่อให้โลกดิจิทัลเป็นที่ปลอดภัยและเชื่อถือได้มากยิ่งขึ้น

1.4 ประโยชน์ที่ได้รับ

การวิจัยนี้คาดว่าจะช่วยเสริมสร้างความรู้ความเข้าใจเรื่องการลดโอกาสภัยคุกคามทางไซเบอร์ในองค์กร ซึ่งจะช่วยลดโอกาสในการเกิดความเสี่ยงและเพิ่มประสิทธิภาพในการป้องกันการโจมตี ทั้งนี้การสร้างวัฒนธรรมที่เน้นความปลอดภัยทางไซเบอร์ภายในองค์กรจะส่งเสริมการมีส่วนร่วมของทุกคนในการรักษาความปลอดภัยข้อมูล ลดผลกระทบทางการเงินและชื่อเสียงที่อาจเกิดจากภัยคุกคาม อีกทั้งยังพัฒนาขีดความสามารถในการปรับปรุงมาตรการรักษาความปลอดภัย ให้เหมาะสมกับภัยคุกคามที่เปลี่ยนแปลงอยู่เสมอ โดยแนวทางในการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร จะส่งผลให้สังคมและองค์กรมีความปลอดภัยทางข้อมูลที่มากยิ่งขึ้น

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ผู้วิจัยได้ศึกษาค้นคว้าทฤษฎีและงานวิจัยที่เกี่ยวข้อง ดังต่อไปนี้

2.1 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

2.2 ภัยคุกคามทางไซเบอร์ (Cyber Threats)

2.3 ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

2.4 ปัจจัยที่ส่งผลให้ลดโอกาสเกิดภัยคุกคามทางไซเบอร์

2.5 แนวทางในการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร

2.1 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีผลบังคับใช้แล้ว ตั้งแต่วันที่ 28 พฤษภาคม 2562 เป็นกลไกการเฝ้าระวัง ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มีการประสานความร่วมมือระหว่างผู้เกี่ยวข้องพัฒนาความรู้ความสามารถของบุคลากรและผู้เชี่ยวชาญ รวมถึงการให้ความรู้และความตระหนักถึงภัยไซเบอร์ เช่น ไวรัส มัลแวร์ และโทรจัน เป็นต้น อาชญากรทางคอมพิวเตอร์ที่อาจเกิดกับระบบโครงสร้างพื้นฐานทางสารสนเทศสำคัญและส่งผลเสียหายในระดับประเทศ หน่วยงาน หรือองค์กร หรือส่วนงานหนึ่งส่วนงานใดของหน่วยงานหรือองค์กรที่เป็นโครงสร้างพื้นฐานสำคัญของประเทศมีธุรกรรมทางอิเล็กทรอนิกส์ที่ส่งผลสำคัญต่อความมั่นคงหรือความสงบเรียบร้อยของประเทศ หรือต่อสาธารณชน ได้แก่ กลุ่มความมั่นคงของรัฐ กลุ่มบริการภาครัฐที่สำคัญกลุ่มการเงินการ-ธนาคาร กลุ่มเทคโนโลยีสารสนเทศ กลุ่มพลังงาน กลุ่มสาธารณูปโภค และกลุ่มสาธารณสุข ระบบสารสนเทศของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศที่ใช้ในการดำเนินงานและให้บริการ หากระบบถูกรบกวนจะทำให้ไม่สามารถดำเนินงานหรือให้บริการได้ ส่วนประกอบของ พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 [2]

2.2 ภัยคุกคามทางไซเบอร์ (Cyber Threats)

แนวคิดเกี่ยวกับภัยคุกคามทางไซเบอร์แบ่งประเภทออกเป็น 4 ประเภทหลัก ดังนี้

ประเภทที่ 1 ภัยคุกคามที่เกิดจากการใช้โปรแกรมประยุกต์: เป็นภัยคุกคามที่มาจากโปรแกรมที่ถูกดาวน์โหลดและติดตั้งบนคอมพิวเตอร์หรืออุปกรณ์เคลื่อนที่ สามารถขโมยข้อมูลหรือส่งข้อความที่ไม่พึงประสงค์ออกไปยังผู้อื่นได้ ตัวอย่างของโปรแกรมในกลุ่มนี้ ได้แก่ ไวรัส เวิร์ม โทรจัน บ็อตเน็ต และสปายแวร์ เป็นต้น

ประเภทที่ 2 ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์ (Web-Based Threats) เป็นภัยคุกคามที่เกิดจากการที่ผู้ใช้คอมพิวเตอร์หรืออุปกรณ์พกพาเปิดเว็บไซต์ขึ้นมาใช้งาน ซึ่งเว็บไซต์ที่เรียกมาใช้อาจ

เป็นเว็บไซต์ฟิชชิ่ง ซึ่งถูกออกแบบให้มีลักษณะคล้ายคลึงกับเว็บไซต์จริงเพื่อหลอกให้ผู้ใช้กรอกข้อมูลเข้าสู่ระบบของผู้ไม่หวังดี

ประเภทที่ 3 ภัยคุกคามจากการใช้งานเครือข่ายไร้สาย ปัจจุบันมีผู้ให้บริการเครือข่ายไร้สายเป็นจำนวนมาก มีทั้งที่น่าเชื่อถือและที่ไม่น่าเชื่อถือ รวมถึงผู้ที่แอบแฝงเพื่อวัตถุประสงค์อื่นดังนั้น ผู้ใช้คอมพิวเตอร์ หรืออุปกรณ์เคลื่อนที่เชื่อมต่อระบบเครือข่ายไร้สายต่าง ๆ อาจได้รับผลกระทบโดยตรง

ประเภทที่ 4 ภัยคุกคามที่เกิดจากการถูกโจมตีแบบเจาะจงเป้าหมาย (Targeted Attack) ที่มาจากหลายประเทศมีมากขึ้น ผู้โจมตี หรือแฮกเกอร์ (Hackers) ในประเทศต่าง ๆ จะใช้การโจมตีแบบเจาะจงเป้าหมายอย่างต่อเนื่อง สร้างความเสียหายให้แก่โครงสร้างพื้นฐานวิกฤติ สถาบันการเงิน และองค์กรอื่น ๆ ของภาครัฐ และภาคเอกชนในหลายประเทศอาชญากรไซเบอร์เหล่านี้จะใช้มาตรการที่รวดเร็วและรุนแรงในการโจรกรรมข้อมูล ภัยคุกคามประเภทนี้จัดว่าเป็นภัยคุกคามที่กระทบต่อความมั่นคงของประเทศเป็นอย่างยิ่ง [3]

การจัดการกับภัยคุกคามทางไซเบอร์จำเป็นต้องใช้วิธีการและมาตรการที่เหมาะสมเพื่อป้องกันและลดความเสี่ยงจากการโจมตี รวมถึงการฝึกอบรมและสร้างความตระหนักรู้ให้กับบุคลากรในองค์กรเพื่อให้สามารถรับมือกับภัยคุกคามต่าง ๆ ได้อย่างมีประสิทธิภาพ

2.3 ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

ความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) หมายถึง ความรู้แจ้งชัดเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เช่น ความเสี่ยง ภัยคุกคาม การระราน การแอบอ้าง การกีดกันการโจมตี การก่อการร้าย เป็นต้น ในระบบความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ จึงเป็นการสร้างความรู้ ความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในการทำงานและมีความรู้เกี่ยวกับวิธีการป้องกันภัยคุกคามทางไซเบอร์ให้ปลอดภัยจากภัยคุกคามทางไซเบอร์รูปแบบต่าง ๆ เพื่อให้บุคลากรสามารถดูแลรักษาและใช้งานทรัพยากรสารสนเทศขององค์กรได้อย่างปลอดภัย ระวังป้องกันภัยต่อการอาชญากรรมการโจมตี การทำลาย และความผิดพลาดต่าง ๆ ที่อาจเกิดขึ้น โดยคำนึงถึงความปลอดภัยของทรัพย์สินเป็นอันดับแรก และสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวัน การสร้างการตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์มีการอธิบายไว้หลายวิธี เช่น การเรียนรู้แบบผสมผสานที่ใช้ออนไลน์และวีดิทัศน์ร่วมกันเพื่อเพิ่มความเข้าใจและความสามารถในการป้องกันตนเองจากภัยคุกคามไซเบอร์ การจัดการข้อมูลองค์กรที่เน้นย้ำความสำคัญของการจัดการข้อมูลส่วนตัวและรหัสผ่าน รวมถึงการใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์อย่างปลอดภัย การอบรมและฝึกฝนเพื่อสร้างความตระหนักรู้โดยเน้นการปฏิบัติตามนโยบายและขั้นตอนขององค์กร การประเมินและปรับปรุงมาตรการความปลอดภัยอย่างต่อเนื่องเพื่อให้การป้องกันมีประสิทธิภาพสูงสุด และการให้ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ เป็นต้น การโจมตี การแอบอ้าง และการหลอกลวงทางอินเทอร์เน็ตเพื่อให้บุคลากรสามารถป้องกันตนเองและรักษาความ

ปลอดภัยของข้อมูลในองค์กรได้อย่างมีประสิทธิภาพ ทั้งหมดนี้จะช่วยให้บุคลากรในองค์กรมีความตระหนักรู้และสามารถป้องกันตนเองจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ [4]

2.4 ปัจจัยที่ส่งผลให้ลดโอกาสเกิดภัยคุกคามทางไซเบอร์

จากการทบทวนงานวิจัยที่เกี่ยวข้องปัจจัยที่ส่งผลให้ลดโอกาสเกิดภัยคุกคามทางไซเบอร์ 20 บทความได้สรุปมาจำนวน 7 ปัจจัย ได้แก่ 1) การรับรู้ภัยคุกคามทางไซเบอร์ 2) พฤติกรรมการใช้งานระบบสารสนเทศ 3) การฝึกอบรมและการให้ความรู้ด้านความปลอดภัยไซเบอร์ 4) การสื่อสารภายในองค์กร 5) วัฒนธรรมองค์กรที่สนับสนุนความปลอดภัยทางไซเบอร์ 6) การใช้มาตรการป้องกันภัยคุกคามทางไซเบอร์ 7) การติดตามและตรวจสอบความปลอดภัยทางไซเบอร์ โดยปัจจัยดังกล่าวสามารถแสดงรายละเอียดของแต่ละปัจจัยได้ดังนี้

2.4.1 การรับรู้ภัยคุกคามทางไซเบอร์

จากการศึกษาสภาพปัญหาและพฤติกรรมการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินฯ และพัฒนาแนวทางการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ โดยพบว่าบุคลากรมีการกำหนดกลยุทธ์ด้านภัยคุกคามทางไซเบอร์และผู้บังคับบัญชาให้ความสำคัญกับนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงมีการระบุภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อการปฏิบัติงานโดยตรง ซึ่งภาพรวมความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อยู่ในระดับมากที่สุด [5] บุคลากรต้องการสร้างความตระหนักรู้ด้วยวิธีการเรียนรู้แบบออนไลน์และการเรียนโดยใช้วีดิทัศน์ผสมผสานกัน ซึ่งการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์นี้เป็นสิ่งสำคัญในการลดความเสี่ยงและความเสียหายจากการใช้งานบนโลกไซเบอร์ โดยการสร้างความรู้ ความเข้าใจ และการป้องกันภัยคุกคามทางไซเบอร์ให้กับบุคลากรในองค์กรอย่างต่อเนื่องและมีประสิทธิภาพ

ปัจจัยที่มีผลต่อการรับรู้ภัยคุกคามทางไซเบอร์ของบุคลากรในองค์กรประกอบด้วยปัจจัยส่วนบุคคลและปัจจัยด้านการฝึกอบรมและการแจ้งเตือนภัยคุกคามทางไซเบอร์ โดยปัจจัยส่วนบุคคลที่สำคัญได้แก่ ระดับการศึกษา แผนกที่สังกัด และประสบการณ์เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งพบว่าบุคลากรที่มีระดับการศึกษาสูงสุดในระดับปริญญาโทมีความตระหนักรู้สูงกว่าผู้ที่มีการศึกษาต่ำกว่า และบุคลากรในแผนกที่มีการใช้งานระบบสารสนเทศมากกว่ามีความตระหนักรู้สูงกว่า นอกจากนี้ บุคลากรที่เคยมีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์มีความตระหนักรู้สูงกว่า ในขณะที่เพศ อายุ และประสบการณ์การทำงานไม่พบความแตกต่างอย่างมีนัยสำคัญในระดับความตระหนักรู้ การฝึกอบรมและการแจ้งเตือนภัยคุกคามทางไซเบอร์อย่างสม่ำเสมอมีผลต่อการเพิ่มความตระหนักรู้ของบุคลากร โดยเฉพาะในด้านการหลอกลวง (Phishing) ซึ่งเป็นด้านที่บุคลากรมีความตระหนักรู้น้อยที่สุด การศึกษานี้เน้นย้ำถึงความสำคัญของการพัฒนานโยบายและการฝึกอบรมเพื่อ

เสริมสร้างความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ในองค์กร เพื่อป้องกันความเสี่ยงและเพิ่มความปลอดภัยในการใช้งานเทคโนโลยีสารสนเทศ

2.4.2 พฤติกรรมการใช้งานระบบสารสนเทศ

การศึกษาพฤติกรรมการใช้งานระบบเครือข่ายอินเทอร์เน็ตในสถานศึกษา โดยเฉพาะการตระหนักรู้ถึงภัยคุกคามและอาชญากรรมไซเบอร์ พบว่าผู้ใช้งานมีประสบการณ์เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ในระดับน้อย แต่มีความตระหนักรู้ในระดับสูง ซึ่งปัจจัยที่มีผลต่อพฤติกรรมการใช้งานระบบสารสนเทศประกอบด้วยอายุและประสบการณ์การทำงานที่แตกต่างกัน โดยผู้ที่มีอายุมากและมีประสบการณ์การทำงานมากจะมีความตระหนักรู้สูงกว่า นอกจากนี้ ความรู้เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ยังมีผลต่อความตระหนักรู้ด้วย โดยผู้ที่มีความรู้มากจะมีความตระหนักรู้สูง การวิจัยนี้ชี้ให้เห็นถึงความสำคัญของการให้ความรู้และการสร้างความตระหนักรู้ในสถานศึกษาเพื่อป้องกันภัยคุกคามและอาชญากรรมไซเบอร์ โดย การออกแบบการเรียนรู้ที่เหมาะสมและทันสมัยตามการเปลี่ยนแปลงของการใช้อินเทอร์เน็ต เพื่อให้ผู้ใช้งานสามารถป้องกันตนเองและทรัพย์สินจากภัยคุกคามไซเบอร์ได้อย่างมีประสิทธิภาพ

จากการศึกษาการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล พบว่าการวิเคราะห์และจำแนกปัจจัยที่มีอิทธิพลต่อมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศด้วยวิธีการวิเคราะห์จำแนกกลุ่ม และการยืนยันองค์ประกอบโดยวิธีทางสถิติ ช่วยให้สามารถระบุปัจจัยที่สำคัญและมีผลกระทบต่อการบริหารจัดการความมั่นคงปลอดภัยได้อย่างชัดเจน ผลการศึกษานี้มีความสำคัญในการเพิ่มประสิทธิภาพการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของ คณะแพทยศาสตร์ศิริราชพยาบาล และยังเป็นแนวทางในการแก้ปัญหาและปรับปรุงการดำเนินงานในอนาคต ทำให้สามารถพัฒนามาตรการและนโยบายที่เหมาะสมเพื่อป้องกันและลดความเสี่ยงที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศได้อย่างมีประสิทธิภาพ[6],[7]

2.4.3 การฝึกอบรมและการให้ความรู้ด้านความปลอดภัยไซเบอร์

การศึกษานี้เน้นถึงความสำคัญของการฝึกอบรมและการให้ความรู้ด้านความปลอดภัยไซเบอร์ในหมู่นักเรียน พบว่าผู้ใช้งานอินเทอร์เน็ตในสถาบันการศึกษามักขาดความตระหนักรู้เกี่ยวกับความปลอดภัยไซเบอร์ ซึ่งนำไปสู่การละเมิดนโยบายความปลอดภัยไซเบอร์และการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ เช่น การฟิชชิ่ง การหลอกลวง และการแฮ็ก เป็นต้น การศึกษานี้ใช้แบบสอบถามเพื่อประเมินระดับความตระหนักรู้ของนักเรียนเกี่ยวกับความปลอดภัยไซเบอร์ และพบว่ามีช่องว่างในความรู้และการปฏิบัติที่จำเป็นต้องได้รับการปรับปรุง การฝึกอบรมและการให้ความรู้ที่เหมาะสมสามารถช่วยเพิ่มทักษะการตัดสินใจของนักเรียนเกี่ยวกับความเป็นส่วนตัวและความปลอดภัย โดยใช้โมเดล Nudge เพื่อกระตุ้นให้ผู้ใช้ทำการตัดสินใจที่ดีขึ้นเกี่ยวกับการปกป้องข้อมูลส่วนบุคคลและความปลอดภัยออนไลน์ การศึกษายังเสนอแนะกลยุทธ์ต่าง ๆ เพื่อปรับปรุงสภาพแวดล้อมความ

