ปัจจัยที่กำหนดพฤติกรรมในการติดตั้งการควบคุมในระบบการบริหารทรัพยากรองค์กรสำหรับธุรกิจขนาดกลางและขนาดย่อม

โกญจนาท สันทัดการ*

คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์

***Correspondence:** suntudgarn@gmail.com
doi: 10.14456/jisb.2022.11

วันที่รับบทความ: 20 มิ.ย. 2565 วันแก้ไขบทความ: 6 ก.ค. 2565 วันตอบรับบทความ: 20 ก.ค. 2565

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาปัจจัยที่กำหนดพฤติกรรมในการติดตั้งการควบคุมในระบบการบริหารทรัพยากรขององค์กร สำหรับธุรกิจขนาดกลางและขนาดย่อม ซึ่งเป็นงานวิจัยเชิงปริมาณ และประยุกต์ใช้ทฤษฎีแรงจูงใจในการป้องกัน และแนวคิดเกี่ยวกับความตระหนัก โดยทำการศึกษากลุ่มตัวอย่างจากผู้ประกอบการ หรือพนักงานผู้ที่เกี่ยวข้องกับระบบการบริหารทรัพยากรองค์กรในธุรกิจขนาดกลางและขนาดย่อมที่นำระบบการบริหารทรัพยากรองค์กรมาใช้งาน จำนวน 162 ตัวอย่าง ด้วยการแจกแบบสอบถามในรูปอิเล็กทรอนิกส์ แล้วนำข้อมูลที่ได้มาประมวลผลด้วยโปรแกรมสำเร็จรูปทางสถิติ เพื่อวิเคราะห์ความสัมพันธ์ของปัจจัยต่าง ๆ ในกรอบแนวคิดในการวิจัยที่กล่าวมาข้างต้น ทั้งนี้ผู้วิจัยได้ทำการตรวจสอบความเที่ยงตรงของเครื่องมือ และทดสอบสมมติฐานตามกรอบแนวคิดในการวิจัยด้วยการวิเคราะห์การถดถอยแบบเชิงชั้น จากผลการศึกษาพบว่า ปัจจัยด้านความคาดหวังในประสิทธิภาพของการตอบสนอง ปัจจัยด้านการรับรู้ถึงความรุนแรง ปัจจัยด้านความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ มีอิทธิพลส่งผลต่อความตั้งใจในการรับมือกับภัยคุกคาม ส่วนปัจจัยด้านการรับรู้จุดอ่อน ปัจจัยด้านความคาดหวังในประสิทธิภาพของตนเอง และปัจจัยด้านค่าใช้จ่ายการตอบสนอง ไม่มีอิทธิพลต่อความตั้งใจในการรับมือกับภัยคุกคาม สำหรับปัจจัยด้านความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ ปัจจัยด้านการรับรู้จุดอ่อน มีอิทธิพลส่งผลต่อความตระหนักถึงความปลอดภัย และ ปัจจัยด้านความตั้งใจในการรับมือกับภัยคุกคาม ปัจจัยด้านความตระหนักถึงความปลอดภัย มีอิทธิพลส่งผลต่อการรับมือภัยคุกคามด้วยการติดตั้งการควบคุมมากที่สุด

คำสำคัญ: ระบบการบริหารทรัพยากรองค์กร; ธุรกิจขนาดกลางและขนาดย่อม; ภัยคุกคามต่อระบบสารสนเทศ; การติดตั้งการควบคุม

Factors Determining Behavior in Control Installation in Enterprise Resource Planning System A Case Studies of Small and Medium Enterprises

Gonchanat Santadgarn*

Thammasat Business School, Thammasat University

***Correspondence:** suntudgarn@gmail.com

doi: 10.14456/jisb.2022.11

Received: 20 Jun 2022 Revised: 6 Jul 2022 Accepted: 20 Jul 2022

Abstract

The objective of this study is to examine factors that determine control installation in ERP system (Enterprise resource planning) in small and medium enterprises (SMEs). This research is quantitative research that applied Protection motivation theory and awareness. Data for this research was collected from 162 Thai participants, entrepreneur and employees who have responsibility in ERP system in SMEs. Data was gathered by online questionnaires and analyzed by statistical software to determine the relationships of factors. This study tested the hypotheses using Hierarchical Regression. The results indicate that Perceived Severity, Response-Efficacy, and Knowledge affect Intention but Perceived Vulnerability, Self-Efficacy, and Response Cost are not affected Intention. Meanwhile, Perceived Vulnerability and Knowledge affect Awareness. Finally, Intention and Awareness affect Behavior.

