URU J.ISD
URU Journal of
Integrated Sciences for Development

URU-J.ISD 254724
ปีที่ 12 ฉบับที่ 1 มกราคม - มิถุนายน 2565
ISSN 2821-9708 (Online)

ปัจจัยที่ส่งผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ของธุรกิจพาณิชย์อิเล็กทรอนิกส์สำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทย

FACTORS AFFECTING THE CYBER SECURITY IN E-COMMERCE BUSINESS FOR SMALL AND MEDIUM-SIZED ENTERPRISES IN THAILAND

นริส อุไรพันธ์*[1*], และ ณัชชา สมจันทร์[2]

Naris Uraipan and Natcha Somjan

คณะเทคโนโลยีสังคม มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก วิทยาเขตจันทบุรี[1]

คณะเทคโนโลยีอุตสาหกรรม มหาวิทยาลัยราชภัฏเลย[2]

*Corresponding email: naris080515@yahoo.com

Receives: 22 February 2022, Revised: 21 June 2022, Accepted: 24 June 2022

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์ 1. เพื่อศึกษาหลักการด้านความมั่นคงปลอดภัยไซเบอร์ของธุรกิจพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทย 2. เพื่อศึกษาความแตกต่างของคุณลักษณะทั่วไปของธุรกิจกับความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทย และ 3. เพื่อศึกษาปัจจัยด้านความสำเร็จในการดำเนินกิจการที่ส่งผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ของธุรกิจพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทย กลุ่มตัวอย่างได้แก่ วิสาหกิจขนาดกลางและขนาดย่อม สำหรับธุรกิจพาณิชย์อิเล็กทรอนิกส์ เก็บรวบรวมข้อมูลจำนวน 852 ชุด โดยการสุ่มแบบเจาะจง เครื่องมือที่ใช้ในการวิจัย คือ แบบสอบถามการวิจัย ซึ่งผ่านการตรวจคุณภาพของเครื่องมือโดยมีค่าความเที่ยงตรงทางเนื้อหาเท่ากับ 0.93 และ มีค่าความเชื่อมั่นเท่ากับ 0.972 สถิติที่ใช้ในการวิเคราะห์ข้อมูล คือค่าร้อยละ ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน สถิติวิเคราะห์ความแปรปรวนทางเดียว และการวิเคราะห์ถดถอยพหุคูณโดยวิธีเป็นขั้นตอน

ผลการวิจัยพบว่า วิสาหกิจขนาดกลางและขนาดย่อมที่ประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ส่วนใหญ่ทำธุรกิจด้านการค้าปลีกและค้าส่ง มีระยะเวลาในการดำเนินธุรกิจ 4-9 ปี มีจำนวนพนักงานในองค์กร 6-10 คน และมีระดับตลาดที่ธุรกิจให้บริการดำเนินธุรกิจภายในประเทศ พนักงานที่มีพื้นฐานความรู้ทางด้านเทคโนโลยีสารสนเทศน้อยกว่า 50% มีการทำรายงานเมื่อโดนโจมตีให้กับทางบริษัทรับทราบแต่น้อยมาก กำลังดำเนินการสร้างแผนฉุกเฉินในการรับมือต่อเหตุการณ์การโจมตีทางไซเบอร์ และพนักงานไม่ทราบว่าบริษัทของตนเองมีโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่เข้มงวด ผลการสำรวจความคิดเห็นจากกลุ่มตัวอย่างพบว่า ปัจจัยด้านความสำเร็จในการดำเนินงานส่งผลต่อความมั่นคงปลอดภัยไซเบอร์ของธุรกิจพาณิชย์อิเล็กทรอนิกส์ ในภาพรวมอยู่ในระดับมาก และระดับความคิดเห็นต่อ

URU-J.ISD 254724
ปีที่ 12 ฉบับที่ 1 มกราคม - มิถุนายน 2565
ISSN 2821-9708 (Online)

ความมั่นคงปลอดภัยไซเบอร์ของธุรกิจพาณิชย์อิเล็กทรอนิกส์ ในภาพรวมอยู่ในระดับมาก โดยด้านความปลอดภัยด้านข้อมูล มีค่ามากที่สุด รองลงมาคือด้านความปลอดภัยด้านผู้ใช้

ผลการศึกษาความแตกต่างของคุณลักษณะทั่วไปของธุรกิจกับความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์สำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทย พบว่า รูปแบบธุรกิจที่แตกต่างกัน ทำให้การรักษาความลับของข้อมูล ด้านการระบุอำนาจหน้าที่ และด้านการปฏิเสธความรับผิดชอบแตกต่างกัน ระยะเวลาในการดำเนินกิจการที่แตกต่างกัน ทำให้การรักษาความลับของข้อมูล แตกต่างกัน จำนวนพนักงานในองค์กรที่แตกต่างกัน ทำให้การรักษาความลับของข้อมูล ด้านการระบุอำนาจหน้าที่ ด้านการระบุตัวตน และด้านการปฏิเสธความรับผิดชอบแตกต่างกัน ระดับตลาดที่ธุรกิจให้บริการที่แตกต่างกัน ทำให้การรักษาความลับของข้อมูล ด้านความพร้อมใช้ของข้อมูล และด้านการระบุตัวตนแตกต่างกัน ผลการศึกษาปัจจัยด้านความสำเร็จในการดำเนินกิจการที่ส่งผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ของธุรกิจพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทย พบว่า ปัจจัยด้านความสำเร็จในการดำเนินกิจการ มีความสัมพันธ์เชิงเส้นและสามารถทำนายความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อม ในประเทศไทยได้

คำสำคัญ: ความปลอดภัยทางไซเบอร์, ภัยคุกคามทางไซเบอร์, พาณิชย์อิเล็กทรอนิกส์: วิสาหกิจขนาดกลางและขนาดย่อม

URU-J.ISD 254724
ปีที่ 12 ฉบับที่ 1 มกราคม - มิถุนายน 2565
ISSN 2821-9708 (Online)

Abstract

This study aims 1. to study the principles cybersecurity of E-Commerce businesses for small and medium-sized enterprises (SMEs) in Thailand 2. to study the differences in general business factors and the security of e-commerce businesses for SMEs in Thailand and 3. to study the success factors in business operations that affect the cybersecurity of electronic commerce businesses for SMEs in Thailand. The sample groups are SMEs for E-commerce businesses, 852 data collected were randomly selected. The instrument of research was a questionnaire. The content validity was 0.93 and the reliability was 0.972. Data were analyzed by percentage, mean, standard deviation, one-way ANOVA, and the stepwise multiple regression.

The research presented that most e-commerce SMEs are engaged in the retail and wholesale business, the duration of the business is 4-9 years, the number of employees in the organization is 6-10 people, and a market level where the service business operates is in the country. There are less than 50% of employees with knowledge of information technology, and employees who have reported when attacked to the company are aware but very few. A contingency plan is being developed in response to cyberattack incidents, and employees are unaware that their company has a strict information security policy. The survey results from the sample group found that operational success factors affect the cybersecurity of e-commerce businesses. Overall, it's at a high level. The level of opinions on cybersecurity of e-commerce businesses Overall, it's at a high level with the information security most valuable followed by user safety.

The results of a study on the differences in general business characteristics and the security of e-commerce businesses for SMEs in Thailand found that the difference in the business model makes the differences in confidentiality, authorization, and non-Repudiation; the difference in operation periods makes the difference in confidentiality; the difference in the number of employees makes the differences in confidentiality, authorization, authentication, and non-Repudiation; and the differences in market level make the differences in confidentiality, availability, and authentication. The results of the study of factors of success in business operations affecting cybersecurity of e-commerce business for SMEs in Thailand found that the success factor in business operations has a linear relationship and can predict the security of e-commerce business for SMEs in Thailand.

Keywords: Cybersecurity, Cyber-attacks, E-Commerce, Small and Medium Enterprises

URU-J.ISD 254724
ปีที่ 12 ฉบับที่ 1 มกราคม - มิถุนายน 2565
ISSN 2821-9708 (Online)

บทนำ

ปัจจุบันการค้าบนโลกไซเบอร์ได้มีการเอาเทคโนโลยีเข้ามาใช้ในรูปแบบของพาณิชย์อิเล็กทรอนิกส์ (E-Commerce) มากขึ้น แต่สิ่งที่มาพร้อมกับเทคโนโลยีดิจิทัล คือภัยคุกคามทางไซเบอร์ (Cyber Attack) ที่ปัจจุบันเพิ่มขึ้นอย่างรวดเร็ว จากการประชุม World Economic Forum เมื่อปี 2021 พบว่าปัญหาภัยคุกคามทางไซเบอร์เป็น 1 ใน 10 ประเด็นที่ยังต้องเร่งหาแนวทางในการแก้ไข (World Economic Forum, 2021) ความเสียหายที่เกิดจากการการโจมตีทางไซเบอร์จะมีผลต่อธุรกิจอย่างร้ายแรง องค์กรต่าง ๆ จะต้องตระหนักและต้องมีมาตรการในการป้องกันภัยคุกคามทางไซเบอร์ จากรายงาน 2021 Global Threat Intelligence Report (GTIR) โดยบริษัท NTT Security (NTT, 2021) เผยว่าแฮกเกอร์ใช้ประโยชน์จากการไร้เสถียรภาพขององค์กรต่าง ๆ ในการโจมตีระบบโดยมุ่งเป้าหมายไปที่อุตสาหกรรมสำคัญและมีช่องโหว่ที่เกิดขึ้น นอกจากนี้จากรายงานพบว่าอุตสาหกรรมด้านการดูแลสุขภาพ (Healthcare) การผลิต (Manufacturing) และการเงิน (Financial) ถูกโจมตีเพิ่มสูงขึ้น 200%, 300% และ 53% ตามลำดับ โดยภาคอุตสาหกรรมทั้งสามรวมกันมีสัดส่วนถึง 62% ของการโจมตีทั้งหมดในปี 2021 เพิ่มขึ้น 11% จากปี 2020 จากรายงานของพาโลอัลโต้ เน็ตเวิร์กส์ เปิดเผยว่าค่าไถ่โดยเฉลี่ยที่แต่ละองค์กรต้องจ่ายในช่วงครึ่งแรกของปี 2564 อยู่ที่ราว 570,000 ดอลลาร์สหรัฐหรือประมาณ 18.8 ล้านบาท ซึ่งเพิ่มขึ้นจากปี 2563 ถึง 82% รายงานความเสียหายในการจ่ายค่าไถ่ข้อมูลเฉลี่ยต่อเดือนสูงถึง 102.3 ล้านดอลลาร์สหรัฐ และจากการศึกษาของ Microsoft ในปี 2564 พบว่าการโจมตี Ransomware กำลังจะพัฒนาไปสู่การโจมตีในลักษณะ Human-operated Ransomware ที่มีมนุษย์เป็นผู้นำปฏิบัติการ พร้อมกับการเพิ่มระดับการขู่กรรโชกหลากหลายรูปแบบ และมุ่งเป้าสร้างความเสียหายทั้งข้อมูลและชื่อเสียงขององค์กร โดยคาดการณ์ว่าจะสร้างความเสียหายสูงถึง 8.9 ล้านล้านบาทภายในปี 2574 (Microsoft, 2021)