ปลอดภัยและกระบวนการตัดสินใจของนักเรียนและองค์กร รวมถึงการเพิ่มการรับรู้และการฝึกอบรมด้านความปลอดภัยไซเบอร์ในหลักสูตรการศึกษา การจัดโปรแกรมการฝึกอบรมที่เน้นการปฏิบัติ และการใช้เทคโนโลยีเพื่อเสริมสร้างความรู้และทักษะด้านความปลอดภัยไซเบอร์ของนักเรียน ความสำคัญของการฝึกอบรมและการให้ความรู้ด้านความปลอดภัยไซเบอร์ในกระบวนการศึกษาออนไลน์ โดยพบว่านักศึกษาส่วนใหญ่ขาดความรู้และความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์ เช่น การโจมตีทางเครือข่าย การโจมตีแบบฟิชชิ่ง และการใช้วิศวกรรมสังคม เป็นต้น ซึ่งทำให้พวกเขาเสี่ยงต่อการตกเป็นเหยื่อของการโจมตีทางไซเบอร์ การฝึกอบรมด้านความปลอดภัยไซเบอร์จึงมีความสำคัญอย่างยิ่งในการเพิ่มพูนความรู้และทักษะในการป้องกันตนเองจากภัยคุกคามเหล่านี้ การศึกษาแสดงให้เห็นว่าการให้ความรู้ด้านความปลอดภัยไซเบอร์สามารถช่วยให้นักศึกษาใช้เทคโนโลยีและอินเทอร์เน็ตได้อย่างปลอดภัยและ มีประสิทธิภาพมากขึ้น นอกจากนี้ยังพบว่าการฝึกอบรมที่มีคุณภาพสูงและครอบคลุมถึงรายละเอียดทางเทคนิคจะช่วยเพิ่มระดับความตระหนักและความรู้ของนักศึกษาได้อย่างมีนัยสำคัญ การให้ความรู้ด้าน ความปลอดภัยไซเบอร์ไม่เพียงแต่ช่วยป้องกันการโจมตีทางไซเบอร์ แต่ยังช่วยให้นักศึกษามีความเข้าใจในมิติทางกฎหมายของอาชญากรรมไซเบอร์และการลงโทษทางกฎหมายที่เกี่ยวข้อง ซึ่งจะทำให้พวกเขามี ความระมัดระวังและปฏิบัติตามกฎระเบียบมากขึ้น [7]

2.4.4 การสื่อสารภายในองค์กร

การสื่อสารภายในองค์กรเป็นปัจจัยสำคัญที่ช่วยเสริมสร้างวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ โดยการสื่อสารที่ดีจะต้องประกอบด้วยการเผยแพร่นโยบายและแนวปฏิบัติให้บุคลากรได้รับทราบและปฏิบัติตาม การเผยแพร่แผนการรับมือภัยคุกคามทางไซเบอร์ และการเผยแพร่ความรู้ด้านการรับมือภัยคุกคามทางไซเบอร์ การสื่อสารที่มีประสิทธิภาพจะช่วยให้บุคลากรมีความเชื่อมั่นในมาตรการปกป้องข้อมูลส่วนบุคคลและไว้วางใจในระบบเครือข่ายคอมพิวเตอร์ขององค์กร นอกจากนี้การมีอุปกรณ์สำนักงานที่อำนวยความสะดวกในการทำงานและการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง ก็เป็นส่วนสำคัญในการสร้างวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ที่ยั่งยืน [8],[9]

ปัจจัยการสื่อสารภายในองค์กรมีความสำคัญอย่างยิ่งต่อการจัดการความปลอดภัยของระบบสารสนเทศ โดยปัจจัยหลักที่มีอิทธิพลได้แก่ ความรู้ด้านสารสนเทศ การตระหนักรู้ การบริหารจัดการและพฤติกรรมการใช้สารสนเทศ ซึ่งทั้งหมดนี้มีผลโดยตรงและโดยอ้อมต่อประสิทธิผลของการจัด การความปลอดภัยของระบบสารสนเทศ การบริหารจัดการมีอิทธิพลมากที่สุด รองลงมาคือการตระหนักรู้ความรู้ด้านสารสนเทศ และพฤติกรรมการใช้สารสนเทศตามลำดับ การสื่อสารที่มีประสิทธิภาพภายในองค์กรจึงต้องครอบคลุมการให้ความรู้ การสร้างความตระหนักรู้ การวางแผนและการจัดการที่ดี รวมถึงการส่งเสริมพฤติกรรมการใช้สารสนเทศที่เหมาะสม นอกจากนี้ การสื่อสารยังต้องมีการควบคุม

และติดตามผล อย่างต่อเนื่องเพื่อให้แน่ใจว่าบุคลากรทุกคนปฏิบัติตามนโยบายและแนวทางที่กำหนดไว้ ซึ่งจะช่วยให้ ระบบสารสนเทศมีความปลอดภัยและมีประสิทธิภาพในการใช้งาน [10],[11],[12]

2.4.5 วัฒนธรรมองค์กรที่สนับสนุนความปลอดภัยทางไซเบอร์

การสร้างวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรเป็นกระบวนการที่ต้องอาศัยความร่วมมือจากทุกระดับของบุคลากรและการจัดการระบบความมั่นคงปลอดภัยไซเบอร์อย่างมีประสิทธิภาพ โดยมีองค์ประกอบหลักสามประการคือ ผู้บริหาร บุคลากรทุกระดับ และระบบการจัดการด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งการมีส่วนร่วมและการสอดคล้องในแนวทางเดียวกันของบุคลากรทุกคนเป็นสิ่งสำคัญ ที่จะทำให้เกิดวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ที่ยั่งยืนในองค์กร การสร้างวัฒนธรรมนี้ต้องเริ่มจาก การพัฒนาความรู้ ความเข้าใจ และความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ รวมถึงการกำหนดนโยบายและแนวทางปฏิบัติที่ชัดเจนจากผู้บริหาร การมีระบบการจัดการที่ครอบคลุมและเชื่อมโยงกัน อย่างมีประสิทธิภาพ และการส่งเสริมให้บุคลากรทุกคนมีส่วนร่วมในการป้องกันและตอบสนองต่อ ภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง นอกจากนี้ การประเมินและปรับปรุงวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์อย่างสม่ำเสมอ

วัฒนธรรมองค์กรที่ดีจะส่งเสริมให้พนักงานมีความตระหนักรู้และเข้าใจถึงความสำคัญของการรักษาความปลอดภัยทางไซเบอร์ ซึ่งรวมถึงการปกป้องข้อมูลสารสนเทศจากการเข้าถึงโดยไม่ได้รับอนุญาต การรักษาความถูกต้องของข้อมูล และการสร้างความมั่นใจว่าระบบสารสนเทศสามารถตอบสนองต่อการใช้งานได้อย่างต่อเนื่อง นอกจากนี้ การมีนโยบายและกระบวนการที่ชัดเจนในการจัดการความเสี่ยงทางไซเบอร์ การฝึกอบรมพนักงานอย่างต่อเนื่อง และการใช้เทคโนโลยีที่เหมาะสม ยังเป็นปัจจัยสำคัญที่ช่วยเสริมสร้าง ความปลอดภัยทางไซเบอร์ในองค์กร ทั้งนี้ การสร้างวัฒนธรรมองค์กรที่เน้นความปลอดภัยทางไซเบอร์ จะช่วยลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์และเพิ่มความมั่นคงในการดำเนินธุรกิจพาณิชย์อิเล็กทรอนิกส์ [13]

2.4.6 การใช้มาตรการป้องกันภัยคุกคามทางไซเบอร์

การตระหนักรู้ถึงภัยคุกคามทางไซเบอร์เป็นปัจจัยสำคัญในการป้องกันและลดความเสี่ยงที่อาจเกิดขึ้นจากการใช้งานอินเทอร์เน็ตและระบบดิจิทัล การวิจัยพบว่าการกำหนดกลยุทธ์ด้านภัยคุกคามทางไซเบอร์ การให้ความสำคัญกับนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ และการระบุภัยคุกคามที่ส่งผลกระทบโดย ตรงต่อการปฏิบัติงานเป็นสิ่งจำเป็น นอกจากนี้ การพัฒนาแนวทางการเสริมสร้างความตระหนักรู้ผ่าน การเรียนรู้แบบออนไลน์และการใช้วีดิทัศน์เป็นวิธีที่มีประสิทธิภาพสูงสุดในการเพิ่มความรู้และความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์ การสร้างแอปพลิเคชันสำหรับการเสริมสร้างและประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ช่วยให้บุคลากรสามารถเรียนรู้และประเมินตนเองได้อย่างต่อเนื่อง การวิจัย ยังเน้นถึงความสำคัญของการปรับพฤติกรรมการใช้งานอินเทอร์เน็ต การใช้งานสื่อสังคม การเข้าถึงสื่อออนไลน์ และการใช้งานโปรแกรม

ต่าง ๆ อย่างปลอดภัย เพื่อป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น การตระหนักรู้ถึงความเสี่ยงและการป้องกันภัยคุกคามทางไซเบอร์จึงเป็นปัจจัยสำคัญที่ช่วยให้บุคลากรและองค์กรสามารถดำเนินงานได้อย่างมั่นคงและปลอดภัยในยุคดิจิทัลนี้

การป้องกันภัยคุกคามทางไซเบอร์จำเป็นต้องมีการเสริมสร้างความรู้และความเข้าใจด้านความปลอดภัยของสารสนเทศให้กับบุคลากรทุกระดับ ทั้งผู้ดูแลระบบและผู้ใช้งานทั่วไป เพื่อให้เกิดความตระหนักและพฤติกรรมที่เหมาะสมในการใช้สารสนเทศอย่างปลอดภัย นอกจากนี้ การออกแบบระบบเครือข่ายต้องคำนึงถึงความมั่นคงปลอดภัยมากกว่าความสะดวกในการเข้าถึง และควรมีการอัปเดตอุปกรณ์และซอฟต์แวร์ให้ทันสมัยอยู่เสมอ การสำรองข้อมูลควรมีความเพียงพอและจัดเก็บในสถานที่ที่ปลอดภัย รวมถึง การมีมาตรการควบคุม ติดตาม และบังคับใช้นโยบายด้านความปลอดภัยอย่างเคร่งครัด การจัดการสารสนเทศที่มีประสิทธิภาพจะช่วยให้ระบบมีความมั่นคงและยั่งยืนในระยะยาว ทั้งนี้ การสร้างแนวทางปฏิบัติที่ชัดเจนและการฝึกอบรมอย่างต่อเนื่องจะช่วยลดความเสี่ยงจากภัยคุกคามทางไซเบอร์และเพิ่มประสิทธิภาพในการจัดการความปลอดภัยของข้อมูลในองค์กร [14]

2.4.7 การติดตามและตรวจสอบความปลอดภัยทางไซเบอร์

การติดตามและตรวจสอบความปลอดภัยทางไซเบอร์มีความสำคัญอย่างยิ่งในการสร้างความมั่นคงและประสิทธิผลของระบบสารสนเทศ โดยปัจจัยเหล่านี้ประกอบด้วยการวางแผนและการบริหารจัดการที่ มีประสิทธิภาพ การควบคุมและกำกับดูแลการใช้งานสารสนเทศ การสร้างความรู้และการตระหนักรู้ในเรื่องความปลอดภัยของสารสนเทศ รวมถึงการปรับปรุงและพัฒนาพฤติกรรมการใช้งานสารสนเทศอย่างต่อเนื่อง ทั้งนี้ การติดตามและตรวจสอบความปลอดภัยทางไซเบอร์ต้องมีการกำหนดสิทธิการเข้าถึงข้อมูลที่เหมาะสม การรักษาความปลอดภัยของฐานข้อมูลและการสำรองข้อมูล การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ และการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศอย่างมีประสิทธิภาพ ซึ่งทั้งหมดนี้จะช่วยให้ระบบสารสนเทศมีความปลอดภัยและสามารถรับมือกับภัยคุกคามทางไซเบอร์

การติดตามและตรวจสอบนี้ประกอบด้วยการวิเคราะห์และประเมินผลระบบการรักษาความปลอดภัยอย่างต่อเนื่อง เพื่อให้มั่นใจว่ามาตรการที่มีอยู่สามารถป้องกันภัยคุกคามได้อย่างมีประสิทธิภาพ การฝึกอบรมและให้ความรู้แก่พนักงานเกี่ยวกับวิธีการรักษาความปลอดภัยทางไซเบอร์เป็นอีกหนึ่งปัจจัยสำคัญที่ช่วยเพิ่มความตระหนักรู้และความสามารถในการป้องกันภัยคุกคาม นอกจากนี้ การข่มขู่ ยับยั้ง และลงโทษผู้ที่ฝ่าฝืนนโยบายความปลอดภัยยังเป็นมาตรการที่ช่วยเสริมสร้างวินัยและความรับผิดชอบในการปฏิบัติตามนโยบายขององค์กร การมีความรู้ความเข้าใจในระบบสารสนเทศและภัยคุกคามทางไซเบอร์ช่วยให้พนักงานสามารถรับมือกับสถานการณ์ต่าง ๆ ได้อย่างมีประสิทธิภาพ [14],[15]

2.5 แนวทางในการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร

กระบวนการสร้างความตระหนักรู้ด้านภัยคุมคามทางไซเบอร์ เป็นการเปลี่ยนทัศนคติและสร้างวัฒนธรรมทางความมั่นคงปลอดภัยไซเบอร์ที่หยั่งรากลึกในระดับบุคคลและองค์กรให้เกิดภูมิคุ้มกันและมีจริยธรรมทางความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้เพื่อสร้างความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ อีกทั้งยังทำให้บุคคลและองค์กรมีขีดความสามารถด้านไซเบอร์ ในอันที่จะป้องกัน ต่อต้าน ตรวจจับ และตอบสนองต่อการบุกรุก การจารกรรม หรือการหลอกลวงที่จะทำให้เกิดความเสียหายได้ โดยจากปัจจัยที่ทำการศึกษามาสามารถนำมาเป็นแนวทางในการสร้างความตระหนักรู้ได้ดังนี้

2.5.1 การฝึกอบรมและการให้ความรู้

การฝึกอบรมและให้ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ เป็นวิธีสำคัญในการสร้างความตระหนักรู้และเสริมทักษะการป้องกันตนเองให้กับบุคลากรและผู้ใช้ทั่วไป การจัดอบรมเป็นระยะ การทำแบบทดสอบออนไลน์ หรือการจำลองเหตุการณ์โจมตีทางไซเบอร์ สามารถช่วยให้ผู้เข้าร่วมมีความเข้าใจในแนวทางการปฏิบัติตัวที่ปลอดภัยในการใช้งานอินเทอร์เน็ตและระบบดิจิทัล เพื่อลดความเสี่ยงจากการโจมตีไซเบอร์ในอนาคต [16],[17]

2.5.2 การสร้างวัฒนธรรมความปลอดภัยไซเบอร์ในองค์กร

การสร้างวัฒนธรรมที่เน้นความปลอดภัยทางไซเบอร์ในองค์กรช่วยส่งเสริมให้ทุกคนมีส่วนร่วมในการป้องกันภัยคุกคาม ด้วยการสร้างความเข้าใจว่านโยบายความปลอดภัยไม่ใช่หน้าที่ของฝ่ายไอทีเพียงอย่างเดียว การสื่อสารเกี่ยวกับนโยบาย การมีส่วนร่วมของพนักงานในกิจกรรมป้องกัน และการติดตามผลอย่างสม่ำเสมอ ช่วยลดโอกาสที่พนักงานจะทำพลาดจากการเปิดเผยข้อมูลสำคัญหรือเผลอเปิดประตูให้แก่ผู้ไม่หวังดีเข้าถึงระบบขององค์กร [18],[19]

2.5.3 การใช้เทคโนโลยีที่ทันสมัย

การนำเทคโนโลยีป้องกันความปลอดภัยที่ทันสมัยมาใช้ เช่น การป้องกันมัลแวร์ การเข้ารหัสข้อมูล และการตรวจสอบสิทธิการเข้าถึง เป็นต้น จะช่วยเพิ่มความปลอดภัยให้กับระบบขององค์กรและข้อมูลของผู้ใช้งาน เทคโนโลยีที่ทันสมัยสามารถตรวจจับและป้องกันภัยคุกคามได้อย่างรวดเร็วและแม่นยำ พร้อมทั้งเสริมสร้างระบบการตอบสนองต่อเหตุการณ์ที่มีประสิทธิภาพมากยิ่งขึ้น ช่วยลดความเสี่ยงในการถูกโจมตี [20],[21],[22]