Keywords: Enterprise resource planning (ERP); Small and medium enterprises (SMEs); Cyber attack; Control installation

1. บทนำ

1.1 ความสำคัญและที่มาของปัญหา

ปัจจุบันเทคโนโลยีสารสนเทศและระบบเครือข่ายได้เข้ามามีบทบาทสำคัญต่อชีวิตประจำวันอย่างมากรวมไปถึงองค์กรธุรกิจที่ได้นำเทคโนโลยีสารสนเทศเข้ามาช่วยในการทำงานเพื่อให้การดำเนินธุรกิจมีการพัฒนาตามเทคโนโลยีที่เปลี่ยนแปลงไป และยังสามารถสร้างความได้เปรียบในการแข่งขันกับธุรกิจอื่นได้ ไม่ว่าจะเป็นธุรกิจขนาดกลางหรือขนาดย่อม ที่ในหลายๆ องค์กรได้นำระบบระบบการบริหารทรัพยากรขององค์กร (Enterprise resource planning หรือ ERP) เข้ามาช่วยในการทำงาน โดยระบบ ERP คือ ระบบสารสนเทศประเภทหนึ่งที่ใช้เพื่อทำให้กิจกรรมแต่ละรายการในธุรกิจหรือองค์กรเป็นแบบอัตโนมัติและเรียบง่าย เช่น การบัญชีและการจัดซื้อ การจัดการโครงการ การจัดการลูกค้าสัมพันธ์ การจัดการความเสี่ยง การปฏิบัติตามข้อกำหนด และการดำเนินงานในห่วงโซ่อุปทาน โดยวัตถุประสงค์หลักของระบบ ERP คือการเพิ่มประสิทธิภาพองค์กรด้วยการจัดการและปรับปรุงวิธีการใช้ทรัพยากรของกิจการ เพื่อเพิ่มประสิทธิภาพในการทำงานซึ่งเป็นกุญแจสำคัญในการเติบโตของธุรกิจ โดยทั่วไปประเภทของระบบ ERP แบ่งออกได้ 3 ประเภท ได้แก่ On-premise ERP, Cloud ERP และ Hybrid ERP (คิวเอดี, ม.ป.ป.) ดังนี้

On-premise ERP เป็นระบบ ERP ที่ต้องใช้งานภายในองค์กรผ่านระบบเครือข่ายภายในองค์กร และจำเป็นต้องมีการบำรุงรักษาในพื้นที่ ฮาร์ดแวร์ ซอฟต์แวร์ และระบบเครือข่าย โดยองค์กรเป็นเจ้าของระบบทั้งหมดซึ่งสามารถปรับแต่งตัวระบบ ERP ได้ตามความต้องการและบริบทขององค์กร

Cloud ERP เป็นระบบ ERP บนคลาวด์เป็นการให้บริการบนเว็บที่เรียกว่า Software as a Service (SaaS) ซึ่งองค์กรเข้าถึงและจัดเก็บข้อมูลบนอุปกรณ์ใดๆ ที่มีการเชื่อมต่ออินเทอร์เน็ต โดยปกติแล้วจะผ่านการสมัครเป็นสมาชิกโดยการอัปเดต และการปรับแต่งระบบจะได้รับการสนับสนุนจากผู้ให้บริการซอฟต์แวร์

Hybrid ERP เป็นระบบ ERP ที่มีลักษณะเป็น “ไฮบริด” กล่าวคือการใช้งานระบบ ERP จะเป็นแบบคลาวด์และแบบภายในองค์กรร่วมกัน การใช้งานระบบ ERP ลักษณะนี้ จะแตกต่างกันไปตามผู้ให้บริการ

จากการสำรวจธุรกิจขนาดกลางและขนาดย่อมในเขตกรุงเทพมหานคร โดยกลุ่มตัวอย่างเป็นผู้บริหาร/เจ้าของกิจการหรือผู้ปฏิบัติงานที่เกี่ยวข้องกับการใช้งานระบบ ERP สำหรับธุรกิจ SMEs เขตกรุงเทพมหานคร จำนวน 450 แห่ง ปี 2560 พบว่าองค์กรโดยส่วนใหญ่ใช้ระบบ ERP ประเภท On-premise ERP (ณชญาภัส รอดประยูร, 2560) ซึ่งพัฒนาระบบขึ้นเพื่อให้มีความเหมาะสมกับบริบทขององค์นั้นๆ ผ่านระบบเครื่องข่ายคอมพิวเตอร์ในรูปแบบ Client/Sever