ด้วยความก้าวหน้าทางเทคโนโลยีทำธุรกิจต่าง ๆ ต้องมุ่งสู่โลกดิจิทัล การค้าขาย การชำระเงินต้องเป็นดิจิทัลทั้งหมด เป็นผลแฮกเกอร์สามารถเข้าถึงธุรกิจมากขึ้น และไม่สามารถติดตามที่มาที่ไปได้ (Donthu, N., & Gustafsson, A., 2020) โดยเฉพาะข้อมูลซึ่งเป็นสิ่งสำคัญของการทำธุรกิจในยุคดิจิทัล ซึ่งเป็นที่หมายปองจากแฮกเกอร์ เช่น การส่งอีเมลหรือ SMS เพื่อหลอกเอาข้อมูลสำคัญ หรือหลอกลวงให้โอนเงิน ข้อมูลบัตรเครดิต (Phishing) โดยจะมาในกรรมวิธีที่แนบเนียนและซับซ้อนกว่าเดิม การโจมตีโดยใช้แรนซัมแวร์ (Ransomware) ที่มุ่งการโจมตี เพื่อขโมยข้อมูลสำคัญไปขายในตลาดมืด และเรียกค่าไถ่ รวมไปถึงการโจมตีเพื่อทำให้ระบบหรือบริการที่สำคัญไม่สามารถให้บริการได้ ธุรกิจจะมองเรื่องของรายได้มากว่าความเสี่ยงที่จะเกิดขึ้น จึงเกิดช่องโหว่ให้แฮกเกอร์เจาะระบบมากขึ้น ธุรกิจมักจะมองแต่ประโยชน์ การเข้าถึงลูกค้าอย่างใกล้ชิด ความสะดวกในการใช้จ่าย ซึ่งอยู่บนความง่ายและรวดเร็ว และนั่นจึงทำให้เกิดช่องโหว่ และแฮกเกอร์สามารถเข้ามาเจาะข้อมูลได้ เมื่อเทียบกับก่อนหน้านี้ที่มีความยุ่งยากซับซ้อน แต่โอกาสที่แฮกเกอร์เข้ามาเจาะข้อมูลนั้นแทบจะไม่มี (Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S., 2020) เพราะว่าในอดีตธุรกิจจะรู้จักแค่ไวรัสคอมพิวเตอร์ที่จะมาทำลายระบบต่าง ๆ เพื่อให้ธุรกิจต้องหยุดชะงัก หรือการหลอกล่อให้โอนเงินในรูปแบบฟิชชิง (Phishing) แต่ในปัจจุบันได้มีการยกระดับไปสู่การจารกรรมข้อมูล การขโมยข้อมูลที่สำคัญและมีผลต่อการทำธุรกิจมาเรียกค่าไถ่

URU-J.ISD 254724
ปีที่ 12 ฉบับที่ 1 มกราคม - มิถุนายน 2565
ISSN 2821-9708 (Online)

จากรายงานความปลอดภัยทางไซเบอร์สำหรับเอสเอ็มอี (SMEs) : การเตรียมพร้อมขององค์กรธุรกิจในเอเชีย-แปซิฟิกสำหรับการป้องกันภัยทางดิจิทัล (Cisco, 2021) ชี้ว่าเอสเอ็มอี ในประเทศไทยได้เผชิญต่อวิธีการในการเจาะเข้าสู่ระบบที่หลากหลาย วิธีการแรกคือการโจมตีด้วยมัลแวร์ 91% ตามด้วยฟิชชิ่ง (Phishing) 77% ทำให้เอสเอ็มอีในไทยเกือบครึ่งหนึ่งถูกโจมตีทางไซเบอร์ สาเหตุที่ทำให้ SMEs เหล่านั้นถูกโจมตี คือโซลูชั่นความปลอดภัยทางไซเบอร์ไม่มีประสิทธิภาพที่จะตรวจจับหรือป้องกันการโจมตี องค์กรไม่ได้ติดตั้งโซลูชั่นด้านวามปลอดภัยทางไซเบอร์ และ 47% ของเอสเอ็มอีในประเทศไทยเคยถูกโจมตีทางไซเบอร์ เหตุการณ์ดังกล่าวสร้างความเสียหายต่อธุรกิจเป็นอย่างมาก นอกจากนั้นรายงานยังชี้ให้เห็นว่ากลุ่มธุรกิจขนาดกลางและขนาดเล็ก หรือเอสเอ็มอี (SME) ในประเทศไทยกำลังเผชิญกับความเสี่ยงหรือการถูกโจมตีทางไซเบอร์มากขึ้นอย่างที่ไม่เคยมีมาก่อน โดยในปี 2564 ที่ผ่านมาเอสเอ็มอีในไทยถูกโจมตีทางไซเบอร์สูงถึง 65% และ 76% นั้นสูญเสียข้อมูลลูกค้าหลังจากการถูกโจมตีทางไซเบอร์ โดย 47% ของเอสเอ็มอีในประเทศไทยที่ถูกโจมตีทางไซเบอร์ในช่วง 12 เดือนที่ผ่านมา ได้รับความเสียหายทางธุรกิจไม่น้อยกว่า 500,000 ดอลลาร์สหรัฐ (ประมาณ 16 ล้านบาท) โดยที่ 28% ได้รับความเสียหาย 1 ล้านดอลลาร์ (ประมาณ 32 ล้านบาท) หรือมากกว่านั้น (Cisco, 2021)

เนื่องจากธุรกิจพาณิชย์อิเล็กทรอนิกส์ (E-Commerce) เป็นการทำธุรกรรมซื้อขายสินค้าและบริการแบบออนไลน์ การถูกโจมตีทางไซเบอร์ก็มีโอกาสเกิดขึ้นได้อยู่ตลอดเวลาและไม่สามารถที่จะคาดเดาได้ การเตรียมรับมือกับการโจมตีทางไซเบอร์ได้ก็สามารถทำได้เช่นกัน ด้วยการมองหาเทคโนโลยี (Technology) ที่สามารถป้องกันการโจมตีทางไซเบอร์ การให้ความสำคัญกับบุคลากร (People) ในองค์กรธุรกิจ ภายใต้กระบวนการ (Process) ที่เหมาะสมกับธุรกิจ ปัจจุบันแฮกเกอร์มีบริการ Ransomware as a Service เป็นรูปแบบที่หากใครรู้ไม่เท่าทันอาจตกเป็นเหยื่อและกลายเป็นผู้ช่วยแฮกเกอร์โดยไม่รู้ตัวในเวลาเดียวกัน (Puat, H. A. M., & Abd Rahman, N. A., 2020) และใช่ว่าเมื่อมีเทคโนโลยีแล้วธุรกิจจะปลอดภัยจากภัยคุกคาม การบริหารความเสี่ยงทางไซเบอร์ที่ดี จะขาดในส่วนของบุคลากร และกระบวนการจัดการต่อเหตุการณ์ที่เกิดขึ้นไปไม่ได้ องค์กรจึงจำเป็นต้องมีการให้ความรู้แก่บุคลากรในองค์กร รวมถึงการสร้างกระบวนการที่ดี เพื่อลดความผิดพลาด และเพิ่มขีดความสามารถให้ทีมงานสามารถตอบสนองต่อเหตุการณ์ได้อย่างมีประสิทธิภาพสูงสุด

จากปัญหาการโจมตีทางไซเบอร์ (Cyber Attacks) ที่มีความรุนแรงที่เพิ่มขึ้น ทำให้ทุกองค์กรต้องหันมาให้ความสำคัญเกี่ยวกับความปลอดภัยทางไซเบอร์ (Cybersecurity) แต่เนื่องจากเป็นเรื่องที่ประเทศไทยเพิ่งตระหนักและตื่นตัว และเป็นเรื่องที่ยากยิ่งต่อการดำเนินการ ทำให้ผู้บริหารระดับสูงจำนวนมากไม่สามารถปรับตัวได้ทัน และไม่เข้าใจถึงบริบทการเปลี่ยนแปลงครั้งใหญ่นี้ จึงทำให้หลายองค์กรไม่สามารถดำเนินการด้านความปลอดภัยทางไซเบอร์ได้อย่างมีประสิทธิภาพ สำหรับธุรกิจพาณิชย์อิเล็กทรอนิกส์จะปฏิเสธไม่ได้เลยว่าธุรกรรมต่าง ๆ ต้องมีความเกี่ยวข้องกับดิจิทัล การตกเป็นเหยื่อสำหรับการโจมตี การจารกรรมจากแฮกเกอร์ยิ่งมากขึ้นตามไปด้วย จากปัญหาที่ได้ทำการศึกษามาทั้งหมด ทำให้ผู้ศึกษามีความสนใจที่จะศึกษาถึงปัจจัยที่มีผลกระทบต่อความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์จากการโจมตีทางไซเบอร์ โดยศึกษาผลที่เกิดขึ้นกับวิสาหกิจขนาดกลางและขนาดย่อมที่มีอยู่เป็นจำนวนมาก เพื่อจะนำผลการศึกษาที่