2.5.4 การส่งเสริมการใช้นโยบายความปลอดภัยภายในองค์กร

การมีนโยบายด้านความปลอดภัยไซเบอร์ที่ชัดเจนในองค์กรจะช่วยให้บุคลากรมีแนวทางการปฏิบัติที่เหมาะสมและปลอดภัย นโยบายควรครอบคลุมถึงการจัดการรหัสผ่าน การใช้งานอินเทอร์เน็ต การสำรองข้อมูล และการจัดการกับข้อมูลสำคัญ นอกจากนี้ การกำหนดขั้นตอนการรับมือกับเหตุการณ์การโจมตี การฟื้นฟูระบบหลังการโจมตี จะช่วยลดความเสี่ยงและป้องกันการสูญเสียข้อมูลได้อย่างมีประสิทธิภาพ [23]

2.5.5 การประเมินผลและปรับปรุงอย่างต่อเนื่อง

ภัยคุกคามทางไซเบอร์มีการเปลี่ยนแปลงตลอดเวลา ดังนั้นการประเมินและปรับปรุงมาตรการความปลอดภัยเป็นระยะจึงจำเป็นเพื่อให้แน่ใจว่าระบบยังคงสามารถป้องกันการโจมตีรูปแบบใหม่ ๆ ได้อย่างมีประสิทธิภาพ การตรวจสอบระบบอย่างต่อเนื่อง การทดสอบความปลอดภัย และการปรับปรุงมาตรการใหม่ ๆ จะช่วยให้ระบบมีความแข็งแรงพร้อมรับมือกับภัยคุกคามได้ในทุกสถานการณ์ [24]

บทที่ 3
วิธีการดำเนินการวิจัย

วิจัยฉบับนี้เป็นงานวิจัยเชิงสำรวจ (Survey Research) มุ่งเน้นการเก็บชุดข้อมูลความคิดเห็น ที่มีอิทธิพลต่อแนวทางในการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร จึงทำการสำรวจกลุ่มประชากรตัวอย่าง พร้อมใช้เครื่องมือในแบบสอบถาม ประกอบเข้ากับการวิเคราะห์ผลจากโปรแกรมสำเร็จ เพื่อวิเคราะห์ข้อมูลทางสถิติ และนำแปรผล โดยได้การศึกษาผลวิจัยดังกล่าวตามลำดับดังนี้ ซึ่งประกอบไปด้วยขั้นตอนดังต่อไปนี้

3.1 โมเดลแนวคิดงานวิจัย

3.2 ประชากรและกลุ่มตัวอย่าง

3.3 การสร้างเครื่องมือที่ใช้ในการศึกษา

3.4 การหาคุณภาพของเครื่องมือจากผู้เชี่ยวชาญ

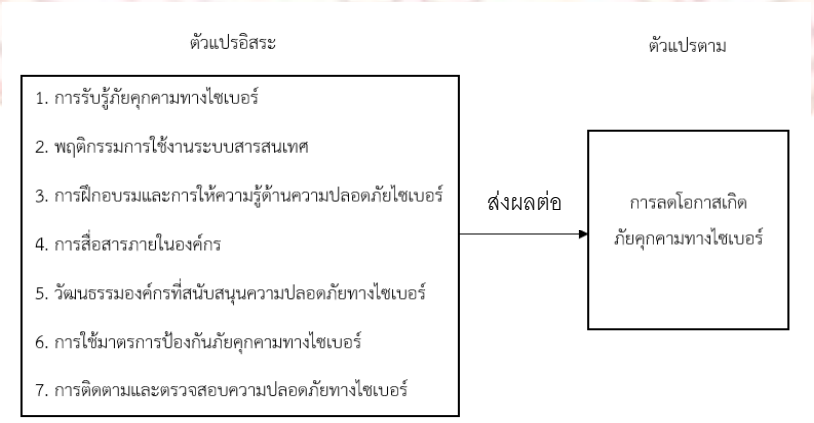
3.5 การหาความเชื่อมั่นของผลแบบสอบถามจากกลุ่มตัวอย่าง

3.6 การเก็บแบบสอบถามจากประชากรกลุ่มตัวอย่าง

3.7 การวิเคราะห์ข้อมูล

3.1 โมเดลงานวิจัย

จากการศึกษาทฤษฎีและงานวิจัยที่เกี่ยวข้อง พบว่า แนวทางในการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กรในเขตพื้นที่กรุงเทพมหานครและปริมณฑล ประกอบด้วยปัจจัยที่ส่งผลให้ลดโอกาสเกิดภัยคุกคามทางไซเบอร์ จำนวน 7 ปัจจัย ดังนั้นผู้วิจัยจึงสรุปโมเดลงานวิจัยได้ ดังนี้



ภาพที่ 3-1 โมเดลการวิเคราะห์ปัจจัยที่ส่งผลให้ลดโอกาสเกิดภัยคุกคามทางไซเบอร์

3.2 ประชากรและกลุ่มตัวอย่าง

การวิจัยนี้ผู้วิจัยได้กาหนดขอบเขตการวิจัยแบ่งออกเป็น 2 ด้าน คือ ขอบเขตด้านประชากรและกลุ่มตัวอย่าง และขอบเขตด้านเนื้อหาการวิจัย ดังนี้

3.2.1 ขอบเขตด้านประชากรและกลุ่มตัวอย่าง

ประชากร คือ ผู้ใช้งานระบบและข้อมูลคอมพิวเตอร์ผ่านเครือข่ายอินเทอร์เน็ตในเขตพื้นที่กรุงเทพมหานครและปริมณฑล โดยการสำรวจจากประชากรในเขตพื้นที่กรุงเทพมหานครและปริมณฑลตามหลักฐาน การทะเบียนราษฎรที่มีจานวนประชากรมากถึง 10,944,863 คนหรือประมาณร้อยละ 16.44 ของประชากรทั่วประเทศ [3] และมีสถิติในการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือน พ.ศ. 2561 ซึ่งใช้งานผ่านอุปกรณ์อิเล็กทรอนิกส์ที่เชื่อมต่อกับเครือข่ายอินเทอร์เน็ตคิดเป็นร้อยละ 30.67 ของการใช้งานถือได้ว่า ประชากรในเขตพื้นที่กรุงเทพมหานครและปริมณฑลเป็นประชาชนส่วนใหญ่ของประเทศไทยที่มีการใช้ระบบและข้อมูลคอมพิวเตอร์

กลุ่มตัวอย่าง คือ ผู้ใช้งานระบบและข้อมูลคอมพิวเตอร์ผ่านเครือข่ายอินเทอร์เน็ต ซึ่งผู้วิจัยได้ทำ การสำรวจข้อมูลผ่านทางแบบสอบถาม (Questionnaire) จำนวน 400 คน โดยการหาขนาดกลุ่มตัวอย่างจากตารางสำเร็จของทาโร่ ยามาเน่ ที่ระดับความคลาดเคลื่อนร้อยละ 5 หรือระดับความเชื่อมั่นร้อยละ 95

3.2.2 ขอบเขตด้านเนื้อหาการวิจัย

การวิจัยนี้เป็นศึกษาความตระหนักรู้ด้านภัยคุมคามทางไซเบอร์ ปัจจุบันเนื่องจากภัยคุกคามทางไซเบอร์มีความซับซ้อนและรุนแรงมากขึ้น การเข้าใจและการรับมือกับภัยคุกคามทางไซเบอร์เป็นสิ่งจำเป็นที่องค์กรและบุคคลทั่วไปต้องมี เพื่อลดความเสี่ยงและปกป้องข้อมูลสำคัญจากการโจมตี ต่าง ๆ ทั้งการศึกษาวิธีการป้องกัน การสร้างความตระหนักรู้ในบุคลากร และการพัฒนานโยบายความปลอดภัยที่เข้มแข็ง เพื่อให้โลกดิจิทัลเป็นที่ปลอดภัยและเชื่อถือได้มากยิ่งขึ้น

3.3 การสร้างเครื่องมือที่ใช้ในการศึกษา

ในการศึกษาค้นคว้าวิจัยครั้งนี้ ได้มีการศึกษาทฤษฎีกระบวนการวิจัยที่เกี่ยวข้องจากเล่มวิจัย การสร้างเครื่องมือแบบสอบถาม ประกอบด้วย 2 ส่วน ได้แก่ ส่วนที่ 1 คำถามทั่วไป สำหรับคัดกรองกลุ่มประชากรกลุ่มซึ่งประกอบด้วย 5 ข้อคำถามเกี่ยวกับ เพศ อายุ ระดับการศึกษา ประสบการณ์การทำงาน และประเภทอาชีพ และส่วนที่ 2 คำถามเกี่ยวกับปัจจัยที่ส่งผลให้ลดโอกาสเกิดภัยคุกคามทางไซเบอร์ทั้งหมด 34 ข้อ โดยลักษณะแบบสอบถามเป็นแบบมาตรวัด 5 ระดับ แบ่งออกเป็น 8 หัวข้อ ประกอบด้วยคำถามเกี่ยวกับการรับรู้ภัยคุกคามทางไซเบอร์ พฤติกรรมการใช้งานระบบสารสนเทศ การฝึกอบรมและการให้ความรู้ด้านความปลอดภัยไซเบอร์ การสื่อสารภายในองค์กร วัฒนธรรมองค์กรที่สนับสนุนความปลอดภัยทางไซเบอร์ การใช้มาตรการป้องกันภัยคุกคามทางไซ

เบอร์ การติดตามและตรวจสอบความปลอดภัยทางไซเบอร์ และการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร

3.4 การหาคุณภาพของเครื่องมือจากผู้เชี่ยวชาญ

การหาค่าความเที่ยงตรงของแบบสอบถาม (Index of Item Objective Congruence) เป็นวิธีการพิจารณาคุณภาพข้อคำถาม ด้านความเหมาะสม ความถูกต้อง ครบถ้วน มีเนื้อหาสอดคล้องตรงกับวัตถุประสงค์ และสมมติฐานของงานวิจัย (Content Validity) จึงจำเป็นต้องอาศัยการประเมินความคิดเห็นของผู้เชี่ยวชาญเกี่ยวกับเนื้อหาในแบบสอบถาม โดยกำหนดผู้เชี่ยวชาญ 3 ท่าน และกำหนดระดับเกณฑ์การตัดสินดังนี้

การทดสอบความเที่ยงตรงของเนื้อหา (Index of Item-Objective Congruence : IOC) นำมาหาค่าดัชนีความสอดคล้องระหว่างคำถามกับวัตถุประสงค์การวิจัยจากสูตรของ Riviovelli and Hambleton (1977) ซึ่งสูตรในการคำนวณที่ใช้ในการหาค่า IOC ดังนี้

$$IOC = \Sigma R/N \qquad (3\text{-}1)$$

IOC	หมายถึง	ค่าดัชนีความสอดคล้อง
ΣR	หมายถึง	ผลรวมของคะแนนความคิดเห็นของผู้เชี่ยวชาญ
N	หมายถึง	จำนวนของผู้เชี่ยวชาญ

โดยที่ ความหมายของคะแนนมีดังนี้

+ 1	หมายถึง	เหมาะสมสอดคล้องตรงกับวัตถุประสงค์
0	หมายถึง	ไม่แน่ใจว่ามีความสอดคล้องวัตถุประสงค์
– 1	หมายถึง	ไม่สอดคล้องไม่ตรงกับวัตถุประสงค์

ทั้งนี้ เกณฑ์การประเมิน หากค่า IOC อยู่ระหว่าง 0.50-1.00 คะแนน แปลว่าข้อคำถามนั้นใช้ได้ แต่ถ้าค่า IOC ต่ำกว่า 0.50 คะแนน จะต้องพิจารณาปรับปรุงหรือตัดทิ้ง

จากแบบสอบถามที่ได้สร้างขึ้นตามสูตร 3-1 มีการปรับแต่งให้สอดคล้องกับวัตถุประสงค์ โดยสร้างข้อคำถามให้มีความกระชับมากขึ้น รวมถึงตัดคำถามที่ ไม่จำเป็นออกไป เมื่อผ่านการตรวจสอบจากอาจารย์ที่ปรึกษาแล้ว หลังจากนั้นจึงนำไปให้ผู้เชี่ยวชาญทั้ง 3 ท่าน ทำการประเมินค่าความสอดคล้องของแบบสอบถาม และนำผลคะแนนของผู้เชี่ยวชาญมาทำการวิเคราะห์หาค่าความสอดคล้องแสดงดังตารางที่ 3-1

ตารางที่ 3-1 แสดงการประเมินค่าความเที่ยงตรงของแบบสอบถาม

รายการประเมิน		ผู้เชี่ยวชาญ			รวม	ค่า IOC	แปรผล
		1	2	3			
การรับรู้ภัยคุกคามทางไซเบอร์							
1.	ท่านคิดว่าการไม่เปิดเผยระบุตัวตนบนเครือข่ายสังคมออนไลน์สาธารณะที่มีผู้ใช้ทั่วไปมีความปลอดภัย	+1	+1	0	2	0.67	สอดคล้อง
2.	ท่านคิดว่าการไม่ให้ข้อมูลส่วนตัวบนเครือข่ายสังคมสาธารณะมีความปลอดภัย	+1	+1	+1	3	1	สอดคล้อง
3.	ท่านคิดว่าการเข้าเว็บไซต์ http มีความปลอดภัยน้อยกว่า https	+1	+1	+1	3	1	สอดคล้อง
4.	ท่านคิดว่าการไม่ซื้อโปรแกรมที่ถูกลิขสิทธิ์มาใช้งานมีความเสี่ยงต่อระบบคอมพิวเตอร์คล้ายคลึงกับโปรแกรมที่แชร์ให้โหลดได้ฟรีในอินเทอร์เน็ต	+1	+1	+1	3	1	สอดคล้อง
5.	ท่านคิดว่าการกำหนดผู้ใช้งานและรหัสผ่านก่อนเข้าสู่ระบบคอมพิวเตอร์ก่อให้เกิดความปลอดภัยในการเข้าใช้งาน	+1	+1	+1	3	1	สอดคล้อง
พฤติกรรมการใช้งานระบบสารสนเทศ							
6.	ท่านไม่อนุญาตให้บุคคลที่ไม่รู้จักเข้าถึงการใช้งานบน Social Media ของตนเอง	+1	+1	+1	3	1	สอดคล้อง
7.	ท่านมีการใช้งานผ่านโปรแกรมที่มีลิขสิทธิ์	+1	+1	+1	3	1	สอดคล้อง

ตารางที่ 3-1 (ต่อ)

รายการประเมิน		ผู้เชี่ยวชาญ			รวม	ค่า IOC	แปรผล
8.	ท่านมีการดาวน์โหลดไฟล์โดยทราบแหล่งที่มาออนไลน์	+1	+1	+1	3	1	สอดคล้อง
9.	ท่านมีการเข้าเว็บไซต์เฉพาะที่เหมาะสมและปลอดภัย	+1	+1	+1	3	1	สอดคล้อง
10.	ท่านติดตั้งโปรแกรมต่าง ๆ โดยพิจารณาจากแหล่งที่มาที่น่าเชื่อถือ	+1	+1	+1	3	1	สอดคล้อง
การฝึกอบรมและการให้ความรู้ด้านความปลอดภัยไซเบอร์							
11.	องค์กรมีการการฝึกอบรมสร้างความตระหนักรู้ด้านความปลอดภัย	+1	+1	+1	3	1	สอดคล้อง
12.	องค์กรมีการการสนับสนุนบุคลากรในการพัฒนาทักษะด้านความมั่นคงปลอดภัยไซเบอร์	+1	+1	+1	3	1	สอดคล้อง
13.	บุคลากรสามารถถ่ายทอดความรู้ด้านความมั่นคงปลอดภัยระหว่างกันในองค์กร	+1	+1	+1	3	1	สอดคล้อง
14.	องค์กรของท่านมีการฝึกอบรมวิธีการใช้สารสนเทศอย่างปลอดภัย	+1	+1	+1	3	1	สอดคล้อง
15.	องค์กรของท่านมีการให้ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กรอยู่เสมอ	+1	+1	+1	3	1	สอดคล้อง
การสื่อสารภายในองค์กร							
16.	องค์กรมีการเผยแพร่ความรู้ด้านการรับมือภัยคุกคามทางไซเบอร์	+1	+1	+1	3	1	สอดคล้อง

ตารางที่ 3-1 (ต่อ)