แต่ธุรกิจขนาดกลางและขนาดย่อมส่วนใหญ่ยังขาดความรู้ความเข้าใจเกี่ยวกับการควบคุม (Control) ซึ่งเป็นวิธีการป้องกันหรือลดจุดอ่อนจากการปฏิบัติงานด้านต่างๆ เพื่อให้มีความมั่นคงปลอดภัย ซึ่งจะช่วยป้องกันทรัพย์สินสารสนเทศจากการเข้าถึง การเปิดเผย การขัดขวาง การเปลี่ยนแปลงแก้ไข การสูญหาย ถูกทำลาย หรือล่วงรู้โดยมิชอบ (Romney et al., 2012) สำหรับการควบคุมของระบบสารสนเทศเบื้องต้น ประกอบด้วย การพิสูจน์ตัวจริง (Authentication) การควบคุมการเข้าถึง (Access control) และการตรวจสอบ (Auditing) ดังนี้ (นิตยา วงศ์ภินันท์วัฒนา, 2563)

การพิสูจน์ตัวจริง (Authentication) เป็นวิธีการที่ใช้ในการตรวจสอบผู้ที่มาใช้งานระบบสารสนเทศ อาทิ การใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) การใช้โทเค็น (Token) และใบรับรองอิเล็กทรอนิกส์หรือใบรับรองดิจิทัล (Digital certificates) หรือการใช้ชีววิทยาหรือลักษณะทางกายภาพของบุคคล (Biometrics) เป็นต้น

การควบคุมการเข้าถึง (Access control) คือ กระบวนการจำกัดการใช้ทรัพยากรทางคอมพิวเตอร์โดยพิจารณาจากลักษณะของผู้ใช้และการเป็นสมาชิกของกลุ่มหรือบางครั้งเรียกว่า การกำหนดอำนาจ (Authorization)

การตรวจสอบ (Auditing) การค้นหาหลักฐานเพื่อให้แน่ใจว่ามีการติดตั้งการควบคุมระบบสารสนเทศและปฏิบัติตามอย่างเหมาะสม

จากข้อมูลสถิติของ สำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม (สสว.) (ม.ป.ป.) พบว่าผู้ประกอบการ SMEs ทั่วประเทศมีจำนวนถึง 3,176,055 ราย มีมูลค่า 1,505,349 ล้านบาท คิดเป็นร้อยละ 35 หรือเป็น 1 ใน 3 ของ GDP มวลรวมของประเทศ โดยมีการจ้างงานรวม 12,803,092 บาท SMEs มีบทบาทสำคัญในการขับเคลื่อนเศรษฐกิจของประเทศ และจากการสัมภาษณ์ SMEs ในยุโรป โดย ENISA (European Union Agency for Cybersecurity) ในช่วงการระบาดใหญ่ของโควิด-19 เหตุการณ์ทางไซเบอร์ที่พบบ่อยที่สุดคือการโจมตีด้วยแรนซัมแวร์ แล็ปท็อปถูกขโมย การโจมตีแบบฟิชชิ่ง และการฉ้อโกงของ CEO จากการสำรวจของ ENISA ในกลุ่ม SMEs ร้อยละ 90 ระบุว่าปัญหาด้านความปลอดภัยทางไซเบอร์จะส่งผลกระทบอย่างร้ายแรงต่อธุรกิจของพวกเขาภายในหนึ่งสัปดาห์หลังจากเกิดปัญหา โดยร้อยละ 57 ระบุว่ามีแนวโน้มว่าจะล้มละลายหรือเลิกกิจการ (ENISA, 2020)