URU-J.ISD 254724
ปีที่ 12 ฉบับที่ 1 มกราคม - มิถุนายน 2565
ISSN 2821-9708 (Online)

ได้ไปเป็นแนวทางสำหรับผู้ประกอบการธุรกิจพาณิชย์อิเล็กทรอนิกส์ได้ตระหนัก เข้าใจ และรับมือจากการโจมตีทางไซเบอร์ต่อไป

วัตถุประสงค์การวิจัย

1. เพื่อศึกษาหลักการด้านความมั่นคงปลอดภัยไซเบอร์ของธุรกิจพาณิชย์อิเล็กทรอนิกส์สำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทย

2. เพื่อศึกษาความแตกต่างของคุณลักษณะทั่วไปของธุรกิจกับความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลาง และขนาดย่อมในประเทศไทย

3. เพื่อศึกษาปัจจัยด้านความสำเร็จในการดำเนินกิจการที่ส่งผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ ของธุรกิจพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทย

วิธีดำเนินการวิจัย

รูปแบบการวิจัย

การวิจัยนี้เป็นการวิจัยเชิงปริมาณแบบสำรวจความคิดเห็น (Survey Research) โดยการศึกษาด้วยการทบทวนวรรณกรรมในเชิงเอกสาร (Documentary Study) ทำการศึกษาและรวบรวมข้อมูลจากเอกสารและหลักฐานที่เกี่ยวข้อง เพื่อให้นำมาพัฒนาเป็นกรอบแนวคิดในการวิจัย เพื่อแสดงถึงความสัมพันธ์ระหว่างตัวแปรต่างๆ ที่จะนำมาใช้การศึกษา

ขอบเขตด้านประชากรและกลุ่มตัวอย่าง

ตัวแปรอิสระ ได้แก่ คุณลักษณะทั่วไปของธุรกิจ ประกอบด้วย รูปแบบธุรกิจ ระยะเวลาในการดำเนินกิจการ จำนวนพนักงานในองค์กร และระดับตลาดที่ธุรกิจให้บริการ สถานการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย สัดส่วนพนักงานที่รู้ IT การได้รับรายงานการโจมตี แผนฉุกเฉินรับมือการโจมตี และนโยบายรับมือการโจมตีที่เข้มงวด และปัจจัยด้านความสำเร็จในการดำเนินกิจการ ประกอบด้วย บุคลากร กระบวนการ และเทคโนโลยี

ตัวแปรตาม ได้แก่ ความมั่นคงปลอดภัยไซเบอร์สำหรับธุรกิจพาณิชย์อิเล็กทรอนิกส์ ซึ่งแบ่งเป็น 2 ด้าน คือ 1. ความปลอดภัยด้านข้อมูล ได้แก่ การรักษาความลับของข้อมูล (Confidential) คือ การปกป้องข้อมูลสารสนเทศจากการเข้าถึงจากผู้ไม่มีสิทธิ การรักษาความถูกต้อง (Integrity) คือ การปกป้องข้อมูลไม่ให้ถูกเปลี่ยนแปลง แก้ไข หรือเกิดความเสียหายจากผู้ไม่มีสิทธิหรือผู้ไม่ได้รับอนุญาตไม่ว่าจะโดยเจตนาหรือความไม่ตั้งใจ และความพร้อมใช้ของข้อมูล (Availability) คือ การสร้างความเชื่อมั่นว่าระบบสารสนเทศสามารถตอบสนอง เมื่อผู้มีสิทธิหรือผู้ที่ได้รับอนุญาตต้องการใช้งาน และ 2. ความปลอดภัยด้านผู้ใช้ ได้แก่ การระบุอำนาจหน้าที่ (Authorization) คือ การอนุญาตให้เข้าใช้งานและระดับสิทธิ์ในการเข้าถึง การระบุตัวบุคคล (Authentication) คือ การพิสูจน์ตัวตนเพื่อยืนยันว่าเป็นบุคคลคนนั้นจริง จึงจะเข้าสู่ข้อมูลหรือระบบนั้นได้ และการปฏิเสธความรับผิดชอบ(Non-Repudiation) คือ การสื่อสารซึ่งผู้ส่งข้อมูลได้รับหลักฐานว่าได้มีการส่งข้อมูลแล้วและผู้รับก็ได้รับการยืนยันว่าผู้ส่งเป็นใคร โดยทั้งผู้ส่งและผู้รับจะไม่สามารถปฏิเสธได้ว่าไม่มีความเกี่ยวข้องกับข้อมูลดังกล่าวในภายหลัง

ประชากรและกลุ่มตัวอย่าง

ประชากรที่ในการวิจัยครั้งนี้ คือวิสาหกิจขนาดกลาง และขนาดย่อม ที่ดำเนินธุรกิจพาณิชย์อิเล็กทรอนิกส์ในประเทศไทย จำนวน 644,071 บริษัท (Electronic Transactions Development

URU-J.ISD 254724
ปีที่ 12 ฉบับที่ 1 มกราคม - มิถุนายน 2565
ISSN 2821-9708 (Online)

Agency (Public Organization), 2018) การกำหนดขนาดตัวอย่าง ทำโดยใช้สูตรการคำนวณของทาโร่ยามาเน่ (Taro Yamane, 1973) ที่ระดับความเชื่อมั่นร้อยละ 95 ได้กลุ่มตัวอย่าง 400 บริษัท โดยขอความอนุเคราะห์จากผู้ตอบแบบสอบถามที่ทำหน้าที่หรือมีส่วนรับผิดชอบในงานด้านพาณิชย์อิเล็กทรอนิกส์ของบริษัทเป็นผู้ตอบแบบสอบถาม โดยผู้วิจัยทำการส่งแบบ สอบถามบริษัทละ 3 ชุด รวมจำนวนแบบสอบถามที่ส่งไปทั้งสิ้น 1200 ชุด ได้รับตอบกลับมาจำนวนทั้งสิ้น 852 ชุดคิดเป็น response rate เท่ากับ 70.83% และดำเนินการประมวลผลข้อมูลด้วยโปรแกรม SPSS

เครื่องมือที่ใช้ในการวิจัย

เครื่องมือใช้ในการวิจัย คือแบบสอบถาม (Questionnaires) โดยแบ่งออกเป็น 5 ส่วน ดังต่อไปนี้ แบบสอบถามในส่วนที่ 1 เป็นข้อมูลทั่วไปของสถานประกอบการ และ ส่วนที่ 2 เป็นข้อมูลเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยส่วนที่ 1 และ 2 มีคำตอบให้เลือกหลายคำตอบ แต่ผู้ตอบสามารถเลือกตอบเพียงข้อเดียว ประกอบด้วยจำนวนคำถามทั้งสิ้น 4 ข้อ มีลักษณะเป็นแบบตรวจสอบรายการ (Checklist) แบบสอบถามในส่วนที่ 3 เป็นแบบสอบถามความคิดเห็นด้านปัจจัยความสำเร็จที่มีผลต่อการโจมตีทางไซเบอร์ต่อระบบพาณิชย์อิเล็กทรอนิกส์ ที่จะส่งผลต่อความปลอดภัยของพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อม ที่ประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ในประเทศไทย และ ส่วนที่ 4 เป็นความคิดเห็นเกี่ยวกับข้อมูลความปลอดภัยของพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อม ที่ประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ในประเทศไทย โดยส่วนที่ 3 และ 4 มีลักษณะคำถามเป็นมาตรวัดแบบ Likert Scale (Likert, R. A.,1932:1-55) ครอบคลุมตัวแปร โดยแบ่งเป็น 5 ระดับ คือ เห็นด้วยมากที่สุด มาก ปานกลาง น้อย และน้อยมาก และส่วนที่ 5 ข้อเสนอแนะเพิ่มเติม โดยเป็นคำถามแบบปลายเปิดให้ผู้ตอบแบบสอบถามได้แสดงความคิดเห็น จากกนั้นนำมาทดสอบความตรงทางเนื้อหา โดยหาค่าดัชนีความสอดคล้อง IOC (Index of Congruence) ของเครื่องมือการวิจัยจากผู้เชี่ยวชาญ 5 ท่าน โดยหาค่าดัชนีความสอดคล้อง IOC (Index of Item Objective Congruence) โดยมีค่า IOC ที่ได้ต้องมีค่ามากกว่า 0.5 (ลัดดาวัลย์ เพชรโรจน์ และอัจรา ชำนิประศาสน์, 2547) ได้ค่า IOC เฉลี่ยทั้งฉบับอยู่ที่ 0.93 และทำการวัดความเชื่อมั่นหรือความสอดคล้องภายในด้วยค่าสัมประสิทธิ์แอลฟาของครอนบาค (Cronbach's Alpha Coefficient) ด้วยการนำแบบสอบถามที่ได้ไปทดลองใช้กับกลุ่มตัวอย่างจำนวน 30 คนซึ่งไม่ใช่กลุ่มตัวอย่าง โดยเกณฑ์ในการพิจารณาค่าสัมประสิทธิ์แอลฟาครอนบาค ต้องมีค่ามากกว่า 0.7 (ศิริชัย กาญจนวาสี, 2544) โดยในการวิจัยได้ค่าความเชื่อมั่นเท่ากับ 0.972