รายการประเมิน		ผู้เชี่ยวชาญ			รวม	ค่า IOC	แปรผล
17.	องค์กรมีการเผยแพร่แผนการรับมือภัยคุกคามทางไซเบอร์	+1	+1	+1	3	1	สอดคล้อง
18.	องค์กรมีแนวทางให้บุคลากรได้เรียนรู้ประสบการณ์ด้านไซเบอร์ร่วมกัน	+1	+1	+1	3	1	สอดคล้อง
19.	องค์กรมีการเผยแพร่นโยบายและแนวปฏิบัติให้บุคลากรในหน่วยงานได้รับทราบและปฏิบัติ	+1	+1	+1	3	1	สอดคล้อง
วัฒนธรรมองค์กรที่สนับสนุนความปลอดภัยทางไซเบอร์							
20.	บุคลากรมีความสามารถถ่ายทอดความรู้ด้านความมั่นคงปลอดภัยระหว่างกันในองค์กร	+1	+1	+1	3	1	สอดคล้อง
21.	บุคลากรมีความเชื่อมั่นในมาตรการปกป้องข้อมูลส่วนบุคคลในองค์กร	+1	+1	+1	3	1	สอดคล้อง
22.	บุคลากรมีความไว้วางใจในระบบเครือข่ายขององค์กร	+1	+1	+1	3	1	สอดคล้อง
23.	บุคลากรมีความพร้อมและให้ความร่วมมือในการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับองค์กร	+1	+1	+1	3	1	สอดคล้อง
การใช้มาตรการป้องกันภัยคุกคามทางไซเบอร์							
24.	องค์กรมีการกำหนดสิทธิ หน้าที่ความรับผิดชอบในการบริหารจัดการข้อมูลของแต่ละส่วนงาน	+1	+1	+1	3	1	สอดคล้อง
25.	องค์กรมีการกำหนดนโยบาย/กฎเกณฑ์การเข้าถึงและใช้ประโยชน์จากข้อมูล	+1	+1	+1	3	1	สอดคล้อง

ตารางที่ 3-1 (ต่อ)

รายการประเมิน		ผู้เชี่ยวชาญ			รวม	ค่า IOC	แปรผล
26.	องค์กรมีแนวทางการดำเนินการปกปิดข้อมูลส่วนบุคคล	+1	+1	+1	3	1	สอดคล้อง
27.	องค์กรมีการกำหนดมาตรการหรือกระบวนการตรวจสอบและประเมินคุณภาพข้อมูล	+1	+1	+1	3	1	สอดคล้อง
การติดตามและตรวจสอบความปลอดภัยทางไซเบอร์							
28.	องค์กรมีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยไซเบอร์	+1	+1	+1	3	1	สอดคล้อง
29.	องค์กรมีการตรวจสอบระบบสารสนเทศ (IT Audit)	+1	+1	+1	3	1	สอดคล้อง
30.	องค์กรของท่านมีการตรวจสอบการปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงานอยู่เสมอ	+1	+1	+1	3	1	สอดคล้อง
31.	องค์กรของท่านมีการประเมินเพื่อหาแนวทางการป้องกันภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ร่วมกับผู้ที่เกี่ยวข้องอย่างสม่ำเสมอ	+1	+1	+1	3	1	สอดคล้อง
32.	องค์กรของท่านมีการทบทวน ติดตาม และตรวจสอบด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างต่อเนื่อง	+1	+1	+1	3	1	สอดคล้อง

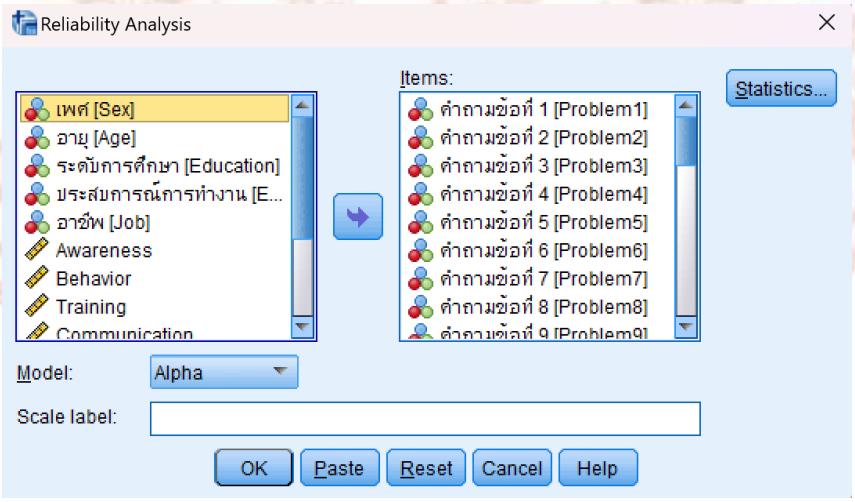
ตารางที่ 3-1 (ต่อ)

รายการประเมิน		ผู้เชี่ยวชาญ			รวม	ค่า IOC	แปรผล
การลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร							
33.	ในปีที่ผ่านมา องค์กรของท่านได้รับความเสียหายจากภัยคุกคามทางไซเบอร์โดยรวมไม่เกิน 1-2 ครั้ง	+1	0	+1	2	0.67	สอดคล้อง
34.	องค์กรของท่านมีโอกาสในการเกิดภัยคุกคามทางไซเบอร์ลดลงในอนาคต	+1	+1	+1	3	1	สอดคล้อง
ค่า IOC เฉลี่ยรวม						0.96	

จากตาราง 3-1 สรุปได้ว่าข้อคำถามมีค่าความเหมาะสม และสอดคล้องกับวัตถุประสงค์สามารถนำไปหาความเชื่อมั่นในขั้นตอนต่อไปได้

3.5 การหาความเชื่อมั่นของผลแบบสอบถามจากกลุ่มตัวอย่าง (Reliability)

วิธีหาค่าความเชื่อมั่นที่นำมาใช้ คือ การหาสัมประสิทธิ์แอลฟาของครอนบาค (Cronbach's Alpha Coefficient) โดยเก็บรวบรวมผลการทำแบบสอบถามจากกลุ่มตัวอย่างทั้งหมด 34 ชุดเพื่อนำมาทดสอบหาค่าความเชื่อมั่นบนโปรแกรม SPSS อ้างอิงตามวิธีของครอนบาค ควรมีค่าร้อยละ 0.70 ขึ้นไป จึงถือว่าค่าความเชื่อมั่นอยู่ในเกณฑ์สูง และเป็นที่ยอมรับในการทำแบบสอบถามในงานวิจัย



ภาพที่ 3-2 แสดงวิธีการหาค่าความเชื่อมั่น

จากภาพประกอบข้อคำถามทั้งหมดได้ถูกวิเคราะห์ผลบนโปรแกรม SPSS และแสดงผลลัพธ์ของค่าสัมประสิทธิ์แอลฟาของครอนบาค ดังนี้

Reliability Statistics

Cronbach's Alpha	N of Items
.966	34

ภาพที่ 3-3 ค่าสัมประสิทธิ์แอลฟาของครอนบาค

จากผลการตรวจสอบข้อคำถามในแบบสอบถามมีจำนวนทั้งสิ้น 34 ข้อคำถาม ซึ่งนำมาวิเคราะห์ความน่าเชื่อถือของ แบบสอบถามด้วยวิธีหาค่าสัมประสิทธิ์ครอนบาค จากการวิเคราะห์พบว่าค่าสัมประสิทธิ์ครอนบาคอยู่ในระดับ 0.966 แสดงให้เห็นว่าแบบสอบถามมีความเที่ยงตรง และสามารถนำไปใช้ในงานวิจัยได้

3.6 การเก็บแบบสอบถามจากประชากรกลุ่มตัวอย่าง

เนื่องจากมีจำนวนประชากรจำนวน 400 คนที่นำมาศึกษา โดยใช้ระยะเวลาเก็บข้อมูลตั้งแต่ธันวาคม 2567 ถึง มกราคม 2568 โดยเครื่องมือที่ใช้คือ Google Form โดยได้มาเป็นจำนวน 411 ชุด

3.7 การวิเคราะห์ข้อมูล

หลังจากที่ได้รวบรวมข้อมูลครบทั้งหมด 411 ชุด ผู้วิจัยได้นำมาประมวลผลด้วยโปรแกรม SPSS ประกอบด้วยการวิเคราะห์ข้อมูล 2 ข้อ

3.7.1 การวิเคราะห์ข้อมูลสถิติเชิงพรรณนา (Descriptive Statistics)

กลุ่มประชากรจะถูกวิเคราะห์ แปลผลข้อมูลออกมาในรูปแบบของการแจงแจกความถี่ (Frequency) ค่าร้อยละ (Percentage) ค่าเฉลี่ย (Mean) และค่าส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) เพื่อนำมาอธิบายถึงประชากรทั้งหมด กำหนดความคิดเห็นออกเป็น 5 ระดับ

ตารางที่ 3-2 เกณฑ์กำหนดระดับความคิดเห็น

ระดับความคิดเห็น	แปลผล
เห็นด้วยอย่างยิ่ง	5
เห็นด้วยมาก	4
เห็นด้วยปานกลาง	3
ไม่เห็นด้วย	2
ไม่เห็นด้วยอย่างยิ่ง	1

ทั้งนี้มีการระบุประเมินค่าเฉลี่ยตามเกณฑ์การหาความกว้างของอันตรภาคชั้น แสดงดังตารางที่ 3-3

ตารางที่ 3-3 เกณฑ์การหาความกว้างของอันตรภาคชั้น

เกณฑ์คะแนนเฉลี่ย	ระดับความคิดเห็น
4.21 – 5.00	เห็นด้วยอย่างยิ่ง
3.41 – 4.20	เห็นด้วยมาก
2.61 – 3.40	เห็นด้วยปานกลาง
1.81 – 2.60	ไม่เห็นด้วย
1.00 – 1.80	ไม่เห็นด้วยอย่างยิ่ง

ใช้อธิบายข้อมูลและลักษณะข้อมูลทั่วไปที่รวบรวมจากกลุ่มตัวอย่าง โดยนำเสนอในรูปแบบของตารางแจกแจงความถี่ ค่าร้อยละ ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน และแผนภูมิต่าง ๆ

3.7.2 การวิเคราะห์ข้อมูลเชิงอนุมาน (Inferential Statistics)

เป็นการศึกษาข้อมูลของกลุ่มตัวอย่างโดยใช้โปรแกรมสำเร็จรูปทางสถิติ SPSS ในการทดสอบสมมุติฐาน โดยใช้เครื่องมือในการวิเคราะห์ผลทางสถิติ เพื่อการวิเคราะห์การถดถอยพหุคูณ

บทที่ 4
ผลการดำเนินงานวิจัย

จากการรวบรวมข้อมูลประชากรทั้งหมด 411 คน เพื่อนำมาเปรียบเทียบ และวิเคราะห์ปัจจัยที่มีอิทธิพลต่อแนวทางในการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร ถูกนำมาวิเคราะห์ แปรผล และนำเสนอรายละเอียดด้านล่างตามลำดับ ดังต่อไปนี้

4.1 ผลการวิเคราะห์ข้อมูลด้านประชากรกลุ่มตัวอย่าง

4.2 ผลการวิเคราะห์สถิติเบื้องต้น

4.3 ผลการวิเคราะห์ถดถอยพหุคูณ

4.4 แนวทางในการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร

4.1 ผลการวิเคราะห์ข้อมูลด้านประชากรกลุ่มตัวอย่าง

สำหรับการวิจัยครั้งนี้ มีการเก็บข้อมูลจากกลุ่มประชากรโดยการใช้แบบสอบถามออนไลน์ผ่าน Google Form ซึ่งได้เริ่มเก็บข้อมูลตั้งแต่เดือนธันวาคม 2567 ถึง มกราคม 2568 ดังนี้

ตารางที่ 4-1 แสดงข้อมูลเกี่ยวกับเพศของผู้ตอบแบบสอบถาม

ข้อมูลด้านประชากร	จำนวน	ร้อยละ
เพศ		
ชาย	210	51.1
หญิง	201	48.9
รวม	411	100.0

จากตารางแสดงข้อมูลเกี่ยวกับเพศของผู้ตอบแบบสอบถาม สามารถสรุปผลการวิจัยได้ดังนี้ ผู้ตอบแบบสอบถามเพศชายมีจำนวน 210 คน คิดเป็นร้อยละ 51.1 ส่วนผู้ตอบแบบสอบถามเพศหญิงมีจำนวน 201 คน คิดเป็นร้อยละ 48.9 โดยมีจำนวนผู้ตอบแบบสอบถามทั้งหมด 411 คน จากข้อมูลข้างต้น พบว่าผู้ตอบแบบสอบถามมีสัดส่วนของเพศชายและเพศหญิงใกล้เคียงกัน โดยเพศชายมีจำนวนมากกว่าเพียงเล็กน้อย (ร้อยละ 51.1 เทียบกับร้อยละ 48.9)

ตารางที่ 4-2 แสดงข้อมูลเกี่ยวกับอายุของผู้ตอบแบบสอบถาม

ข้อมูลด้านประชากร	จำนวน	ร้อยละ
อายุ		
ต่ำกว่า 30 ปี	39	9.5
30-40 ปี	90	21.9
41-50 ปี	108	26.3
51-60 ปี	174	42.3
รวม	411	100.0

จากตารางแสดงข้อมูลเกี่ยวกับอายุของผู้ตอบแบบสอบถาม สามารถสรุปผลการวิจัยได้ดังนี้ กลุ่มอายุต่ำกว่า 30 ปี มีจำนวน 39 คน คิดเป็นร้อยละ 9.5 กลุ่มอายุ 30-40 ปี มีจำนวน 90 คน คิดเป็นร้อยละ 21.9 กลุ่มอายุ 41-50 ปี มีจำนวน 108 คน คิดเป็นร้อยละ 26.3 และกลุ่มอายุ 51-60 ปี มีจำนวน 174 คน คิดเป็นร้อยละ 42.3 โดยมีจำนวนผู้ตอบแบบสอบถามทั้งหมด 411 คน จากข้อมูลข้างต้น พบว่าผู้ตอบแบบสอบถามส่วนใหญ่อยู่ในช่วงอายุ 51-60 ปี (ร้อยละ 42.3) รองลงมาคือ 41-50 ปี (ร้อยละ 26.3) ในขณะที่กลุ่มอายุต่ำกว่า 30 ปีมีจำนวนผู้ตอบแบบสอบถามน้อยที่สุด (ร้อยละ 9.5)

ตารางที่ 4-3 แสดงข้อมูลเกี่ยวกับประสบการณ์การทำงานของผู้ตอบแบบสอบถาม

ข้อมูลด้านประชากร	จำนวน	ร้อยละ
ประสบการณ์การทำงาน		
ตำกว่า 5 ปี	27	6.6
5-10 ปี	102	24.8
10 ปีขึ้นไป	282	68.6
รวม	411	100.0

จากตารางแสดงข้อมูลเกี่ยวกับประสบการณ์การทำงานของผู้ตอบแบบสอบถาม สามารถสรุปผลการวิจัยได้ดังนี้ กลุ่มที่มีประสบการณ์ทำงานต่ำกว่า 5 ปี มีจำนวน 27 คน คิดเป็นร้อยละ 6.6 กลุ่มที่มีประสบการณ์ทำงาน 5-10 ปี มีจำนวน 102 คน คิดเป็นร้อยละ 24.8 กลุ่มที่มีประสบการณ์ทำงาน 10 ปีขึ้นไป มีจำนวน 282 คน คิดเป็นร้อยละ 68.6 โดยมีจำนวนผู้ตอบแบบสอบถามทั้งหมด 411 คน จากข้อมูลข้างต้น พบว่าผู้ตอบแบบสอบถามส่วนใหญ่มีประสบการณ์ทำงาน 10 ปีขึ้นไป (ร้อยละ 68.6) รองลงมาคือกลุ่มที่มีประสบการณ์ 5-10 ปี (ร้อยละ 24.8) ขณะที่กลุ่มที่มีประสบการณ์ต่ำกว่า 5 ปีมีจำนวนผู้ตอบแบบสอบถามน้อยที่สุด (ร้อยละ 6.6) ซึ่งแสดงให้เห็นว่ากลุ่มตัวอย่างส่วนมากเป็นผู้ที่มีประสบการณ์การทำงานมายาวนาน

ตารางที่ 4-4 แสดงข้อมูลเกี่ยวกับอาชีพของผู้ตอบแบบสอบถาม

ข้อมูลด้านประชากร	จำนวน	ร้อยละ
อาชีพ		
พนังงานบริษัทเอกชน	42	10.2
พนักงาน/ข้าราชการ	318	77.4
เจ้าของธุรกิจ/ธุรกิจส่วนตัว	51	12.4
รวม	411	100.0

จากตารางแสดงข้อมูลเกี่ยวกับอาชีพของผู้ตอบแบบสอบถาม สามารถสรุปผลการวิจัยได้ดังนี้ กลุ่มพนักงานบริษัทเอกชน มีจำนวน 42 คน คิดเป็นร้อยละ 10.2 กลุ่มพนักงาน/ข้าราชการ มีจำนวน 318 คน คิดเป็นร้อยละ 77.4 กลุ่มเจ้าของธุรกิจ/ธุรกิจส่วนตัว มีจำนวน 51 คน คิดเป็นร้อยละ 12.4 โดยมีจำนวนผู้ตอบแบบสอบถามทั้งหมด 411 คน จากข้อมูลข้างต้น พบว่าผู้ตอบแบบสอบถามส่วนใหญ่ประกอบอาชีพพนักงาน/ข้าราชการ (ร้อยละ 77.4) รองลงมาคือกลุ่มเจ้าของธุรกิจ/ธุรกิจส่วนตัว (ร้อยละ 12.4) ขณะที่กลุ่มพนักงานบริษัทเอกชนมีจำนวนผู้ตอบแบบสอบถามน้อยที่สุด (ร้อยละ 10.2) ซึ่งแสดงให้เห็นว่ากลุ่มตัวอย่างส่วนมากเป็นผู้ที่ทำงานในภาครัฐ

ตารางที่ 4-5 แสดงข้อมูลเกี่ยวกับระดับการศึกษาของผู้ตอบแบบสอบถาม

ข้อมูลด้านประชากร	จำนวน	ร้อยละ
ระดับการศึกษา		
ต่ำกว่าปริญญาตรี	42	10.2
ปริญญาตรี	255	62.0
ปริญญาโท	102	24.8
ปริญญาเอก	12	2.9
รวม	411	100.0

จากตารางแสดงข้อมูลเกี่ยวกับระดับการศึกษาของผู้ตอบแบบสอบถาม สามารถสรุปผลการวิจัยได้ดังนี้ กลุ่มผู้ที่มีการศึกษาต่ำกว่าปริญญาตรี มีจำนวน 42 คน คิดเป็นร้อยละ 10.2 กลุ่มผู้ที่มีการศึกษาระดับปริญญาตรี มีจำนวน 255 คน คิดเป็นร้อยละ 62.0 กลุ่มผู้ที่มีการศึกษาระดับปริญญาโท มีจำนวน 102 คน คิดเป็นร้อยละ 24.8 กลุ่มผู้ที่มีการศึกษาระดับปริญญาเอก มีจำนวน 12 คน คิดเป็นร้อยละ 2.9 โดยมีจำนวนผู้ตอบแบบสอบถามทั้งหมด 411 คน จากข้อมูลข้างต้น พบว่าผู้ตอบแบบสอบถามส่วนใหญ่มีการศึกษาระดับปริญญาตรี (ร้อยละ 62.0) รองลงมาคือกลุ่มที่มีการศึกษาระดับปริญญาโท (ร้อยละ 24.8) ขณะที่กลุ่มผู้ที่มีการศึกษาต่ำกว่าปริญญาตรีและปริญญา

เอกมีจำนวนผู้ตอบแบบสอบถามน้อยที่สุด (ร้อยละ 10.2 และ ร้อยละ 2.9 ตามลำดับ) ซึ่งแสดงให้เห็นว่ากลุ่มตัวอย่างส่วนมากมีการศึกษาสูงในระดับปริญญาตรีและปริญญาโท

4.2 ผลการวิเคราะห์สถิติเบื้องต้น

จากข้อมูลแบบสอบถามที่ได้รวบรวมมาทั้งสิ้น 411 ชุด สามารถสรุปเป็นค่าเฉลี่ย (Mean) และส่วนเบี่ยงเบนมาตรฐาน (SD) สามารถสรุปออกมา ในรูปแบบของตารางได้ดังนี้

ตารางที่ 4-6 แสดงผลการวิเคราะห์สถิติเบื้องต้นของค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานแบบรายด้าน

ตัวแปร	คำถาม	Mean	SD	แปลผล
การรับรู้ภัยคุกคามทางไซเบอร์	Problem1.ท่านคิดว่าการไม่เปิดเผยระบุตัวตนบนเครือข่ายสังคมออนไลน์สาธารณะที่มีผู้ใช้ทั่วไปมีความปลอดภัย	4.12	1.013	เห็นด้วยมาก
	Problem2.ท่านคิดว่าการไม่ให้ข้อมูลส่วนตัวบนเครือข่ายสังคมสาธารณะมีความปลอดภัย	4.45	.755	เห็นด้วยอย่างยิ่ง
	Problem3.ท่านคิดว่าการเข้าเว็บไซต์ http มีความปลอดภัยน้อยกว่า https	3.67	.938	เห็นด้วยมาก
	Problem4.ท่านคิดว่าการไม่ซื้อโปรแกรมที่ถูกลิขสิทธิ์มาใช้งานมีความเสี่ยงต่อระบบคอมพิวเตอร์คล้ายคลึงกับโปรแกรมที่แชร์ให้โหลดได้ฟรีในอินเทอร์เน็ต	4.12	.930	เห็นด้วยมาก
	Problem5.ท่านคิดว่าการกาหนดผู้ใช้งานและรหัสผ่านก่อนเข้าสู่ระบบคอมพิวเตอร์ก่อให้เกิดความปลอดภัยในการเข้าใช้งาน	4.28	.725	เห็นด้วยอย่างยิ่ง
	รวม	4.127	.554	เห็นด้วยมาก

ตารางที่ 4-6 (ต่อ)

ตัวแปร	คำถาม	Mean	SD	แปลผล
พฤติกรรมการใช้งานระบบสารสนเทศ	Problem6.ท่านไม่อนุญาตให้บุคคลที่ไม่รู้จักเข้าถึงการใช้งานบน Social Media ของตนเอง	4.50	.757	เห็นด้วยอย่างยิ่ง
	Problem7.ท่านมีการใช้งานผ่านโปรแกรมที่มีลิขสิทธิ์	4.03	.975	เห็นด้วยมาก
	Problem8.ท่านมีการดาวน์โหลดไฟล์โดยทราบแหล่งที่มาออนไลน์	3.87	1.067	เห็นด้วยมาก
	Problem9.ท่านมีการเข้าเว็บไซต์เฉพาะที่เหมาะสมและปลอดภัย	4.23	.858	เห็นด้วยอย่างยิ่ง
	Problem10.ท่านติดตั้งโปรแกรมต่าง ๆ โดยพิจารณาจากแหล่งที่มาที่น่าเชื่อถือ	4.37	.756	เห็นด้วยอย่างยิ่ง
	รวม	4.202	.617	เห็นด้วยมาก
การฝึกอบรมและการให้ความรู้ด้านความปลอดภัยไซเบอร์	Problem11.องค์กรมีการฝึกอบรมสร้างความตระหนักรู้ด้านความปลอดภัย	3.75	1.025	เห็นด้วยมาก
	Problem12.องค์กรมีการสนับสนุนบุคลากรในการพัฒนาทักษะด้านความมั่นคงปลอดภัยไซเบอร์	3.86	1.076	เห็นด้วยมาก
	Problem13.บุคลากรสามารถถ่ายทอดความรู้ด้านความมั่นคงปลอดภัยระหว่างกันในองค์กร	3.65	1.059	เห็นด้วยมาก
	Problem14.องค์กรของท่านมีการฝึกอบรมวิธีการใช้สารสนเทศอย่างปลอดภัย	3.65	1.132	เห็นด้วยมาก

ตารางที่ 4-6 (ต่อ)

การฝึกอบรมและการให้ความรู้ด้านความปลอดภัยไซเบอร์	Problem15.องค์กรของท่านมีการให้ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กรอยู่เสมอ	3.58	1.164	เห็นด้วยมาก
	รวม	3.699	.9657	เห็นด้วยมาก
การสื่อสารภายในองค์กร	Problem16.องค์กรมีการเผยแพร่ความรู้ด้านการรับมือภัยคุกคามทางไซเบอร์	3.62	1.148	เห็นด้วยมาก
	Problem17.องค์กรมีการเผยแพร่แผนการรับมือภัยคุกคามทางไซเบอร์	3.45	1.172	เห็นด้วยมาก
	Problem18.องค์กรมีแนวทางให้บุคลากรได้เรียนรู้ประสบการณ์ด้านไซเบอร์ร่วมกัน	3.47	1.089	เห็นด้วยมาก
	Problem19.องค์กรมีการเผยแพร่นโยบายและแนวปฏิบัติให้บุคลากรในหน่วยงานได้รับทราบและปฏิบัติ	3.64	1.094	เห็นด้วยมาก
	รวม	3.546	1.067	เห็นด้วยมาก
วัฒนธรรมองค์กรที่สนับสนุนความปลอดภัยทางไซเบอร์	Problem20.บุคลากรมีความสามารถถ่ายทอดความรู้ด้านความมั่นคงปลอดภัยระหว่างกันในองค์กร	3.61	1.056	เห็นด้วยมาก
	Problem21.บุคลากรมีความเชื่อมั่นในมาตรการปกป้องข้อมูลส่วนบุคคลในองค์กร	3.80	.967	เห็นด้วยมาก
	Problem22.บุคลากรมีความไว้วางใจในระบบเครือข่ายขององค์กร	3.97	.921	เห็นด้วยมาก

ตารางที่ 4-6 (ต่อ)

ตัวแปร	คำถาม	Mean	SD	แปลผล
วัฒนธรรมองค์กรที่สนับสนุนความปลอดภัยทางไซเบอร์	Problem23.บุคลากรมีความพร้อมและให้ความร่วมมือในการรักษาความมั่นคงปลอดภัยไซเบอร์สาหรับองค์กร	3.99	.901	เห็นด้วยมาก
	รวม	3.845	.856	เห็นด้วยมาก
การใช้มาตรการป้องกันภัยคุกคามทางไซเบอร์	Problem24.องค์กรมีการกาหนดสิทธิหน้าที่ความรับผิดชอบในการบริหารจัดการข้อมูลของแต่ละส่วนงาน	3.96	.948	เห็นด้วยมาก
	Problem25.องค์กรมีการกาหนดนโยบาย/กฎเกณฑ์การเข้าถึงและใช้ประโยชน์จากข้อมูล	4.01	.905	เห็นด้วยมาก
	Problem26.องค์กรมีแนวทางการดาเนินการปกปิดข้อมูลส่วนบุคคล	4.06	.935	เห็นด้วยมาก
	Problem27.องค์กรมีการกาหนดมาตรการหรือกระบวนการตรวจสอบและประเมินคุณภาพข้อมูล	3.87	.989	เห็นด้วยมาก
	รวม	3.976	.860	เห็นด้วยมาก

ตารางที่ 4-6 (ต่อ)

ตัวแปร	คำถาม	Mean	SD	แปลผล
การใช้มาตรการป้องกันภัยคุกคามทางไซเบอร์	Problem27.องค์กรมีการกาหนดมาตรการหรือกระบวนการตรวจสอบและประเมินคุณภาพข้อมูล	3.87	.989	เห็นด้วยมาก
	รวม	3.976	.860	เห็นด้วยมาก
การติดตามและตรวจสอบความปลอดภัยทางไซเบอร์	Problem28.องค์กรมีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยไซเบอร์	3.77	1.049	เห็นด้วยมาก
	Problem29.องค์กรมีการตรวจสอบระบบสารสนเทศ (IT Audit)	3.77	1.035	เห็นด้วยมาก
	Problem30.องค์กรของท่านมีการตรวจสอบการปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงานอยู่เสมอ	3.68	1.075	เห็นด้วยมาก
	Problem31.องค์กรของท่านมีการประเมินเพื่อหาแนวทางการป้องกันภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ร่วมกับผู้ที่เกี่ยวข้องอย่างสม่าเสมอ	3.66	1.105	เห็นด้วยมาก
	Problem32.องค์กรของท่านมีการทบทวน ติดตาม และตรวจสอบด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างต่อเนื่อง	3.73	1.085	เห็นด้วยมาก
	รวม	3.720	1.008	เห็นด้วยมาก

ตารางที่ 4-6 (ต่อ)

ตัวแปร	คำถาม	Mean	SD	แปลผล
การลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร	Problem33.ในปีที่ผ่านมา องค์กรของท่านได้รับความเสียหายจากภัยคุกคามทางไซเบอร์โดยรวมไม่เกิน 1-2 ครั้ง	3.26	1.397	เห็นด้วยปานกลาง
	Problem34.องค์กรของท่านมีโอกาสในการเกิดภัยคุกคามทางไซเบอร์ลดลงในอนาคต	3.60	1.200	เห็นด้วยมาก
	รวม	3.431	1.170	เห็นด้วยมาก

ตารางที่ 4-7 แสดงผลการวิเคราะห์ความคิดเห็นเกี่ยวกับปัจจัยที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

หัวข้อ	Mean	SD	แปลผล
การรับรู้ภัยคุกคามทางไซเบอร์	3.431	1.170	เห็นด้วยมาก
พฤติกรรมการใช้งานระบบสารสนเทศ	4.202	.617	เห็นด้วยมาก
การฝึกอบรมและการให้ความรู้ด้านความปลอดภัยไซเบอร์	3.699	.9657	เห็นด้วยมาก
การสื่อสารภายในองค์กร	3.546	1.067	เห็นด้วยมาก
วัฒนธรรมองค์กรที่สนับสนุนความปลอดภัยทางไซเบอร์	3.845	.856	เห็นด้วยมาก
การใช้มาตรการป้องกันภัยคุกคามทางไซเบอร์	3.976	.860	เห็นด้วยมาก
การติดตามและตรวจสอบความปลอดภัยทางไซเบอร์	3.720	1.008	เห็นด้วยมาก
การลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร	3.431	1.170	เห็นด้วยมาก

จากตารางแสดงผลการวิเคราะห์ความคิดเห็นเกี่ยวกับปัจจัยที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ สามารถสรุปผลการวิจัยได้ดังนี้ พฤติกรรมการใช้งานระบบสารสนเทศ ได้ค่าเฉลี่ย (Mean) สูงสุดที่ 4.202 คะแนนและส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation หรือ SD) 0.617 คะแนน แสดงว่าผู้ตอบแบบสอบถามมีความคิดเห็น เห็นด้วยมาก กับพฤติกรรมการใช้งานระบบสารสนเทศอย่างปลอดภัย การใช้มาตรการป้องกันภัยคุกคามทางไซเบอร์ มีค่าเฉลี่ยเท่ากับ 3.976 คะแนนและส่วนเบี่ยงเบนมาตรฐาน 0.860 คะแนนแสดงว่าผู้ตอบแบบสอบถามมีความคิดเห็น เห็นด้วยมาก กับการนำมาตรการป้องกันภัยคุกคามมาใช้ วัฒนธรรมองค์กรที่สนับสนุนความปลอดภัยทางไซเบอร์ มีค่าเฉลี่ยเท่ากับ 3.845 คะแนนและ ส่วนเบี่ยงเบนมาตรฐาน 0.856 คะแนนซึ่งสะท้อนให้เห็นว่าองค์กรมีการสนับสนุนด้านความปลอดภัยไซเบอร์ในระดับที่ดี การฝึกอบรมและการให้ความรู้ด้านความ

ปลอดภัยไซเบอร์ มีค่าเฉลี่ยเท่ากับ 3.699 คะแนนและ ส่วนเบี่ยงเบนมาตรฐาน 0.9657 คะแนนบ่งบอกว่าผู้ตอบแบบสอบถามให้ความสำคัญกับการอบรมในระดับที่สูง การติดตามและตรวจสอบความปลอดภัยทางไซเบอร์ มีค่าเฉลี่ยเท่ากับ 3.720 คะแนนและ ส่วนเบี่ยงเบนมาตรฐาน 1.008 คะแนน แสดงว่าการติดตามและ ตรวจสอบเป็นสิ่งที่ผู้ตอบแบบสอบถามให้ความสำคัญ การสื่อสารภายในองค์กร มีค่าเฉลี่ยเท่ากับ 3.546 และ ส่วนเบี่ยงเบนมาตรฐาน 1.067 คะแนนบ่งบอกว่าการสื่อสารเกี่ยวกับความปลอดภัยภายในองค์กรมีความสำคัญ แต่ยังมีโอกาสพัฒนาได้มากขึ้น การรับรู้ภัยคุกคามทางไซเบอร์ และ การลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร ได้ค่าเฉลี่ยเท่ากันที่ 3.431 คะแนนและ ส่วนเบี่ยงเบนมาตรฐาน 1.170 คะแนนสะท้อนว่าผู้ตอบแบบสอบถามมีความคิดเห็นว่าองค์กรมีมาตรการด้านนี้ในระดับปานกลางถึงสูง

สรุปโดยรวมแล้ว ผู้ตอบแบบสอบถามมีความคิดเห็น เห็นด้วยมาก กับทุกปัจจัยที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ ซึ่งแสดงให้เห็นว่าความตระหนักและมาตรการด้านความปลอดภัยไซเบอร์ในองค์กรอยู่ในระดับที่ดี แต่ยังมีพื้นที่สำหรับการปรับปรุงโดยเฉพาะในด้านการสื่อสารภายในองค์กรและการเสริมสร้างการรับรู้ภัยคุกคามทางไซเบอร์