การวิเคราะห์ข้อมูล

วิเคราะห์ข้อมูลทางสถิติผู้วิจัยได้นำข้อมูลที่ได้จากเครื่องมือการวิจัยมาทำการวิเคราะห์ข้อมูลโดยใช้สถิติเชิงพรรณนาประกอบด้วย ค่าร้อยละมาทำการวิเคราะห์ข้อมูลในส่วนที่ 1 และ ส่วนที่ 2 ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐานในการวิเคราะห์ข้อมูลได้จากเครื่องมือวิจัยในส่วนที่ 3 และส่วนที่ 4 มีการใช้สถิติเชิงอนุมานในการวิเคราะห์ข้อมูลและทดสอบสมมติฐานของงานวิจัย โดยการทดสอบสมมติฐานเพื่อทดสอบความแตกต่างระหว่างค่าเฉลี่ยของกลุ่มตัวอย่าง 2 กลุ่มที่เป็นอิสระกัน ผู้วิจัยได้ใช้สถิติ ทดสอบสมมติฐานในความแตกต่างระหว่างค่าเฉลี่ยของกลุ่มตัวอย่างที่มีมากกว่า 2 กลุ่ม โดยทดสอบความ

URU-J.ISD 254724
ปีที่ 12 ฉบับที่ 1 มกราคม - มิถุนายน 2565
ISSN 2821-9708 (Online)

เท่ากันของความแปรปรวน (Homogeneity of Variances) โดยใช้สถิติ Levene Statistic เพื่อการวิเคราะห์ ถ้าผลที่ได้จาก Levene Statistic มีค่า Sig ≥ 0.05 แล้วจะได้ใช้สถิติวิเคราะห์ความแปรปรวนทางเดียว (One-Way Analysis of Variance) (Wanichbuncha Kalaya, 2011) กับทำการทดสอบเป็นรายคู่ต่อไปเพื่อดูว่ามีคู่ใดบ้างที่แตกต่างกัน โดยใช้วิธี Fisher's Least Significant Difference (LSD) (กัลยา วานิชย์บัญชา, 2545: 332-333) และถ้าผลที่ได้จาก Levene Statistic มีค่า Sig < 0.05 แล้วจะได้ใช้สถิติวิเคราะห์ Brown-Forsythe (B) (Hartung, Joachim, 2001) กับการวิเคราะห์ผลต่างค่าเฉลี่ยรายคู่ Dunnett's T3 (Keppel, Geoffrey, 1982) โดยผลการทดสอบมีความแตกต่างอย่างมีนัยสำคัญทางสถิติแล้ว

ผลการวิจัย

ผลการวิเคราะห์ข้อมูลนำเสนอตามวัตถุประสงค์ของการวิจัยและการทดสอบสมมติฐานการวิจัยในการวิเคราะห์ข้อมูลครั้งนี้ผู้วิจัยได้ทำการวิเคราะห์ข้อมูล โดยแบ่งการนำเสนอดังต่อไปนี้

1. ผลการศึกษาหลักการด้านความมั่นคงปลอดภัยไซเบอร์ของธุรกิจพาณิชย์อิเล็กทรอนิกส์สำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทย สามารถนำเสนอผลการศึกษาได้ดังนี้

ผลการวิเคราะห์คุณลักษณะทั่วไปของธุรกิจสำหรับวิสาหกิจขนาดกลางและขนาดย่อม ที่ประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ จากการวิเคราะห์ข้อมูลคุณลักษณะทั่วไปของธุรกิจจากกลุ่มตัวอย่าง พบว่าวิสาหกิจขนาดกลางและขนาดย่อมที่ประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ส่วนใหญ่ทำธุรกิจด้านการค้าปลีกและค้าส่ง มีระยะเวลาในการดำเนินธุรกิจมาแล้ว 4-9 ปี มีจำนวนพนักงานในองค์กร 6-10 คน และวิสาหกิจขนาดและขนาดย่อมที่ประกอบธุรกิจพาณิชย์ธุรกิจพาณิชย์อิเล็กทรอนิกส์ส่วนใหญ่มีการทำการค้าโดยมีระดับตลาดที่ธุรกิจให้บริการดำเนินธุรกิจภายในประเทศ

ผลการวิเคราะห์สถานการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อม ที่ประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ จากการวิเคราะห์ข้อมูลสถานการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จากกลุ่มตัวอย่าง พบว่าวิสาหกิจขนาดกลางและขนาดย่อมที่ประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ส่วนใหญ่ มีสัดส่วนของพนักงานที่มีพื้นฐานความรู้ทางด้านเทคโนโลยีสารสนเทศน้อยกว่า 50% พนักงานที่ตกเป็นเหยื่อจากการโจมตีทางไซเบอร์มีการทำรายงานให้กับทางบริษัทรับทราบแต่น้อยมาก มีแผนฉุกเฉินในการรับมือต่อเหตุการณ์การโจมตีทางไซเบอร์โดยกำลังดำเนินการภายใต้แผนฉุกเฉินนี้อยู่ และไม่ทราบว่าบริษัทหรือองค์กรของตนเองมีโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่เข้มงวดเลย

ผลการวิเคราะห์ข้อมูลปัจจัยด้านความสำเร็จในการดำเนินงานที่ส่งผลกระทบต่อความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อม การวิเคราะห์ข้อมูลปัจจัยด้านความสำเร็จในการดำเนินงานจากกลุ่มตัวอย่าง แสดงได้ดังรายละเอียดแสดงได้ดัง ตารางที่ 1

ตารางที่ 1 แสดงการวิเคราะห์ข้อมูลปัจจัยด้านความสำเร็จในการดำเนินงานที่ส่งผลกระทบต่อความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อม

ด้านที่	ปัจจัยด้านความสำเร็จในการดำเนินงาน	ระดับความคิดเห็น		
		$\overline{X}$	SD	แปลผล
1	ด้านบุคลากร	3.58	0.708	มาก
2	ด้านกระบวนการ	3.56	0.681	มาก
3	ด้านเทคโนโลยี	3.59	0.676	มาก
	รวม	**3.58**	**0.687**	**มาก**

จากตารางที่ 1 พบว่าปัจจัยด้านความสำเร็จในการดำเนินงาน โดยภาพรวมอยู่ในระดับมาก ($\overline{X}$ = 3.58, SD =0.687) เมื่อพิจารณาเป็นรายด้านพบว่าทุกด้านอยู่ในระดับมาก โดยด้านเทคโนโลยี มีค่าเฉลี่ยมากที่สุด รองลงมาคือด้านบุคลากร และด้านกระบวนการที่มีค่าเฉลี่ยน้อยที่สุด

ผลการวิเคราะห์ข้อมูลความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อม การวิเคราะห์ข้อมูลความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อม แสดงรายละเอียดแสดงได้ดังตารางที่ 2

ตารางที่ 2 แสดงการวิเคราะห์ข้อมูลความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อม

ด้านที่	ความปลอดภัยในธุรกิจพาณิชย์อิเล็กทรอนิกส์	ระดับความคิดเห็น		
		$\overline{X}$	SD	แปลผล
1	**ความปลอดภัยด้านข้อมูล**	**3.59**	**0.690**	**มาก**
	1.1 การรักษาความลับของข้อมูล	3.59	0.701	มาก
	1.2 การรักษาความถูกต้อง	3.58	0.687	มาก
	1.3 ความพร้อมใช้ของข้อมูล	3.61	0.671	มาก
2	**ความปลอดภัยด้านผู้ใช้**	**3.57**	**0.691**	**มาก**
	2.1 การระบุอำนาจหน้าที่	3.57	0.676	มาก
	2.2 การระบุตัวตน	3.59	0.705	มาก
	2.3 การปฏิเสธความรับผิดชอบ	3.57	0.678	มาก
	รวม	**3.58**	**0.691**	**มาก**

ในการวิเคราะห์ข้อมูลการศึกษาความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อม โดยภาพรวมอยู่ในระดับมาก ($\overline{X}$ = 3.58, SD =0.691) เมื่อพิจารณาเป็นรายด้าน พบว่าทุกด้านอยู่ในระดับมาก โดยด้านความปลอดภัยด้านข้อมูล มีค่าเฉลี่ยมากที่สุด รองลงมาคือด้านความปลอดภัยด้านผู้ใช้ เมื่อพิจารณาในด้านความปลอดภัยด้านข้อมูล พบว่า

URU-J.ISD 254724
ปีที่ 12 ฉบับที่ 1 มกราคม - มิถุนายน 2565
ISSN 2821-9708 (Online)

ทุกด้านอยู่ในระดับมาก โดยด้านความพร้อมใช้ของข้อมูล มีค่าเฉลี่ยมากที่สุด รองลงมาคือด้านการรักษาความลับของข้อมูล และด้านการรักษาความถูกต้อง และเมื่อพิจารณาในด้านความปลอดภัยด้านผู้ใช้ พบว่าทุกด้านอยู่ในระดับมาก โดยด้านการระบุตัวตนมีค่าเฉลี่ยมากที่สุด รองลงมาคือ ด้านการระบุอำนาจหน้าที่ และด้านการปฏิเสธความรับผิดชอบ

2. ผลการศึกษาความแตกต่างของคุณลักษณะทั่วไปของธุรกิจกับความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทย สามารถนำเสนอผลการศึกษาได้ดังนี้

ผลการวิเคราะห์ความแตกต่างของคุณลักษณะทั่วไปของธุรกิจ ที่ส่งผลกระทบต่อความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อม

2.1 การเปรียบเทียบคุณลักษณะทั่วไปของธุรกิจ ด้านรูปแบบธุรกิจกับความปลอดภัยต่อธุรกิจพาณิชย์อิเล็กทรอนิกส์สำหรับวิสาหกิจขนาดกลางและขนาดย่อม ผลการวิเคราะห์สรุปผลแสดงตามตารางที่ 3