4.3 ผลการวิเคราะห์ถดถอยพหุคูณ

ตารางที่ 4-8 แสดงผลการวิเคราะห์การถดถอยเชิงพหุ

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.540[a]	.292	.290	.98567	.292	168.718	1	409	.000
2	.551[b]	.304	.301	.97841	.012	7.091	1	408	.008

a. Predictors: (Constant), Communication

b. Predictors: (Constant), Communication, Behavior

c. Dependent Variable: Reduce

ผลการวิเคราะห์การถดถอยพหุคูณแบบ Stepwise เพื่อค้นหาตัวแปรที่มีผลมากที่สุดจากตาราง Model Summary แสดงปัจจัยที่มีผลต่อเป้าหมายที่ศึกษา โดยใช้ตัวแปรพยากรณ์ที่แตกต่างกันในแต่ละโมเดล สามารถสรุปผล ได้ดังนี้ ค่าความสัมพันธ์และความสามารถในการอธิบายข้อมูล ค่า R เพิ่มขึ้นเล็กน้อยเมื่อเพิ่มตัวแปรพยากรณ์ ในแต่ละโมเดล ค่า R Square เพิ่มขึ้นจาก .292

ในโมเดล ที่ 1 และเป็น .304 ในโมเดลที่ 2 แสดงว่าตัวแปรพยากรณ์ ที่เพิ่มเข้ามาช่วยอธิบายความแปรปรวนของตัวแปรตาม ได้ดีขึ้น

จากโมเดล Communication (การสื่อสารภายในองค์กร) เป็นตัวแปรที่มีอิทธิพลมากที่สุด และการเพิ่ม Behavior (พฤติกรรมการใช้งานระบบสารสนเทศ) ทาให้โมเดล ดีขึ้นเล็กน้อย แต่ไม่ได้เพิ่มความสามารถในการพยากรณ์อย่างมีนัยสาคัญ

ตารางที่ 4-9 แสดงผลการวิเคราะห์ Anova ถดถอยพหุคูณ

ANOVA						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	163.915	1	163.915	168.718	.000[b]
	Residual	397.358	409	.972		
	Total	561.274	410			
2	Regression	170.703	2	85.352	89.161	.000[c]
	Residual	390.570	408	.957		
	Total	561.274	410			
a. Dependent Variable: Reduce						
b. Predictors: (Constant), Communication						
c. Predictors: (Constant), Communication, Behavior						

จากตารางได้ข้อสรุปว่า Communication (การสื่อสารภายในองค์กร) เป็นตัวแปรหลักที่มีอิทธิพลสูงสุด เนื่องจากโมเดลที่ 1 มีค่า F เท่ากับ 168.718 ซึ่งสูงสุดในบรรดาทุกโมเดล Behavior (พฤติกรรมการใช้งานระบบสารสนเทศ) มีผลต่อโมเดล แต่ไม่ได้ช่วยเพิ่มความสามารถในการพยากรณ์อย่างมีนัยสำคัญมากนัก เพราะค่า Sum of Squares (Regression) เพิ่มขึ้นเล็กน้อย

ตารางที่ 4-10 แสดงผลการวิเคราะห์ค่าสัมประสิทธิ์ถดถอย

Coefficients								
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
2	(Constant)	.562	.333		1.687	.092		
	Communication	.534	.050	.487	10.611	.000	.809	1.235
	Behavior	.232	.087	.122	2.663	.008	.809	1.235
a. Dependent Variable: Reduce								

ตารางนี้แสดงค่าสัมประสิทธิ์ของตัวแปรในโมเดล โดยใช้ตัวแปรตามคือ Reduce (การลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร) และตัวแปรอิสระที่แตกต่างกันในแต่ละโมเดลโดยตัวแปร Communication (การสื่อสารภายในองค์กร) มีอิทธิพลสูงสุด ต่อ Reduce ในทุกโมเดล รองลงมาคือ Behavior (พฤติกรรมการใช้งานระบบสารสนเทศ)โดยค่าความมีนัยสำคัญทางสถิติที่ระดับ 0.05 แสดงว่ามีความสำคัญทางสถิติ โดยผ่านการวัดMulticollinearity มีค่า Tolerance มากกว่า 0.2 และ VIF น้อยกว่า 5 จึงสรุปได้ว่าไม่มีปัญหา Multicollinearity [25] ข้อสรุปจากผลการวิเคราะห์สามารถสรุปสมการถดถอยเชิงเส้นในรูปแบบสมการมาตราฐานที่ใช้ดังสมการที่ 4-1 ดังนี้

$$Y = 0.562 + 0.534(X_1) + 0.232(X_2) \quad (4\text{-}1)$$

โดยที่

Y คือ Reduce (การลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร)

X_1 คือ Communication (การสื่อสารภายในองค์กร)

X_2 คือ Behavior (พฤติกรรมการใช้งานระบบสารสนเทศ)

สรุปคือ Communication (การสื่อสารภายในองค์กร) เป็นปัจจัยที่สำคัญที่สุด ต่อ Reduce (การลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร) โดยมีผลอย่างมีนัยสำคัญทางสถิติในทุกโมเดล Behavior (พฤติกรรมการใช้งานระบบสารสนเทศ) มีผลต่อ Reduce แต่มีอิทธิพลต่ำกว่า Communication

4.4 แนวทางในการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร

4.4.1 การสื่อสารภายในองค์กร

องค์กรควรพัฒนาระบบการสื่อสารภายในองค์กร ในด้านความมั่นคงปลอดภัยไซเบอร์ให้มีความชัดเจนและครอบคลุม โดยจัดทำแนวทางปฏิบัติที่สามารถนำไปใช้ได้จริง พร้อมทั้งเผยแพร่ข้อมูลเกี่ยวกับภัยคุกคามไซเบอร์ในรูปแบบต่าง ๆ และแผนการรับมือที่มีประสิทธิภาพอย่างสม่ำเสมอ เพื่อให้บุคลากรทุกระดับสามารถเข้าถึงและเข้าใจถึงแนวทางการป้องกันภัยคุกคามที่อาจเกิดขึ้น องค์กรควรสร้างช่องทางการสื่อสารที่เปิดโอกาสให้บุคลากรสามารถรายงานเหตุการณ์ผิดปกติด้านความปลอดภัยไซเบอร์ได้อย่างรวดเร็วและปลอดภัย ตลอดจนมีการจัดกิจกรรมให้ความรู้ เช่น การฝึกอบรม การประชุมเชิงปฏิบัติการ หรือการจำลองสถานการณ์ เพื่อให้บุคลากรเกิดความตระหนักและสามารถปฏิบัติตามแนวทางที่กำหนดได้อย่างถูกต้อง ควบคู่ไปกับการสร้างวัฒนธรรมองค์กรที่ส่งเสริมให้ทุกคนมีส่วนร่วมในการรักษาความมั่นคงปลอดภัยของข้อมูล โดยเน้นให้เกิดการแลกเปลี่ยนความรู้และประสบการณ์เกี่ยวกับภัยคุกคามไซเบอร์ระหว่างบุคลากรในทุกระดับขององค์กร เพื่อให้เกิดการเรียนรู้ร่วมกันและสามารถนำแนวทางการป้องกันที่เหมาะสมไปประยุกต์ใช้ได้อย่างมีประสิทธิภาพ ทั้งนี้ ควรมีการกำหนดนโยบายและมาตรการที่สนับสนุนให้บุคลากรปฏิบัติตามหลักความปลอดภัยไซเบอร์อย่างต่อเนื่อง [4],[11]

4.4.2 พฤติกรรมการใช้งานระบบสารสนเทศ

องค์กรควรส่งเสริมให้บุคลากรมีพฤติกรรมที่สอดคล้องกับหลักการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยการปลูกฝังวินัยในการใช้งานระบบสารสนเทศอย่างปลอดภัย ตั้งแต่การตั้งค่ารหัสผ่านที่รัดกุม การหลีกเลี่ยงการใช้ซอฟต์แวร์ที่ไม่น่าเชื่อถือ ไปจนถึงการป้องกันไม่ให้บุคคลภายนอกเข้าถึงข้อมูลสำคัญขององค์กร การสร้างความตระหนักรู้ในหมู่บุคลากรเกี่ยวกับแนวทางปฏิบัติที่ปลอดภัย เช่น การหลีกเลี่ยงอีเมลหรือไฟล์แนบที่น่าสงสัย การไม่แชร์ข้อมูลบัญชีผู้ใช้ เป็นสิ่งสำคัญที่ช่วยลดความเสี่ยงจากการโจมตีทางไซเบอร์ ในขณะเดียวกัน องค์กรควรมีมาตรการตรวจสอบและติดตามพฤติกรรมการใช้งานระบบสารสนเทศอย่างต่อเนื่อง ไม่ว่าจะเป็นการตรวจสอบการเข้าถึงข้อมูลที่สำคัญ การบันทึกและวิเคราะห์พฤติกรรมที่อาจเป็นภัย เพื่อให้มั่นใจว่ามีมาตรการป้องกันที่เพียงพอและสามารถระบุความเสี่ยงได้อย่างรวดเร็ว การบังคับใช้มาตรการรักษาความมั่นคงปลอดภัยผ่านนโยบายที่ชัดเจน จะช่วยให้ทุกคนในองค์กรตระหนักถึงความรับผิดชอบของตนและปฏิบัติตามแนวทางป้องกันอย่างเคร่งครัด ทั้งหมดนี้ล้วนเป็นปัจจัยสำคัญที่ช่วยลดความเสี่ยงจากพฤติกรรมการใช้งานระบบสารสนเทศที่ไม่ปลอดภัย ลดโอกาสการรั่วไหลของข้อมูล และป้องกันการถูกโจมตีทางไซเบอร์ ซึ่งจะช่วยให้องค์กรสามารถดำเนินงานได้อย่างมั่นคงปลอดภัย [4],[8]

บทที่ 5
สรุปผล อภิปรายผล และข้อเสนอแนะ

จากการศึกษาและวิจัย เรื่อง “แนวทางในการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร” โดยสามารถสรุปผลการวิจัยเป็น 3 ส่วนได้ดังนี้

5.1 สรุปผล

5.2 อภิปรายผล

5.3 ข้อเสนอแนะจากงานวิจัย

5.1 สรุปผล

การศึกษาผ่านแบบสอบถามจากกลุ่มตัวอย่างประกอบด้วยบุคลากรในองค์กรต่าง ๆ จำนวน 411 คน การวิเคราะห์ปัจจัยที่มีผลต่อการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ทั้ง 7 ปัจจัย ประกอบด้วย การรับรู้ภัยคุกคามทางไซเบอร์ พฤติกรรมการใช้งานระบบสารสนเทศ การฝึกอบรมและการให้ความรู้ด้านความปลอดภัยไซเบอร์ การสื่อสารภายในองค์กร วัฒนธรรมองค์กรที่สนับสนุนความปลอดภัยทางไซเบอร์ การใช้มาตรการป้องกันภัยคุกคามทางไซเบอร์ และการติดตามและตรวจสอบความปลอดภัยทางไซเบอร์ จากการศึกษากลุ่มตัวอย่างจำนวน 411 คน พบว่าผู้ตอบแบบสอบถามมีสัดส่วนของเพศชาย ร้อยละ 51.1 และเพศหญิงร้อยละ 48.9 ใกล้เคียงกัน โดยกลุ่มอายุที่มีจำนวนมากที่สุดคือ 51-60 ปี ร้อยละ 42.3 และส่วนใหญ่มากกว่าร้อยละ 68.6 มีประสบการณ์ทำงานมากกว่า 10 ปี นอกจากนี้ ผู้ตอบแบบสอบถามส่วนใหญ่เป็นพนักงาน/ข้าราชการ ร้อยละ 77.4 และมีระดับการศึกษาปริญญาตรีเป็นหลักร้อยละ 62.0 ในการวิเคราะห์ความคิดเห็นเกี่ยวกับปัจจัยที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ พบว่าผู้ตอบแบบสอบถามมีระดับความเห็นด้วยมากในทุกปัจจัย โดยพฤติกรรมการใช้งานระบบสารสนเทศ มีค่าเฉลี่ยเท่ากับ 4.202 คะแนนและ ส่วนเบี่ยงเบนมาตรฐาน 0.617 ได้คะแนนสูงสุด ขณะที่การสื่อสารภายในองค์กร มีค่าเฉลี่ยเท่ากับ 3.546 คะแนน และมีส่วนเบี่ยงเบนมาตรฐาน 1.067 ได้คะแนนต่ำสุด แต่ยังคงอยู่ในระดับที่ดี อย่างไรก็ตาม ปัจจัยด้านการรับรู้ภัยคุกคามทางไซเบอร์ และการลดโอกาสเกิดภัยคุกคามยังอยู่ในระดับปานกลางถึงสูง มีค่าเฉลี่ยเท่ากับ 3.431 คะแนน มีส่วนเบี่ยงเบนมาตรฐานเท่ากับ 1.170 คะแนนซึ่งชี้ให้เห็นว่ามีช่องว่างในการพัฒนา การเปรียบเทียบระหว่างเพศ พบว่าผู้หญิงมีค่าเฉลี่ยสูงกว่าผู้ชายใน 7 ปัจจัย ได้แก่ การรับรู้ภัยคุกคามพฤติกรรมการใช้งาน การฝึกอบรม การสื่อสาร วัฒนธรรมองค์กร มาตรการป้องกันภัยคุกคาม และการติดตามตรวจสอบ

การวิเคราะห์ปัจจัยที่มีผลต่อการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ พบว่าองค์กรควรมีแนวทางดังนี้ มากที่สุดคือการสื่อสารภายในองค์กรมีอิทธิพลมากที่สุด องค์กรควรมีการสื่อสารที่ดีด้านความปลอดภัยมั่นคงไซเบอร์ มีการเผยแพร่แนวทางในการปฏิบัติ แผนการรับมือภัยคุกคามไซเบอร์ในรูปแบบต่าง ๆ รองลงมาคือพฤติกรรมการใช้งานระบบสารสนเทศ องค์กรควรมีกระบวนการให้ความรู้ความตระหนักในความมั่นคงปลอดภัยสารสนเทศแก่บุคลากร ช่วยลดความเสี่ยงจากพฤติกรรมการใช้งานระบบสารสนเทศ จะช่วยให้บุคลากรสามารถปฏิบัติตามมาตรการรักษาความปลอดภัยอย่างถูกต้อง

5.2 อภิปรายผล

ผลการวิจัยชี้ให้เห็นว่าแนวทางที่มีประสิทธิภาพสูงสุดในการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กรคือการสื่อสารภายในองค์กร ซึ่งสอดคล้องกับงานวิจัยของ [4] และ [11] ที่ระบุว่าการสื่อสารที่ดีช่วยเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ ผ่านการเผยแพร่ข้อมูลที่ถูกต้องและทันเวลา ทำให้บุคลากรสามารถรับรู้ถึงภัยคุกคามและแนวทางป้องกันได้อย่างมีประสิทธิภาพ การมีช่องทางการสื่อสารที่เปิดกว้างและการให้ข้อมูลเกี่ยวกับภัยคุกคามไซเบอร์อย่างต่อเนื่อง ช่วยให้บุคลากรมีความพร้อมในการรับมือและลดความเสี่ยงจากการถูกโจมตี ทั้งนี้ผลการวิจัยยังพบว่าพฤติกรรมการใช้งานระบบสารสนเทศของบุคลากรในองค์กรเป็นอีกปัจจัยสำคัญที่ส่งผลต่อความมั่นคงปลอดภัยไซเบอร์ ซึ่งสนับสนุนงานวิจัยของ [7] และ [8] ที่ระบุว่าความมีส่วนร่วมของบุคลากรในทุกระดับสามารถช่วยต่อต้านภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ การใช้งานระบบสารสนเทศอย่างระมัดระวังการปฏิบัติตามแนวทางด้านความปลอดภัย และการให้ความสำคัญกับการป้องกันข้อมูล ล้วนช่วยลดความเสี่ยงจากภัยคุกคามที่อาจเกิดขึ้นในองค์กร และช่วยให้บุคลากรสามารถปฏิบัติตามมาตรการป้องกันได้อย่างถูกต้อง ดังนั้นการพัฒนาแนวทางการสื่อสารภายในองค์กร และการส่งเสริมพฤติกรรมการใช้งานระบบสารสนเทศที่ปลอดภัย จึงเป็นแนวทางสำคัญที่องค์กรควรให้ความสำคัญเพื่อป้องกันและลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร

5.3 ข้อเสนอแนะจากงานวิจัย

จากผลการศึกษาพบว่าการสื่อสารภายในองค์กรเป็นปัจจัยสำคัญที่สุดในการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ ดังนั้น องค์กรควรให้ความสำคัญกับการสร้างช่องทางการสื่อสารที่มีประสิทธิภาพ รวมถึงการเผยแพร่ข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ให้แก่พนักงานอย่างสม่ำเสมอ เพื่อให้การลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กรเป็นไปอย่างมีประสิทธิภาพ ทั้งนี้ในงานวิจัยครั้งถัดไปขอเสนอให้มีการทำว่าต้องเพิ่มขนาดตัวอย่างงานวิจัยให้เมีความเจาะจงมากยิ่งขึ้น เช่น เฉพาะในหน่วยงานภาครัฐ ภาคเอกชน และเจ้าของธุรกิจ เป็นต้น เพราะแต่ละกลุ่มอาจมีโครงสร้างองค์กร

ลักษณะงาน และวิธีการรับมือภัยคุกคามที่แตกต่างกัน ซึ่งจะช่วยให้ผลการศึกษาแม่นยำและสามารถนำไปใช้ในบริบทจริงได้มากยิ่งขึ้น นอกจากนี้ ควรมีการสัมภาษณ์เชิงลึกจากผู้เชี่ยวชาญหรือผู้บริหารด้านความมั่นคงไซเบอร์ เพื่อเก็บข้อมูลเชิงคุณภาพเพิ่มเติม ที่อาจไม่ปรากฏในแบบสอบถาม และสามารถใช้สนับสนุนผลการวิเคราะห์เชิงสถิติให้มีความน่าเชื่อถือมากยิ่งขึ้น นอกจากนี้จะช่วยให้ได้ข้อเสนอแนะเชิงกลยุทธ์ที่มีความเหมาะสมใช้งานได้จริง และช่วยพัฒนาองค์ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้ก้าวทันต่อการเปลี่ยนแปลงของโลกดิจิทัลในปัจจุบัน

บรรณานุกรม

1, ทรู ดิจิทัล อคาเดมี. (10 สิงหาคม 2566). [ออนไลน์]. 6 การโจมตีทางไซเบอร์ (Cyber Attack) ที่ควรรู้จัก และวิธีรับมือ [สืบค้นวันที่ 1 สิงหาคม 2567]. จาก https://www.truedigitalacademy.com/blog/6-types-of-cyber-security-threats

2. ราชกิจจานุเบกษา. (28 พฤษภาคม พ.ศ. 2562). พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. เล่ม 136 ตอนที่ 69 ก3. ราชกิจจานุเบกษา. (วันที่ 30 มกราคม 2563). ประกาศสำนักทะเบียนกลาง. จำนวนราษฎรทั่วราชอาณาจักร ตามหลักฐานการทะเบียนราษฎร ณ วันที่ 31 ธันวาคม 2563. เล่ม 137 ตอนพิเศษ 24 ง : 17-19.
3. ราชกิจจานุเบกษา. (วันที่ 30 มกราคม 2563). ประกาศสานักทะเบียนกลาง. จำนวนราษฎรทั่วราชอาณาจักร ตามหลักฐานการทะเบียนราษฎร ณ วันที่ 31 ธันวาคม 2563. เล่ม 137 ตอนพิเศษ 24 ง : 17-19.
4. ฐิติมา ภู่ห้อย. (2564)."การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์" สารนิพนธ์ปริญญามหาบัณฑิต. มหาวิทยาลัยศรีปทุม.
5. สุทธิพันธุ์ ชวลิตเลขา. (2565)."การเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด" สารนิพนธ์ปริญญามหาบัณฑิต. มหาวิทยาลัยศรีปทุม.
6. ศิวกร รัตติโชติ. (2565)."การศึกษาวิจัยเกี่ยวกับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล" สารนิพนธ์ปริญญามหาบัณฑิต. มหาวิทยาลัยธุรกิจบัณฑิตย์.
7. วิทวัส สุขชีพ และ จรัญ แสนราช. (2566). “การตระหนักรู้ถึงภัยคุกคามและอาชญากรรมไซเบอร์ของผู้ใช้งาน ระบบเครือข่ายอินเทอร์เน็ตในสถานศึกษา จังหวัดสุรินทร์” วารสารวิชาการเทคโนโลยีอุตสาหกรรม มหาวิทยาลัยราชภัฏสุรินทร์ ปีที่ 8 ฉบับที่ 1.
8. วิไล ฤทธิเดช และ สรวง รุ่งประกายพรรณ. (2566). “ความรู้ ความตระหนัก และพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ ของบุคลากรสาธารณสุขในประเทศไทย: กรณีศึกษาโรงพยาบาลพุทธโสธร” วารสารวิชาการ มหาวิทยาลัยการจัดการและเทคโนโลยีอีสเทิร์น. ปีที่ 17 ฉบับที่ 1.

เอกสารอ้างอิง (ต่อ)

9. ปวริศร์ จันทวัฒน์ และ ศรีรัฐ โกวงศ์. (2566).“ความตระหนักในการรักษาความปลอดภัยทางสารสนเทศของบุคลากร กรมประชาสัมพันธ์” สหวิทยาการและความยั่งยืนปริทรรศน์ไทย (e-ISSN: 2985-2684) ปีที่ 12 ฉบับที่ 2.
10. เมธาพร ธรรมศิริ และ ศิรภัสสรศ์ วงศ์ทองดี. (2565).“ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากร ในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร” วารสารวิชาการไทยวิจัยและการจัดการ Thai Research and Management Journal ปีที่ 3 ฉบับที่ 2.
11. สมศิริ พันธุ์ศักดิ์ศิริ และ เสาวนีย์ สมันต์ตรีพร. (2566). “ภาวะวิกฤติของระบบสารสนเทศโรงพยาบาลสระบุรี” วารสารสหวิทยาการมนุษยศาสตร์และสังคมศาสตร์ (ISSN: 2773-9775) ปีที่ 5 ฉบับที่ 1.
12. สมศิริ พันธุ์ศักดิ์ศิริ และ เสาวนีย์ สมันต์ตรีพร. (2566).“ประสิทธิผลของการจัดการความปลอดภัยระบบสารสนเทศโรงพยาบาลสระบุรี” วารสารสหวิทยาการมนุษยศาสตร์และสังคมศาสตร์ (ISSN: 2697-6471) ปีที่ 6 ฉบับที่ 2.
13. นริส อุไรพันธ์ และ ณัชชา สมจันทร์. (2565). “ปัจจัยที่ส่งผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ของธุรกิจพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทย” วารสารสหวิทยาการเพื่อการพัฒนา มหาวิทยาลัยราชภัฏอุตรดิตถ์ (ISSN: 2821-9708) ปีที่ 12 ฉบับที่ 1.
14. กิตติศักดิ์ จันทร์นิเวศน์ และ ชัยวัฒน์ อุตตมากร. (2566). “การวิเคราะห์องค์ประกอบของปัจจัยที่ส่งผลต่อความตั้งใจในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรในบริษัทกลุ่มน้ำมันและก๊าซ” สารนิพนธ์ปริญญามหาบัณฑิต. มหาวิทยาลัยธรรมศาสตร์.
15. Nurul Alieyah Azam, Alya Geogiana Buja, Nor Masri Sahri, Rehan Ahmad, Nurul Fadly Habidin, Shekh Faisal Abdul Latip, Mohamad Yusof Darus, Mohamed Saiful Firdaus Hussin, Saharudin Saat. (2567)."A Light Review on Cyber Security Awareness Models for the Elderly" Journal of Advanced Research in Applied Sciences and Engineering Technology Vol. 44, Iss: 1, pp 31-45.
16. Shouq Alrobaian,Saif Alshahrani and Abdulaziz Almaleh. (2566). “Cybersecurity Awareness Assessment among Trainees of the Technical and Vocational Training Corporation” Big data and cognitive computing Vol. 7, Iss: 2, pp 73-73.

เอกสารอ้างอิง (ต่อ)

17. Shaliet Rose Sebastian and Bichu P Babu. (2565). “Are we Cyber aware? A cross sectional study on the prevailing Cyber practices among adults from Thiruvalla, Kerala” International Journal of Community Medicine and Public Health Vol. 10, Iss: 1, pp 235-235.

18. Said Baadel, Fadi Thabtah and Joan Lu (2564). “Cybersecurity Awareness: A Critical Analysis of Education and Law Enforcement Methods” Informatica (lithuanian Academy of Sciences) Vol. 45, Iss: 3.

19. Tibor Pósa และ Jens Grossklags .(2565). “Work Experience as a Factor in Cyber-Security Risk Awareness: A Survey Study with University Students” Journal of cybersecurity and privacy Vol. 2, Iss: 3, pp 490-515.

20. Mohammed A. Alqahtani (2565) . “Cybersecurity Awareness Based on Software and E-mail Security with Statistical Analysis” Computational Intelligence and Neuroscience Vol. 2022, pp 1-12.

21. กิติยา วิสิฐพงศ์พันธ์ ชูเกียรติ บุญก่อเกื้อ กิตติพงศ์ อยู่นิรันดร และ นลินภัสร์ บำเพ็ญเพียร. (2565) . “ปัจจัยที่ส่งต่อการตระหนักรู้ถึงความปลอดภัยทางไซเบอร์ของนักศึกษามหาวิทยาลัย” วารสารวิชาการวิทยาศาสตร์ มหาวิทยาลัยราชภัฏจันทรเกษม ปีที่ 32 ฉบับที่ 1.

22. สุภาพร พันธ์ยา คริชณะ ฉิมมณี และ ราชศักดิ์ สมยานนทนากุล. (2565) . “การตระหนักรู้เท่าทันภัยคุกคามจากการใช้อินเทอร์เน็ต กรณีจำลองการโจมตีด้วยการคาดเดารหัสผ่าน (Password Attack)” วารสารวิชาการนวัตกรรมสื่อสารสังคม ปีที่ 11 ฉบับที่ 1.

23. Mehmet Emin Erendor และ Merve YILDIRIM.(2565) .“CYBERSECURITY AWARENESS IN ONLINE EDUCATION: A CASE STUDY ANALYSIS” IEEE Access Vol. 10, pp 52319-52335.

24. Musleh Alsulami.(2565) . “Social Media Security Awareness in Saudi Arabia” Tehnički glasnik Vol. 16, Iss: 2, pp 213-218.

25. Hair, J.F., Black, W.C., Babin, B.J. and Anderson, R.E. (2010). Multivariate Data Analysis. 7th Edition, Pearson, New York.

ภาคผนวก ก

รายนามผู้เชี่ยวชาญ

รายนามผู้เชี่ยวชาญตรวจสอบเครื่องมือที่ใช้ในการศึกษา

รายนามผู้เชี่ยวชาญตรวจสอบความตรงเชิงเนื้อหา (Content Validity) ของแบบสอบถาม การค้นคว้าอิสระ เรื่อง แนวทางในการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร จำนวน 3 ท่าน

1. นาย สุดใจ พรมพล
ตำแหน่ง ผู้อำนวยการส่วนระบบสารสนเทศและบริการ
ศูนย์เทคโนโลยีสารสนเทศ กรมสรรพสามิต

2. นาย ประดิษฐ์ ศรีบุญ
ตำแหน่ง นักวิเคราะห์ระบบอาวุโส
บริษัท โปรเฟสชั่นนัล คอมพิวเตอร์ จำกัด

3. นาย นวศิลป์ อินเต็ม
ตำแหน่ง นักวิเคราะห์ระบบ
บริษัท เท็คไอทีโซลูชั่น จำกัด

ภาคผนวก ข

หนังสือขอความอนุเคราะห์เป็นผู้เชี่ยวชาญตรวจคุณภาพแบบสอบถาม

ที่ อว ๗๑๐๗/๒๗๑๐

คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
๑๕๑๘ ถนนประชาราษฎร์ ๓ แขวงวงศ์สว่าง
เขตบางซื่อ กทม. ๑๐๘๐๐

๒๑ มีนาคม ๒๕๖๘

เรื่อง ขอความอนุเคราะห์เป็นผู้เชี่ยวชาญในการประเมินคุณภาพเพื่อประกอบการทำการค้นคว้าอิสระ

เรียน นายสุดใจ พรมพล ผู้อำนวยการส่วนระบบสารสนเทศและบริการ
ศูนย์เทคโนโลยีสารสนเทศ กรมสรรพสามิต

เนื่องด้วยนายอภิรักษ์ มิตรประสาร รหัสประจำตัว ๖๖-๐๗๐๑๑๘-๕๗๐๗-๒ นักศึกษาระดับบัณฑิตศึกษา ภาควิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ กำลังดำเนินการจัดทำการค้นคว้าอิสระ เรื่อง "แนวทางในการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร" โดยมี รองศาสตราจารย์ ดร.นลินภัสร์ บำเพ็ญเพียร เป็นประธานคณะกรรมการที่ปรึกษาการค้นคว้าอิสระ ในการนี้นักศึกษามีความประสงค์ขอความอนุเคราะห์จากท่านเพื่อโปรดพิจารณาแบบประเมินเพื่อประกอบการทำการค้นคว้าอิสระดังกล่าว

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ จักขอบพระคุณยิ่ง

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์ ดร.ศักดิ์ชาย ตั้งวรรณวิทย์)
รองคณบดีฝ่ายวิชาการและวิจัย

ภาควิชาเทคโนโลยีสารสนเทศ
โทร. ๐ ๒๕๕๕ ๒๐๐๐ ต่อ ๒๗๒๘
www.itd.kmutnb.ac.th

ที่ อว ๗๑๐๗/๒๑๔

คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
๑๕๑๘ ถนนประชาราษฎร์ ๑ แขวงวงศ์สว่าง
เขตบางซื่อ กทม. ๑๐๘๐๐

๒๑ มีนาคม ๒๕๖๘

เรื่อง ขอความอนุเคราะห์เป็นผู้เชี่ยวชาญในการประเมินคุณภาพเพื่อประกอบการทำการค้นคว้าอิสระ

เรียน นายประดิษฐ์ ศรีบุญ นักวิเคราะห์ระบบอาวุโส บริษัท โปรเฟสชั่นนัล คอมพิวเตอร์ จำกัด

เนื่องด้วยนายอภิรักษ์ มิตรประสาร รหัสประจำตัว ๖๖-๐๗๐๑๑๘-๕๗๐๗-๒นักศึกษาระดับบัณฑิตศึกษา ภาควิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ กำลังดำเนินการจัดทำการค้นคว้าอิสระ เรื่อง "แนวทางในการลดโอกาสภัยคุกคามทางไซเบอร์ในองค์กร" โดยมี รองศาสตราจารย์ ดร.นลินภัสร์ บำเพ็ญเพียร เป็นประธานคณะกรรมการที่ปรึกษาการค้นคว้าอิสระ ในการนี้นักศึกษามีความประสงค์ขอความอนุเคราะห์จากท่านเพื่อโปรดพิจารณาแบบประเมินเพื่อประกอบการทำการค้นคว้าอิสระดังกล่าว

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ จักขอบพระคุณยิ่ง

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์ ดร.ศักดิ์ชาย ดั้งวรรณวิทย์)
รองคณบดีฝ่ายวิชาการและวิจัย

ภาควิชาเทคโนโลยีสารสนเทศ
โทร. ๐ ๒๕๕๕ ๒๐๐๐ ต่อ ๒๗๒๘
www.itd.kmutnb.ac.th

ที่ อว ๗๓๐๗/๒๙๗

คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
๑๕๑๘ ถนนประชาราษฎร์ ๑ แขวงวงศ์สว่าง
เขตบางซื่อ กทม. ๑๐๘๐๐

๒๑ มีนาคม ๒๕๖๘

เรื่อง ขอความอนุเคราะห์เป็นผู้เชี่ยวชาญในการประเมินคุณภาพเพื่อประกอบการทำการค้นคว้าอิสระ

เรียน นายนวศิลป์ อินเต็ม นักวิเคราะห์ระบบ บริษัท เท็คไอที โซลูชั่น จำกัด

เนื่องด้วยนายอภิรักษ์ มิตรประสาร รหัสประจำตัว ๖๖-๐๗๐๑๑๘-๕๗๐๗-๒ นักศึกษาระดับบัณฑิตศึกษา ภาควิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ กำลังดำเนินการจัดทำการค้นคว้าอิสระ เรื่อง "แนวทางในการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร" โดยมี รองศาสตราจารย์ ดร.นลินภัสร์ บำเพ็ญเพียร เป็นประธานคณะกรรมการที่ปรึกษาการค้นคว้าอิสระ ในการนี้นักศึกษามีความประสงค์ขอความอนุเคราะห์จากท่านเพื่อโปรดพิจารณาแบบประเมินเพื่อประกอบการทำการค้นคว้าอิสระดังกล่าว

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ จักขอบพระคุณยิ่ง

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์ ดร.ศักดิ์ชาย ตั้งวรรณวิทย์)
รองคณบดีฝ่ายวิชาการและวิจัย