ตารางที่ 3 วิเคราะห์เปรียบเทียบคุณลักษณะทั่วไปของธุรกิจ ด้านรูปแบบธุรกิจ กับความปลอดภัยต่อธุรกิจพาณิชย์อิเล็กทรอนิกส์สำหรับวิสาหกิจขนาดกลางและขนาดย่อม

ความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์	ทดสอบความแปรปรวน		ทดสอบค่าเฉลี่ย				ผลการทดสอบ
	Levene Statistic	Sig.	F-Test	Sig.	Brown-Forsythe	Sig.	
การรักษาความลับของข้อมูล	1.881	0.070	2.143	0.037*			แตกต่าง
การรักษาความถูกต้อง	1.068	0.382	1.253	0.271			ไม่แตกต่าง
ความพร้อมใช้ของข้อมูล	4.195	0.000			0.437	0.879	ไม่แตกต่าง
การระบุอำนาจหน้าที่	7.057	0.000			2.519	0.015*	แตกต่าง
การระบุตัวตน	2.009	0.051	2.006	0.052			ไม่แตกต่าง
การปฏิเสธความรับผิดชอบ	7.057	0.000			2.519	0.023*	แตกต่าง

*มีนัยสำคัญทางสถิติที่ระดับ 0.05

จากตารางที่ 3 พบว่ารูปแบบธุรกิจที่แตกต่างกัน มีผลทำให้ความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์สำหรับวิสาหกิจขนาดกลางและขนาดย่อม ด้านการรักษาความลับของข้อมูล ด้านการระบุอำนาจหน้าที่ และด้านการปฏิเสธความรับผิดชอบ แตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ส่วนด้านการรักษาความถูกต้อง ด้านความพร้อมใช้ของข้อมูล และด้านการระบุตัวตน ไม่แตกต่างกัน

2.2 การเปรียบเทียบคุณลักษณะทั่วไปของธุรกิจ ด้านระยะเวลาในการดำเนินกิจการกับความปลอดภัยต่อธุรกิจพาณิชย์อิเล็กทรอนิกส์สำหรับวิสาหกิจขนาดกลางและขนาดย่อม ผลการวิเคราะห์สรุปผลแสดงตามตารางที่ 4

ตารางที่ 4 วิเคราะห์เปรียบเทียบคุณลักษณะทั่วไปของธุรกิจ ด้านระยะเวลาในการดำเนินกิจการกับความปลอดภัยต่อธุรกิจพาณิชย์อิเล็กทรอนิกส์สำหรับวิสาหกิจขนาดกลางและขนาดย่อม

ความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์	ทดสอบความแปรปรวน		ทดสอบค่าเฉลี่ย				ผลการทดสอบ
	Levene Statistic	Sig.	F-Test	Sig.	Brown-Forsythe	Sig.	
การรักษาความลับของข้อมูล	1.050	0.370	3.258*	0.021*			แตกต่าง
การรักษาความถูกต้อง	1.806	0.145	1.756	0.154			ไม่แตกต่าง
ความพร้อมใช้ของข้อมูล	1.555	0.199	2.595	0.051			ไม่แตกต่าง
การระบุอำนาจหน้าที่	6.739	0.000			1.350	0.219	ไม่แตกต่าง
การระบุตัวตน	1.814	0.143	2.010	0.111			ไม่แตกต่าง
การปฏิเสธความรับผิดชอบ	6.739	0.000			1.350	0.258	ไม่แตกต่าง

*มีนัยสำคัญทางสถิติที่ระดับ 0.05

จากตารางที่ 4 พบว่าระยะเวลาในการดำเนินกิจการที่แตกต่างกัน มีผลทำให้ความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์สำหรับวิสาหกิจขนาดกลางและขนาดย่อม ด้านการรักษาความลับของข้อมูลแตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ส่วนด้านการรักษาความถูกต้อง ด้านความพร้อมใช้ของข้อมูล ด้านการระบุอำนาจหน้าที่ ด้านการระบุตัวตน และด้านการปฏิเสธความรับผิดชอบไม่แตกต่างกัน

2.3 การเปรียบเทียบคุณลักษณะทั่วไปของธุรกิจ ด้านจำนวนพนักงานในองค์กรกับความปลอดภัยต่อธุรกิจพาณิชย์อิเล็กทรอนิกส์สำหรับวิสาหกิจขนาดกลางและขนาดย่อม ผลการวิเคราะห์สรุปผลแสดงตามตารางที่ 5

ตารางที่ 5 วิเคราะห์เปรียบเทียบคุณลักษณะทั่วไปของธุรกิจ ด้านจำนวนพนักงานในองค์กรกับความปลอดภัยต่อธุรกิจพาณิชย์อิเล็กทรอนิกส์สำหรับวิสาหกิจขนาดกลางและขนาดย่อม

ความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์	ทดสอบความแปรปรวน		ทดสอบค่าเฉลี่ย				ผลการทดสอบ
	Levene Statistic	Sig.	F-Test	Sig.	Brown-Forsythe	Sig.	
การรักษาความลับของข้อมูล	1.441	0.237	4.850	0.008*			แตกต่าง
การรักษาความถูกต้อง	2.465	0.086	2.173	0.114			ไม่แตกต่าง
ความพร้อมใช้ของข้อมูล	2.718	0.067	0.209	0.812			ไม่แตกต่าง
การระบุอำนาจหน้าที่	3.167	0.043			3.562	0.028*	แตกต่าง
การระบุตัวตน	3.806	0.023			8.355	0.000*	แตกต่าง
การปฏิเสธความรับผิดชอบ	3.157	0.048			3.763	0.033*	แตกต่าง

*มีนัยสำคัญทางสถิติที่ระดับ 0.05

URU-J.ISD 254724
ปีที่ 12 ฉบับที่ 1 มกราคม - มิถุนายน 2565
ISSN 2821-9708 (Online)

จากตารางที่ 5 พบว่าจำนวนพนักงานในองค์กรที่แตกต่างกัน มีผลทำให้ความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์สำหรับวิสาหกิจขนาดกลางและขนาดย่อม ด้านการรักษาความลับของข้อมูล ด้านการระบุอำนาจหน้าที่ ด้านการระบุตัวตน และด้านการปฏิเสธความรับผิดชอบแตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ส่วนด้านการรักษาความถูกต้อง และด้านความพร้อมใช้ของข้อมูล ไม่แตกต่างกัน

2.4 การเปรียบเทียบคุณลักษณะทั่วไปของธุรกิจ ด้านระดับตลาดที่ธุรกิจให้บริการความปลอดภัยต่อธุรกิจพาณิชย์อิเล็กทรอนิกส์สำหรับวิสาหกิจขนาดกลางและขนาดย่อม ผลการวิเคราะห์สรุปผลแสดงตามตารางที่ 6

ตารางที่ 6 วิเคราะห์เปรียบเทียบคุณลักษณะทั่วไปของธุรกิจ ด้านระดับตลาดที่ธุรกิจให้บริการกับความปลอดภัยต่อธุรกิจพาณิชย์อิเล็กทรอนิกส์สำหรับวิสาหกิจขนาดกลางและขนาดย่อม

ความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์	ทดสอบความแปรปรวน		ทดสอบค่าเฉลี่ย				ผลการทดสอบ
	Levene Statistic	Sig.	F-Test	Sig.	Brown-Forsythe	Sig.	
การรักษาความลับของข้อมูล	4.852	0.000			5.303	0.000*	แตกต่าง
การรักษาความถูกต้อง	2.400	0.036			2.047	0.072	ไม่แตกต่าง
ความพร้อมใช้ของข้อมูล	0.514	0.766	2.324	0.041*			แตกต่าง
การระบุอำนาจหน้าที่	2.235	0.049			1.301	0.269	ไม่แตกต่าง
การระบุตัวตน	4.788	0.000			3.209	0.009*	แตกต่าง
การปฏิเสธความรับผิดชอบ	2.235	0.045			1.301	0.286	ไม่แตกต่าง

*มีนัยสำคัญทางสถิติที่ระดับ 0.05

จากตารางที่ 6 พบว่าระดับตลาดที่ธุรกิจให้บริการที่แตกต่างกัน มีผลทำให้ความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์สำหรับวิสาหกิจขนาดกลางและขนาดย่อม ด้านการรักษาความลับของข้อมูล ด้านความพร้อมใช้ของข้อมูล และด้านการระบุตัวตนแตกต่างกันอย่างมีนัยสำคัญ ทางสถิติที่ระดับ 0.05 โดยเมื่อทำการทดสอบเป็นรายคู่โดยใช้วิธี Fisher's Least Significant Difference (LSD) ได้ทำการพิจารณาในแต่ละด้าน โดยในด้านการรักษาความลับของข้อมูลพบว่า ระดับตลาดของวิสาหกิจขนาดกลางและขนาดย่อมที่ให้บริการในระดับภูมิภาค มีค่าเฉลี่ยรายคู่มากกว่าระดับตลาดที่อยู่ในระดับประเทศ และระดับนานาชาติ ในด้านความพร้อมใช้ของข้อมูลไม่พบความแตกต่างรายคู่ และในด้านการระบุตัวตน พบว่า ระดับตลาดของวิสาหกิจขนาดกลางและขนาดย่อมที่ให้บริการในระดับภูมิภาค มีค่าเฉลี่ยรายคู่มากกว่าระดับตลาดที่อยู่ในระดับประเทศ และระดับนานาชาติ ส่วนด้านการรักษาความถูกต้อง ด้านการระบุอำนาจหน้าที่ และด้านการปฏิเสธความรับผิดชอบไม่แตกต่างกัน

3. ผลการศึกษาปัจจัยด้านความสำเร็จในการดำเนินกิจการที่ส่งผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ ของธุรกิจพาณิชย์อิเล็กทรอนิกส์สำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทย พบว่า ปัจจัยด้านความสำเร็จในการดำเนินกิจการ ที่ประกอบด้วยตัวแปรด้านบุคลากร

URU-J.ISD 254724
ปีที่ 12 ฉบับที่ 1 มกราคม - มิถุนายน 2565
ISSN 2821-9708 (Online)

ด้านกระบวนการ และด้านเทคโนโลยี มีค่า Tolerance สูงกว่าเกณฑ์ที่กำหนด คือมากกว่า 0.10 (Foxall, G.R., & Yani-de-Soriano, M.M. (2005) และค่า VIF ไม่เกิน 10 (Belsley D., 1991) แสดงให้เห็นว่า ตัวแปรแต่ละตัวไม่มีความเป็นเส้นตรงร่วมกันเป็นอย่างมาก (Multicollinearity) หรือไม่มีความซ้ำซ้อนกันในการวัดจึงสรุปได้ว่าตัวแปรอิสระทั้ง 3 ตัวแปร มีความเหมาะสมที่จะนำไปวิเคราะห์การถดถอยพหุคูณ (Multiple regression) โดยการวิเคราะห์ถดถอยเชิงพหุคูณและค่าสัมประสิทธิ์สหสัมพันธ์พหุคูณ แสดงดังตารางที่ 7

ตารางที่ 7 ผลการวิเคราะห์ Stepwise Multiple Regression Analysis ของปัจจัยด้านความสำเร็จในการดำเนินกิจการที่ส่งผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ของธุรกิจพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทย

ตัวแปร	B	SE	t	Sig.	Tolerance	VIF
ค่าคงที่ (constant)	0.925	0.064	14.450	0.000		
ด้านบุคลากร (X_1)	0.396	0.012	33.663	0.000*	0.489	2.043
ด้านกระบวนการ (X_2)	0.197	0.014	14.123	0.000*	0.138	7.243
ด้านเทคโนโลยี (X_3)	0.150	0.013	11.520	0.000*	0.129	7.764
$R = 0.852$, $R^2 = 0.725$, Adjust $R^2 = 0.724$, SE = 0.145, F = 746.938, Sig. = 0.000*						

* มีนัยสำคัญทางสถิติที่ระดับ .05

จากตาราง 7 ผลการวิเคราะห์พบว่า ตัวแปรที่สามารถทำนายความปลอดภัยของธุรกิจพาณิชย์ (X_2) และด้านเทคโนโลยี (X_3) โดยมีค่าสัมประสิทธิ์สหสัมพันธ์พหุคูณ ได้ร้อยละ 72.50 ($R^2 = 0.725$) และสามารถพยากรณ์ ความมั่นคงปลอดภัยไซเบอร์ของธุรกิจพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อม โดยมีความคลาดเคลื่อนมาตรฐานในการพยากรณ์เท่ากับ ± 0.145 อย่างมีนัยสำคัญทางสถิติที่ 0.00 นำค่าสัมประสิทธิ์ของตัวทำนายมาเขียนเป็นสมการทำนายความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อม (Y) ดังนี้

$$Y = 0.925 + 0.396\ X_1\ 0.195\ X_2 + 0.15\ X_3$$

ผลการศึกษา สรุปได้ว่าตัวแปรด้านบุคลากร ด้านกระบวนการ และด้านเทคโนโลยี มีความสัมพันธ์ทางบวกกับความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อม (Y) อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 และเป็นปัจจัยที่เป็นตัวกำหนด ความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อม

URU-J.ISD 254724
ปีที่ 12 ฉบับที่ 1 มกราคม - มิถุนายน 2565
ISSN 2821-9708 (Online)

อภิปรายผลการวิจัย

จากการศึกษา ปัจจัยที่ส่งผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ของธุรกิจพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อม สามารถนำมาอภิปรายผลได้ดังนี้

1. ปัจจัยด้านความสำเร็จในการดำเนินงานที่ส่งผลกระทบต่อความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทยด้านบุคลากร โดยภาพรวมพบว่าอยู่ในระดับมาก เนื่องจากพนักงานมีเข้าใจประเด็นทางจริยธรรมและกฎหมายที่เกี่ยวข้องกับการเข้าถึงและการใช้ข้อมูล มีความเท่าทันการเปลี่ยนแปลงของเทคโนโลยีและรู้จักวิธีใช้เพื่อการเรียนรู้ มีความเข้าใจแนวคิดและการทำงานพื้นฐานของเครื่องมือดิจิทัล และเลือกใช้เทคโนโลยีได้เหมาะกับวัตถุประสงค์ เข้าใจข้อดีข้อเสียของเทคโนโลยีที่มีอยู่ในตลาด สอดคล้องกับงานวิจัยของ Jordan, M. (2020) ซึ่งพบว่าการสร้างความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ให้กับพนักงานขององค์กร ถึงความเสียหายอันจะเกิดจากภัยคุกคามทางไซเบอร์ รวมไปถึงการมองไปถึงเพื่อนร่วมงานที่พนักงานจะต้องพึงระวังและมองข้ามไม่ได้เด็ดขาด อีกทั้งยังสอดคล้องกับงานวิจัยของ He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., & Tian, X. (2019) ที่พบว่าการพัฒนาความสามารถของพนักงานในรักษาความปลอดภัยทางไซเบอร์ผ่านการฝึกอบรมมัลแวร์เสมือนจริง ทำให้พนักงานในองค์กรได้ตระหนักรู้ถึงความปลอดภัยในโลกไซเบอร์เพื่อป้องกันการรั่วไหลของข้อมูล เพื่อหาวิธีการตรวจสอบผลกระทบของวิธีการฝึกอบรมความมั่นคงปลอดภัยทางไซเบอร์ ที่มีต่อการรับรู้ความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ของพนักงาน

2. ปัจจัยด้านความสำเร็จในการดำเนินงานที่ส่งผลกระทบต่อความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทยด้านกระบวนการ โดยภาพรวมพบว่าอยู่ในระดับมาก ทั้งนี้เนื่องมาจากบริษัทมีการกำกับดูแลกิจการและวัฒนธรรมองค์กรให้เกิดประสิทธิภาพสูงสุด ส่งเสริมให้มีการตระหนักถึงความเสี่ยง และสร้างวัฒนธรรมการบริหารจัดการความเสี่ยงที่ดีภายใน ซึ่งสอดคล้องกับ Iaiani, M., Tugnoli, A., Bonvicini, S., & Cozzani, V. (2021) พบว่าเหตุการณ์ผิดปกติที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ในกระบวนการสำหรับโรงงานอุตสาหกรรม มาจากการที่ไม่ได้กำหนดกรอบของกระบวนการในการป้องกันการโจมตีทางไซเบอร์ จึงได้ทำการศึกษาถึงจุดมุ่งหมายเพื่อกำหนดกรอบภาพที่ชัดเจนของการโจมตีทางไซเบอร์บนกระบวนการการทำงานในโรงงานอุตสาหกรรม และเพื่อนำเสนอบทเรียนที่ได้รับจากเหตุการณ์ในอดีตและเตรียมพร้อมสำหรับเหตุการณ์ที่อาจจะเกิดขึ้นในอนาคต เช่นเดียวกับงานวิจัยของ Morrow, P. J., & Fitzpatrick, T. M. (2020) พบว่ามุมมองทางกฎหมายของสหรัฐอเมริกาและระหว่างประเทศที่มีผลต่อการกำกับดูแลกิจการด้านความปลอดภัยทางไซเบอร์ การศึกษามุ่งเน้นไปในเรื่องของการให้คำแนะนำให้กับผู้บริหารขององค์กรเกี่ยวกับข้อบังคับและกฎหมายที่มีผลต่อการตัดสินใจด้านความปลอดภัยทางไซเบอร์ เพื่อให้สามารถนำมาประยุกต์ใช้กับการบริหารจัดการได้อย่างเหมาะสม

3. ปัจจัยด้านความสำเร็จในการดำเนินงานที่ส่งผลกระทบต่อความปลอดภัยของธุรกิจพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทยด้านเทคโนโลยี โดยภาพรวมพบว่าอยู่ในระดับมาก ทั้งนี้เนื่องจากบริษัทมีมาตรการป้องกันและตรวจสอบภัยคุกคามจากโปรแกรมที่ไม่ประสงค์ บริษัทยังมีระบบหรือกระบวนการในการป้องกันเพื่อลดความเสี่ยงจากการ