ภาควิชาเทคโนโลยีสารสนเทศ
โทร. ๐ ๒๕๕๕ ๒๐๐๐ ต่อ ๒๗๒๘
www.itd.kmutnb.ac.th

แบบประเมินความสอดคล้องของแบบสอบถามเพื่อใช้ในการค้นคว้าอิสระ
ของผู้เชี่ยวชาญที่มีต่อแบบสอบถามแนวทางในการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร

คำชี้แจง ขอให้ท่านพิจารณาว่า ข้อคำถามที่กำหนดให้วัดได้สอดคล้องตรงตามจุดประสงค์ที่กำหนดไว้หรือไม่ โดยทำเครื่องหมาย X ในบนช่องที่ตรงกับความคิดเห็นของท่าน พร้อมเขียนข้อเสนอแนะที่เป็นประโยชน์

ในการนำไปพิจารณาปรับปรุงต่อไป โดยกำหนดคะแนนความคิดเห็น ดังนี้

+1 เมื่อแน่ใจว่าข้อคำถามนั้นมีความสอดคล้องกับวัตถุประสงค์

0 เมื่อไม่แน่ใจว่าข้อคำถามนั้นมีความสอดคล้องกับวัตถุประสงค์

-1 เมื่อแน่ใจว่าข้อคำถามนั้นไม่มีความสอดคล้องกับวัตถุประสงค์

รายการข้อคำถาม		ระดับความสอดคล้อง			ข้อเสนอแนะ
		สอดคล้อง +1	ไม่แน่ใจ 0	ไม่สอดคล้อง -1	
การรับรู้ภัยคุกคามทางไซเบอร์					
1.	ท่านคิดว่าการไม่เปิดเผยระบุตัวตนบนเครือข่ายสังคมออนไลน์สาธารณะที่มีผู้ใช้ทั่วไปมีความปลอดภัย				
2.	ท่านคิดว่าการไม่ให้ข้อมูลส่วนตัวบนเครือข่ายสังคมสาธารณะมีความปลอดภัย				
3.	ท่านคิดว่าการเข้าเว็บไซต์ http มีความปลอดภัย น้อยกว่า https				
4.	ท่านคิดว่าการไม่ซื้อโปรแกรมที่ถูกลิขสิทธิ์มาใช้งานมีความเสี่ยงต่อระบบ				

รายการข้อคำถาม		ระดับความสอดคล้อง			ข้อเสนอแนะ
		สอดคล้อง +1	ไม่แน่ใจ 0	ไม่สอดคล้อง -1	
	คอมพิวเตอร์คล้ายคลึงกับโปรแกรมที่แชร์ให้โหลดได้ฟรีในอินเทอร์เน็ต				
5.	ท่านคิดว่าการกำหนดผู้ใช้งานและรหัสผ่านก่อนเข้าสู่ระบบคอมพิวเตอร์ก่อให้เกิดความปลอดภัยในการเข้าใช้งาน				
พฤติกรรมการใช้งานระบบสารสนเทศ					
6.	ท่านไม่อนุญาตให้บุคคลที่ไม่รู้จักเข้าถึงการใช้งานบน Social Media ของตนเอง				
7.	ท่านมีการใช้งานผ่านโปรแกรมที่มีลิขสิทธิ์				
8.	ท่านมีการดาวน์โหลดไฟล์โดยทราบแหล่งที่มาออนไลน์				
9.	ท่านมีการเข้าเว็บไซต์เฉพาะที่เหมาะสมและปลอดภัย				
10.	ท่านติดตั้งโปรแกรมต่าง ๆ โดยพิจารณาจากแหล่งที่มาที่น่าเชื่อถือ				
การฝึกอบรมและการให้ความรู้ด้านความปลอดภัยไซเบอร์					
11.	องค์กรมีการการฝึกอบรมสร้างความตระหนักรู้ด้านความปลอดภัย				
12.	องค์กรมีการการสนับสนุนบุคลากรในการพัฒนาทักษะด้านความมั่นคงปลอดภัยไซเบอร์				
13.	บุคลากรสามารถถ่ายทอดความรู้ด้านความมั่นคงปลอดภัยระหว่างกันในองค์กร				
14.	องค์กรของท่านมีการฝึกอบรมวิธีการใช้สารสนเทศอย่างปลอดภัย				

รายการข้อคำถาม		ระดับความสอดคล้อง			ข้อเสนอแนะ
		สอดคล้อง +1	ไม่แน่ใจ 0	ไม่สอดคล้อง -1	
15.	องค์กรของท่านมีการให้ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กรอยู่เสมอ				
การสื่อสารภายในองค์กร					
16.	องค์กรมีการเผยแพร่ความรู้ด้านการรับมือภัยคุกคามทางไซเบอร์				
17.	องค์กรมีการเผยแพร่แผนการรับมือภัยคุกคามทางไซเบอร์				
18.	องค์กรมีแนวทางให้บุคลากรได้เรียนรู้ประสบการณ์ด้านไซเบอร์ร่วมกัน				
19.	องค์กรมีการเผยแพร่นโยบายและแนวปฏิบัติให้บุคลากรในหน่วยงานได้รับทราบและปฏิบัติ				
วัฒนธรรมองค์กรที่สนับสนุนความปลอดภัยทางไซเบอร์					
20.	บุคลากรมีความสามารถถ่ายทอดความรู้ด้านความมั่นคงปลอดภัยระหว่างกันในองค์กร				
21.	บุคลากรมีความเชื่อมั่นในมาตรการปกป้องข้อมูลส่วนบุคคลในองค์กร				
22.	บุคลากรมีความไว้วางใจในระบบเครือข่ายขององค์กร				
23.	บุคลากรมีความพร้อมและให้ความร่วมมือในการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับองค์กร				
การใช้มาตรการป้องกันภัยคุกคามทางไซเบอร์					

รายการข้อคำถาม		ระดับความสอดคล้อง			ข้อเสนอแนะ
		สอดคล้อง +1	ไม่แน่ใจ 0	ไม่สอดคล้อง -1	
24.	องค์กรมีการกำหนดสิทธิ หน้าที่ความรับผิดชอบในการบริหารจัดการข้อมูลของแต่ละส่วนงาน				
25.	องค์กรมีการกำหนดนโยบาย/กฎเกณฑ์การเข้าถึงและใช้ประโยชน์จากข้อมูล				
26.	องค์กรมีแนวทางการดำเนินการปกปิดข้อมูลส่วนบุคคล				
27.	องค์กรมีการกำหนดมาตรการหรือกระบวนการตรวจสอบและประเมินคุณภาพข้อมูล				
การติดตามและตรวจสอบความปลอดภัยทางไซเบอร์					
28.	องค์กรมีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยไซเบอร์				
29.	องค์กรมีการตรวจสอบระบบสารสนเทศ (IT Audit)				
30.	องค์กรของท่านมีการตรวจสอบการปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงานอยู่เสมอ				
31.	องค์กรของท่านมีการประเมินเพื่อหาแนวทางการป้องกันภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ร่วมกับผู้ที่เกี่ยวข้องอย่างสม่ำเสมอ				
32.	องค์กรของท่านมีการทบทวน ติดตามและตรวจสอบด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างต่อเนื่อง				
การลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร					

รายการข้อคำถาม		ระดับความสอดคล้อง			ข้อเสนอแนะ
		สอดคล้อง +1	ไม่แน่ใจ 0	ไม่สอดคล้อง -1	
33.	ในปีที่ผ่านมา องค์กรของท่านได้รับความเสียหายจากภัยคุกคามทางไซเบอร์ โดยรวมไม่เกิน 1-2 ครั้ง				
34.	องค์กรของท่านมีโอกาสในการเกิดภัยคุกคามทางไซเบอร์ลดลงในอนาคต				

ลงชื่อ.....ผู้เชี่ยวชาญ

(.....)

ตำแหน่ง.....

วันที่.....

ภาคผนวก ค

แบบสอบถามเก็บข้อมูล

แบบสอบถามเพื่อการวิจัย

เรื่อง แนวทางในการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร

ตอนที่ 1 แบบสอบถามเกี่ยวกับปัจจัยส่วนบุคคลของผู้ตอบแบบสอบถาม

<u>คำชี้แจง</u> จงทำเครื่องหมาย ✓ ในช่องที่ตรงกับความเป็นจริงของท่านมากที่สุด

1. เพศ

☐ 1. ชาย ☐ 2. หญิง ☐ 3. อื่น ๆ

2. อายุ

☐ 1. ต่ำกว่า 30 ปี ☐ 2. 30 – 40 ปี

☐ 3. 41 – 50 ปี ☐ 4. 51 - 60 ปี

3. ระดับการศึกษา

☐ 1. ต่ำกว่าปริญญาตรี ☐ 2. ปริญญาตรี

☐ 3. ปริญญาโท ☐ 4. ปริญญาเอก

4. ประสบการณ์การทำงาน

☐ 1. ต่ำกว่า 5 ปี ☐ 2. 5 – 10 ปี

☐ 3. 10 ปี ขึ้นไป

5. ประเภทอาชีพ

☐ 1. นักเรียน/นิสิตนักศึกษา ☐ 2. พนักงานบริษัทเอกชน

☐ 3. พนักงานข้าราชการ ☐ 4. เจ้าของธุรกิจ/ธุรกิจส่วนตัว

☐ 5. อื่น ๆ

ตอนที่ 2 ปัจจัยที่ส่งผลให้ลดโอกาสเกิดภัยคุกคามทางไซเบอร์

คำชี้แจง : กรุณาเขียนเครื่องหมาย (✓) ลงใน ☐ ในแต่ละข้อที่ตรงกับความคิดเห็นของท่านมากที่สุด ช่องเดียวเท่านั้น โดยแต่ละช่องจะแสดงระดับความต้องการดังนี้

5 = เห็นด้วยในระดับมากที่สุด 4 = เห็นด้วยในระดับมาก

3 = เห็นด้วยในระดับปานกลาง 2 = เห็นด้วยในระดับน้อย

1 = เห็นด้วยในระดับน้อยที่สุด

ปัจจัยที่ส่งผลให้ลดโอกาสเกิดภัยคุกคามทางไซเบอร์	ระดับความคิดเห็น				
	5 มากที่สุด	4 มาก	3 ปานกลาง	2 น้อย	1 น้อยที่สุด
การรับรู้ภัยคุกคามทางไซเบอร์					
1. ท่านคิดว่าการไม่เปิดเผยระบุตัวตนบนเครือข่ายสังคมออนไลน์สาธารณะที่มีผู้ใช้ทั่วไปมีความปลอดภัย					
2. ท่านคิดว่าการไม่ให้ข้อมูลส่วนตัวบนเครือข่ายสังคมสาธารณะมีความปลอดภัย					
3. ท่านคิดว่าการเข้าเว็บไซต์ http มีความปลอดภัยน้อยกว่า https					
4. ท่านคิดว่าการไม่ซื้อโปรแกรมที่ถูกลิขสิทธิ์มาใช้งานมีความเสี่ยงต่อระบบคอมพิวเตอร์คล้ายคลึงกับโปรแกรมที่แชร์ให้โหลดได้ฟรีในอินเทอร์เน็ต					
5. ท่านคิดว่าการกำหนดผู้ใช้งานและรหัสผ่านก่อนเข้าสู่ระบบคอมพิวเตอร์ก่อให้เกิดความปลอดภัยในการเข้าใช้งาน					
พฤติกรรมการใช้งานระบบสารสนเทศ					
1. ท่านไม่อนุญาตให้บุคคลที่ไม่รู้จักเข้าถึงการใช้งานบน Social Media ของตนเอง					
2. ท่านมีการใช้งานผ่านโปรแกรมที่มีลิขสิทธิ์					
3. ท่านมีการดาวน์โหลดไฟล์โดยทราบแหล่งที่มาออนไลน์					
4. ท่านมีการเข้าเว็บไซต์เฉพาะที่เหมาะสมและปลอดภัย					
5. ท่านติดตั้งโปรแกรมต่าง ๆ โดยพิจารณาจากแหล่งที่มาที่น่าเชื่อถือ					
การฝึกอบรมและการให้ความรู้ด้านความปลอดภัยไซเบอร์					
1. องค์กรมีการฝึกอบรมสร้างความตระหนักรู้ด้านความปลอดภัย					
2. องค์กรมีการสนับสนุนบุคลากรในการพัฒนาทักษะด้านความมั่นคงปลอดภัยไซเบอร์					

ปัจจัยที่ส่งผลให้ลดโอกาสเกิดภัยคุกคามทางไซเบอร์	ระดับความคิดเห็น				
	5 มากที่สุด	4 มาก	3 ปานกลาง	2 น้อย	1 น้อยที่สุด
3. บุคลากรสามารถถ่ายทอดความรู้ด้านความมั่นคงปลอดภัยระหว่างกันในองค์กร					
4. องค์กรของท่านมีการฝึกอบรมวิธีการใช้สารสนเทศอย่างปลอดภัย					
5. องค์กรของท่านมีการให้ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กรอยู่เสมอ					
การสื่อสารภายในองค์กร					
1. องค์กรมีการเผยแพร่ความรู้ด้านการรับมือภัยคุกคามทางไซเบอร์					
2. องค์กรมีการเผยแพร่แผนการรับมือภัยคุกคามทางไซเบอร์					
3. องค์กรมีแนวทางให้บุคลากรได้เรียนรู้ประสบการณ์ด้านไซเบอร์ร่วมกัน					
4. องค์กรมีการเผยแพร่นโยบายและแนวปฏิบัติให้บุคลากรในหน่วยงานได้รับทราบและปฏิบัติ					
วัฒนธรรมองค์กรที่สนับสนุนความปลอดภัยทางไซเบอร์					
1. บุคลากรมีความสามารถถ่ายทอดความรู้ด้านความมั่นคงปลอดภัยระหว่างกันในองค์กร					
2. บุคลากรมีความเชื่อมั่นในมาตรการปกป้องข้อมูลส่วนบุคคลในองค์กร					
3. บุคลากรมีความไว้วางใจในระบบเครือข่ายขององค์กร					
4. บุคลากรมีความพร้อมและให้ความร่วมมือในการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับองค์กร					
การใช้มาตรการป้องกันภัยคุกคามทางไซเบอร์					
1. องค์กรมีการกำหนดสิทธิ หน้าที่ความรับผิดชอบในการบริหารจัดการข้อมูลของแต่ละส่วนงาน					

ปัจจัยที่ส่งผลให้ลดโอกาสเกิดภัยคุกคามทางไซเบอร์	ระดับความคิดเห็น				
	5 มากที่สุด	4 มาก	3 ปานกลาง	2 น้อย	1 น้อยที่สุด
2. องค์กรมีการกำหนดนโยบาย/กฎเกณฑ์การเข้าถึงและใช้ประโยชน์จากข้อมูล					
3. องค์กรมีแนวทางการดำเนินการปกปิดข้อมูลส่วนบุคคล					
4. องค์กรมีการกำหนดมาตรการหรือกระบวนการตรวจสอบและประเมินคุณภาพข้อมูล					
การติดตามและตรวจสอบความปลอดภัยทางไซเบอร์					
1. องค์กรมีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยไซเบอร์					
2. องค์กรมีการตรวจสอบระบบสารสนเทศ (IT Audit)					
3. องค์กรของท่านมีการตรวจสอบการปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงานอยู่เสมอ					
4. องค์กรของท่านมีการประเมินเพื่อหาแนวทางการป้องกันภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ร่วมกับผู้ที่เกี่ยวข้องอย่างสม่ำเสมอ					
5. องค์กรของท่านมีการทบทวน ติดตาม และตรวจสอบด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างต่อเนื่อง					
การลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร					
1. ในปีที่ผ่านมา องค์กรของท่านได้รับความเสียหายจากภัยคุกคามทางไซเบอร์โดยรวมไม่เกิน 1-2 ครั้ง					
2. องค์กรของท่านมีโอกาสในการเกิดภัยคุกคามทางไซเบอร์ลดลงในอนาคต					

ประวัติผู้เขียน

ชื่อ นายอภิรักษ์ มิตรประสาร

ชื่อการค้นคว้าอิสระ แนวทางในการลดโอกาสเกิดภัยคุกคามทางไซเบอร์ในองค์กร

สาขาวิชา วิทยาศาสตร์ข้อมูลเพื่อนวัตกรรม

ประวัติ

ประวัติ

สถานที่ติดต่อ บ้านเลขที่ 8/56 หมู่ 2 อำเภอฉิมพลี แขวงฉิมพลี ถนนฉิมพลี เขตตลิ่งชัน จังหวัดกรุงเทพมหานคร 10170
Email: s6607011857072@email.kmutnb.ac.th,eakapiruck@gmail.com

ประวัติการศึกษา

สำเร็จการศึกษาระดับปริญญาตรี วิทยาศาสตรมหาบัณฑิต คณะเทคโนลยีสารสนเทศ สถาบันเทคโนโลยีไทย-ญี่ปุ่น ปี พ.ศ. 2556

ประวัติการทำงาน

ปัจจุบันทำงานอยู่ที่ กรมสรรพสามิต ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