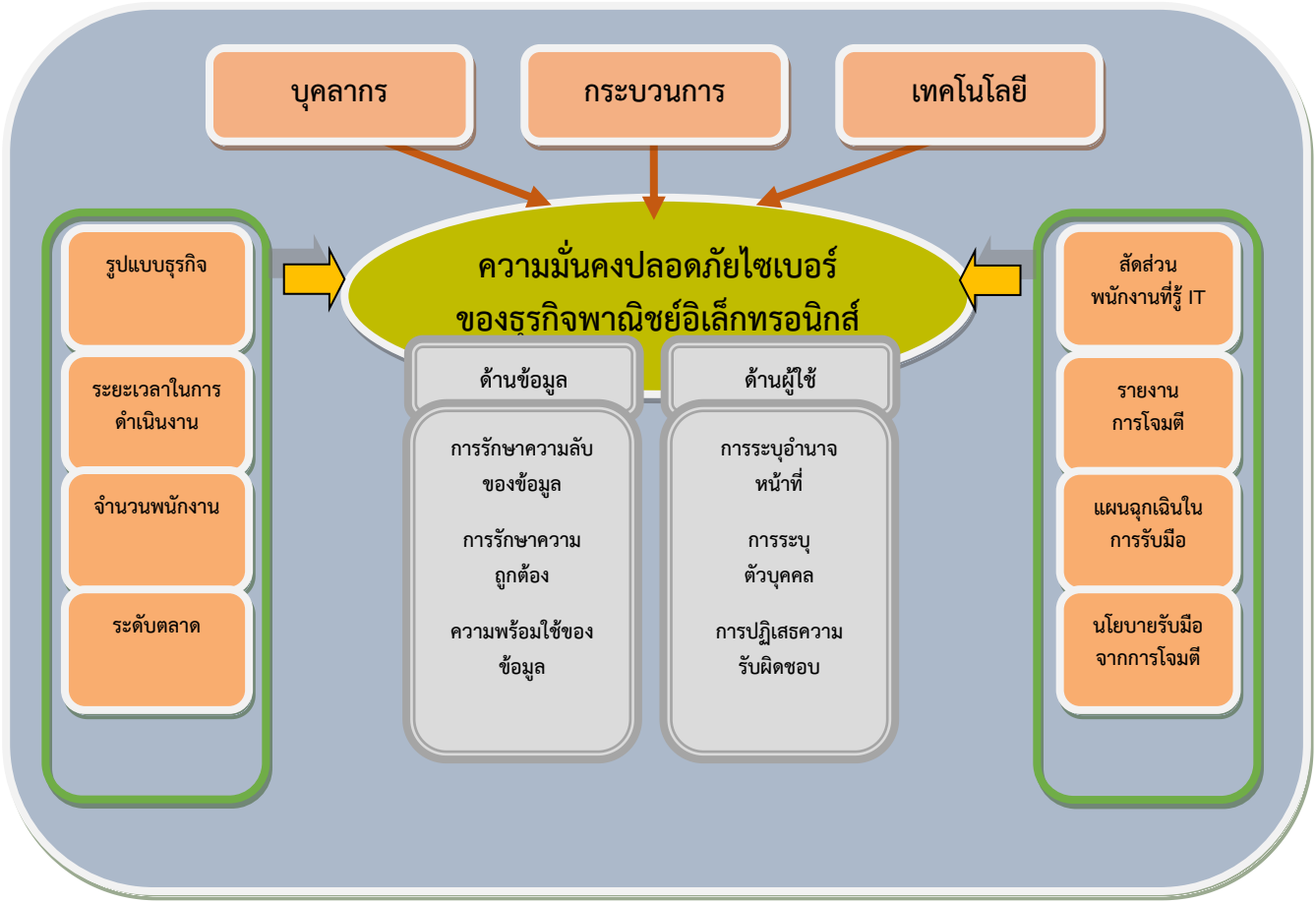
URU-J.ISD 254724
ปีที่ 12 ฉบับที่ 1 มกราคม - มิถุนายน 2565
ISSN 2821-9708 (Online)

ทำเว็ปไซต์เลียนแบบ มีการควบคุมและจำกัดสิทธิการติดตั้งซอฟท์แวร์บนระบบงาน รวมถึงทำการทดสอบการเจาะระบบ กับระบบงานที่มีความสำคัญที่เชื่อมต่อกับ การกำหนดให้ผู้ใช้งานต้องยืนยันตัวบุคคลโดยกำหนดชื่อผู้ใช้และรหัสผ่าน เพื่อเข้าถึงข้อมูลได้ตามสิทธิที่กำหนด และบันทึกการเข้าถึงระบบโดยบัญชีผู้ใช้ทุกประเภทมีการรักษาความถูกต้องปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ สอดคล้องกับงานวิจัยของ Alqahtani, H., & Kavakli-Thorne, M. (2020) พบว่าการยอมรับแอปพลิเคชัน Augmented Reality บนมือถือสำหรับการรับรู้ความปลอดภัยทางไซเบอร์ โดยการยอมรับเทคโนโลยีดังกล่าว เพื่อจะได้นำเอาพฤติกรรมนั้นไปตรวจสอบความสัมพันธ์ระหว่างทัศนคติและความตั้งใจที่จะใช้เทคโนโลยีนี้ได้อย่างดีที่สุด อันส่งจะผลต่อการรับรู้ถึงผลของความมั่นคงปลอดภัยทางไซเบอร์ได้เป็นอย่างดี เช่นเดียวกับงานวิจัยของ Thach, N. N., Hanh, H. T., Huy, D. T. N., & Vu, Q. N. (2021) พบว่าการจัดการคุณภาพเทคโนโลยีของอุตสาหกรรม 4.0 และการจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์ในกิจกรรมการธนาคารในปัจจุบันในตลาดเกิดใหม่ – กรณีในเวียดนาม โดยเฉพาะในอุตสาหกรรมการเงินที่มีการนำเอาเทคโนโลยีต่าง ๆ มาใช้งานเพื่อความสะดวกสบาย ซึ่งทำให้เกิดช่องโหว่เพิ่มมากขึ้น การศึกษามุ่งเน้นไปที่การเพิ่มศักยภาพและประสิทธิภาพในการรับมือจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นเพื่อการจัดการคุณภาพเทคโนโลยีที่ดีขึ้น

4. การศึกษาความปลอดภัยของพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อม ที่ประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ในประเทศไทยโดยภาพรวมอยู่ในระดับมาก ทั้งนี้เนื่องจากการที่วิสาหกิจขนาดกลางและขนาดย่อมมีการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านข้อมูลซึ่งได้แก่ มีการรักษาความลับของข้อมูล มีการรักษาความถูกต้องของข้อมูล และมีความพร้อมใช้ของข้อมูล และมีการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านผู้ใช้ ซึ่งได้แก่ มีการระบุอำนาจหน้าที่ มีการระบุตัวตน และมีการปฏิเสธความรับผิดชอบ สอดคล้องกับงานวิจัยของ Bada, M., & Nurse, J. R. (2019) พบว่าการศึกษาแนวทางในการรับรู้เพื่อสร้างความตระหนักรู้ถึงอันตรายของการโจมตีทางไซเบอร์ที่ส่งผลต่อวิสาหกิจขนาดกลางและขนาดย่อมผ่านการพัฒนาโปรแกรมการศึกษาและการรับรู้ด้านความมั่นคงปลอดภัยในโลกไซเบอร์สำหรับวิสาหกิจขนาดกลางและขนาดย่อม (SMEs) มีการศึกษาเพื่อให้เกิดการรับรู้ในเรื่องการรักษาความลับ ความถูกต้อง และความพร้อมใช้งานของข้อมูล เช่นเดียวกับการศึกษาของ Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021) พบว่า การจำลองแบบไดนามิกเพื่อสนับสนุนการประเมินความเสี่ยงทางไซเบอร์และการลงทุนด้านความปลอดภัยใน SMEs ทำให้เกิดความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับผู้ใช้งาน เป็นการพิจารณานำการมีอำนาจหน้าที่ของผู้ใช้งาน การระบุตัวตน รวมไปถึงการปฏิเสธการรับผิดชอบมาพิจารณาเพื่อสร้างเป็นแบบจำลองในการศึกษา

URU-J.ISD 254724
ปีที่ 12 ฉบับที่ 1 มกราคม - มิถุนายน 2565
ISSN 2821-9708 (Online)

องค์ความรู้จากการวิจัย



องค์ความรู้จากการศึกษาเรื่องความมั่นคงปลอดภัยไซเบอร์ของธุรกิจพาณิชย์อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อม สามารถสรุปได้ดังต่อไปนี้

จากผลการศึกษาพบว่า ความมั่นคงปลอดภัยไซเบอร์ของธุรกิจพาณิชย์อิเล็กทรอนิกส์สำหรับวิสาหกิจขนาดกลางและขนาดย่อมประกอบด้วยความปลอดภัยใน 2 ส่วนคือความปลอดภัยด้านข้อมูล โดยมีองค์ประกอบด้านการรักษาความลับของข้อมูล การรักษาความถูกต้อง และความพร้อมใช้ของข้อมูล ความปลอดภัยด้านผู้ใช้ โดยมีองค์ประกอบด้านการระบุอำนาจหน้าที่ การระบุตัวตน และการปฏิเสธความรับผิดชอบ โดยที่ธุรกิจพาณิชย์อิเล็กทรอนิกส์ต้องมีปัจจัยด้านความสำเร็จของธุรกิจที่ประกอบด้วย ด้านบุคลากร ด้านกระบวนการ และด้านเทคโนโลยีเป็นตัวผลักดันให้ธุรกิจมีความปลอดภัยจากการดำเนินธุรกิจในปัจจุบัน

จากองค์ความรู้ที่ได้ดังกล่าวนี้ ทางผู้วิจัยจะได้นำเอาองค์ความรู้ดังกล่าวไปต่อยอดการทำวิจัยเพื่อพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมให้มีความเป็นองค์กรดิจิทัล เพื่อรองรับ (ร่าง) แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 13 ตามแผนกลยุทธ์รายหมุดหมาย หมุดหมายที่ 7 ในประเด็น “ไทยมีวิสาหกิจขนาดกลางและขนาดย่อมที่เข้มแข็ง มีศักยภาพสูง และสามารถแข่งขันได้” ตามกลยุทธ์

URU-J.ISD 254724
ปีที่ 12 ฉบับที่ 1 มกราคม - มิถุนายน 2565
ISSN 2821-9708 (Online)

การพัฒนาในกลยุทธ์ที่ 2 การพัฒนาแพลตฟอร์มเชื่อมโยงฐานข้อมูลวิสาหกิจขนาดกลางและขนาดย่อมและส่งเสริมให้วิสาหกิจขนาดกลางและขนาดย่อมเข้าสู่ระบบ โดยมีแผนกลยุทธ์จัดให้มีระบบไอดีเดียวของวิสาหกิจขนาดกลางและขนาดย่อมและส่งเสริมให้ วิสาหกิจขนาดกลางและขนาดย่อมใช้ในการทำธุรกรรมผ่านระบบดิจิทัล พัฒนาพอร์ทัลกลางเชื่อมโยงข้อมูลของวิสาหกิจขนาดกลางและขนาดย่อมเข้ากับระบบการให้บริการภาครัฐ และพัฒนาระบบคลังข้อมูลและความรู้สำหรับให้บริการวิสาหกิจขนาดกลางและขนาดย่อมให้เป็นระบบออนไลน์และระบบบริการอิเล็กทรอนิกส์ครบวงจร โดยผู้วิจัยได้มีโอกาสได้ทำงานวิจัยร่วมกับสมาคมอุตสาหกรรมซอฟต์แวร์ไทย (ATSI) ศึกษาเพื่อเตรียมความพร้อมให้กับวิสาหกิจขนาดกลางและขนาดย่อม โดยเฉพาะธุรกิจพาณิชย์อิเล็กทรอนิกส์ที่ปฏิเสธไม่ได้ว่าต้องเผชิญต่อความเสี่ยงทางด้านไซเบอร์ ซึ่งความมั่นคงปลอดภัยไซเบอร์เป็นเรื่องที่ต้องตระหนักถึงเป็นลำดับต้น ๆ ต่อการดำเนินธุรกิจนั้น

ข้อเสนอแนะ

ข้อเสนอแนะทั่วไป

1. ปัจจัยที่มีผลต่อการโจมตีทางไซเบอร์ต่อระบบพาณิชย์อิเล็กทรอนิกส์ ด้านบุคลากร ที่มีต่อระบบพาณิชย์อิเล็กทรอนิกส์ นั้นบริษัทควรจะให้ความรู้เกี่ยวกับพนักงานของตนในความเท่าทันที่เกี่ยวกับเนื้อหาที่พบในโลกออนไลน์ว่า ไม่สามารถเชื่อถือได้ทั้งหมด ต้องให้พนักงานรู้จักวิธีการตรวจสอบความน่าเชื่อถือของเว็ปไซต์ ควรจะให้พักงานของบริษัทจัดเก็บข้อมูลไว้อย่างเป็นระบบ มีเข้าใจในประเด็นเรื่องจริยธรรมและกฎหมายที่เกี่ยวข้องกับการเข้าถึงและการใช้ข้อมูล รวมถึงต้องมีการเข้าใจถึงแนวคิดและการทำงานพื้นฐานของเครื่องมือดิจิทัล ประกอบกับการเปลี่ยนแปลงของเทคโนโลยีเพื่อจะได้สามารถไม่ตกเป็นเหยื่อของการโจมตีได้

2. ปัจจัยที่มีผลต่อการโจมตีทางไซเบอร์ต่อระบบพาณิชย์อิเล็กทรอนิกส์ ด้านกระบวนการ บริษัทควรมีการกำกับดูแลกิจกรรมและวัฒนธรรมองค์กร ในการควบคุม และติดตามการบริหารจัดการความเสี่ยงขององค์กร รวมไปถึงการที่ให้ผู้บริหารระดับสูงได้ตระหนักถึงความเสี่ยง และสร้างวัฒนธรรมการบริหารความเสี่ยงให้เกิดขึ้น โดยกำหนดให้มีกลยุทธ์ วัตถุประสงค์ ที่สามารถจัดการต่อความเสี่ยงทางไซเบอร์ มีแผนระยะสั้น กลาง และยาวในการรับมือต่อความเสี่ยง มีเป้าหมายที่ชัดเจน มีการทบทวนและปรับปรุงขั้นตอนในการรับมือต่อความเสี่ยง รวมถึงการจัดการด้านสารสนเทศให้มีการรายงานผลต่อทั้งผู้บริหาร ผู้มีส่วนได้ส่วนเสียต่อบริษัททั้งภายในและภายนอก

3. ปัจจัยที่มีผลต่อการโจมตีทางไซเบอร์ต่อระบบพาณิชย์อิเล็กทรอนิกส์ ด้านเทคโนโลยี บริษัทต้องมีการรักษาความถูกต้องปลอดภัยเกี่ยวกับเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับบริษัท โดยเฉพาะการรับ-ส่งข้อมูลสารสนเทศ ทั้งภายในและภายนอก มีการป้องกันข้อมูลที่เป็นความลับหรือที่มีความสำคัญในการส่งต่อข้อมูลในรูปของไฟล์แนบและการส่งต่อจดหมายอิเล็กทรอนิกส์ โดยอาจจะมีการให้มีการเข้ารหัสข้อมูล และต้องมีมาตรการในการป้องกันการโจมตีจากโปรแกรมที่ไม่ประสงค์ดี (Malware) ควบคุมการติดตั้งซอฟต์แวร์ในระบบงาน มีการจำกัดสิทธิ์ในการเข้าถึงข้อมูลต่อผู้รับผิดชอบ และกำหนดรหัสผู้ใช้ (Username) และรหัสผ่าน (Password) ในการเข้าทำงานและต้องให้สามารถเปลี่ยน ข้อมูลดังกล่าวได้อยู่เสมอ

ข้อเสนอแนะในการทำวิจัยครั้งต่อไป

1. ศึกษาโมเดลเชิงโครงสร้างระหว่างปัจจัยที่มีอิทธิพลต่อความปลอดภัยของระบบพาณิชย์อิเล็กทรอนิกส์

2. พัฒนาตัวแบบความความปลอดภัยของระบบพาณิชย์อิเล็กทรอนิกส์สำหรับภาคธุรกิจต่างๆ ให้เฉพาะเจาะจงเป็นกรณี ๆ ไป

เอกสารอ้างอิง

Alqahtani, H., & Kavakli-Thorne, M. (2020), February). Factors affecting acceptance of a mobile augmented reality application for cybersecurity awareness. In *Proceedings of the 2020 4th International Conference on Virtual and Augmented Reality Simulations* (pp. 18-26).

Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, *147*, 113580.

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmed for small-and medium-sized enterprises (SMEs). *Information & Computer Security*.

Belsley,D. (1991). *Conditional diagnostics: collinearity and weak data in regression.* Wiley Series in Probability.Jonh Wiley, New York

Cisco. (2021). *Cybersecurity for SMBs: Asia Pacific Businesses Prepare for Digital Defense.* Retrieved 2021, Oct 15, from https://www.cisco.com/c/en_sg/ products/security/cyber-security-for-smbs-in-asia-pacific/index.html

Donthu, N., & Gustafsson, A. (2020). Effects of COVID-19 on business and research. Journal *of business research, 117*, 284-289.

Electronic Transactions Development Agency (Public Organization). (2018). *Value of E-Commerce Survey in Thailand 2018.* The Electronic Transactions Development Agency (ETDA), the Ministry of Information and Communication Technology.

Foxall, G.R., & Yani-de-Soriano, M.M. (2005). Situational influences on consumers, attitudes and behavior. *Journal of Business research*, 58, 518-525.

Hartung, Joachim. (2001). Testing for Homogeneity in Combining of two-armed trials with normally distributed responses. *The Indian Journal of Statistics.* Sankhya. 63, 293-310.

He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., & Tian, X. (2019). Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *Journal of Intellectual Capital*.

Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering, 45*(4), 3171-3189.

URU-J.ISD 254724
ปีที่ 12 ฉบับที่ 1 มกราคม - มิถุนายน 2565
ISSN 2821-9708 (Online)

Iaiani, M., Tugnoli, A., Bonvicini, S., & Cozzani, V. (2021). Analysis of cybersecurity-related incidents in the process industry. *Reliability Engineering & System Safety*, *209*, 107485.

Jordan, M. (2020). Cybersecurity awareness. *American Nurse Today*, *15*(2), 5.

Keppel, Geoffrey. (1982). *Design and Analysis A Researcher's Handbook.* New Jersey : Prentice-Hall Inc.

Likert, R. A. (1932). Technique for the Measurement of Attitudes. *Arch Psychological, 25*(140), 1–55.

Microsoft. (2021). *Microsoft Digital Defense Report (October 2021).* Retrieved 2022, June 08, from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi

Morrow, P. J., & Fitzpatrick, T. M. (2020). US and International Legal Perspectives Affecting Cybersecurity Corporate Governance. *International Relations, 8*(06), 231-239.

NTT. (2021). 2021. *Global Threat Intelligence Report, Accelerating your cybersecurity: intelligence-driven and secure by design.* Retrieved 2021, Oct 15, from https://services.global.ntt/enus/insights/ 2021-global-threat-intelligence-report.

Puat, H. A. M., & Abd Rahman, N. A.(2020). Ransomware as a service and public awareness. *PalArch's Journal of Archaeology of Egypt/Egyptology*, *17*(7), 5277-5292.

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

Thach, N. N., Hanh, H. T., Huy, D. T. N., & Vu, Q. N. (2021). Technology Quality Management of the industry 4.0 and Cybersecurity Risk Management on Current Banking Activities in Emerging Markets-the Case in Vietnam. *International Journal for Quality Research*, *15*(3), 845.

Wanichbuncha Kalaya. (2011). *Statistic for research.* Bangkok. Thamsarn Press.)

Wongrattana Choosri. (2007). *Techniques for Appling Statistics to Research.* Nonthaburi: Taineramitkij Inter.

World Economic Forum. (2021). *The Global Risks Report 2021 16th Edition.* Retrieved 2021, Oct 15, from https://www3.weforum.org/docs/WEF_The_ Global_Risks_Report_2021.pdf.

กัลยา วานิชย์บัญชา. (2545). *หลักสถิติ*. (พิมพ์ครั้งที่ 7*)*. กรุงเทพฯ: โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

ลัดดาวัลย์ เพชรโรจน์ และอัจรา ชำนิประศาสน์. (2547). *ระเบียบวิธีการวิจัย (Research methodology).* กรุงเทพฯ : พิมพ์ดีการพิมพ์.

ศิริชัย กาญจนวาสี. (2544). *การเลือกใชสถิติที่เหมาะสมสำหรับการวิจัย.* (พิมพครั้งที่ 4). กรุงเทพฯ: บุญศิริการพิมพ์.