ผลการศึกษาล่าสุดของซิสโก้ (Cisco) ชี้ว่า ธุรกิจขนาดกลางและขนาดเล็ก หรือ SMEs ในไทยกำลังเผชิญกับความเสี่ยงหรือถูกโจมตีทางไซเบอร์ และมีความกังวลเกี่ยวกับภัยคุกคามด้านไซเบอร์ซีเคียวริตี้ (Cyber security) มากขึ้นอย่างที่ไม่เคยมีมาก่อน โดยร้อยละ 65 ของ SMEs ในไทยถูกโจมตีทางไซเบอร์ในปีที่ผ่านมา และร้อยละ 76 สูญเสียข้อมูลลูกค้าหลังถูกโจมตีทางไซเบอร์ ร้อยละ 47 ของ SMEs ที่ถูกโจมตีทางไซเบอร์ได้รับความเสียหายทางธุรกิจกว่า 500,000 ดอลลาร์สหรัฐ (ประมาณ 16 ล้านบาท) หรือมากกว่านั้นซึ่งการโจมตีด้วยมัลแวร์ ครองอันดับหนึ่งในไทยส่งผลกระทบต่อ SMEs ร้อยละ 91 ตามด้วยฟิชชิ่ง (Phishing) ร้อยละ 77 ในปี 2564

โดย SMEs ในไทยเกือบครึ่งหนึ่งร้อยละ 49 ที่ถูกโจมตีพบว่าสาเหตุสำคัญที่สุดที่ทำให้องค์กรถูกโจมตีเป็นเพราะว่าโซลูชั่นด้านไซเบอร์ซีเคียวริตี้ไม่มีประสิทธิภาพเพียงพอที่จะตรวจจับ หรือป้องกันการโจมตี ขณะที่ร้อยละ 25 ระบุว่าองค์กรไม่ได้ติดตั้งโซลูชั่นด้านไซเบอร์ซีเคียวริตี้ และไม่ได้ให้ความสำคัญเป็นอันดับแรก ๆ โดยสูญเสียข้อมูลลูกค้าคิดเป็นร้อยละ 76 สูญเสียข้อมูลของพนักงาน ร้อยละ 69 อีเมลภายในองค์กร ร้อยละ 65 ข้อมูลด้านการเงิน ร้อยละ 57 ซึ่งอาจส่งผลให้ธุรกิจประสบปัญหาการดำเนินงานหยุดชะงักอันเนื่องมาจากการโจมตีทางไซเบอร์ (ดิจิทเดย์, 2564) งานวิจัยนี้จึงต้องการศึกษาว่าหน่วยงานที่ติดตั้งระบบ ERP มีมาตรการป้องกัน หรือเครื่องมือที่ช่วยป้องกันไม่ให้ผู้อื่นสามารถเข้าถึงข้อมูลภายในระบบ ERP ได้ รวมไปถึงการมีมาตรการในการรับมือและโต้ตอบกับความเสี่ยงที่อาจจะเกิดขึ้น โดยเน้นระบบ ERP สำหรับธุรกิจขนาดกลางและขนาดย่อมเป็นหลัก

1.2 วัตถุประสงค์ในการวิจัย

เพื่อศึกษาปัจจัยที่กำหนดพฤติกรรมในการติดตั้งการควบคุมในระบบ ERP สำหรับธุรกิจขนาดกลางและขนาดย่อม ดังนี้

(1) ความรู้ความเข้าใจถึงความปลอดภัย การรับรู้ถึงจุดอ่อน การรับรู้ถึงความรุนแรง ความคาดหวังในประสิทธิผลของการตอบสนอง ความคาดหวังในประสิทธิผลของตนเอง ค่าใช้จ่ายในการตอบสนอง ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ ส่งผลต่อความตั้งใจในการรับมือกับภัยคุกคาม

(2) ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ การรับรู้จุดอ่อน ส่งผลต่อความตระหนักถึงความปลอดภัย

(3) ความตระหนักถึงความปลอดภัย และความตั้งใจในการรับมือกับภัยคุกคาม ส่งผลต่อ การรับมือภัยคุกคามด้วยการติดตั้งการควบคุมบนระบบ ERP

2. วรรณกรรมและงานวิจัยที่เกี่ยวข้อง

จากการศึกษาทฤษฎีแรงจูงใจในการป้องกัน (Protection motivation theory) ได้แก่ การรับรู้ถึงจุดอ่อน การรับรู้ถึงความรุนแรง ความคาดหวังในประสิทธิผลของการตอบสนอง การรับรู้ความสามารถของตนเอง ค่าใช้จ่ายการตอบสนอง แรงจูงใจในการป้องกัน พฤติกรรมในการป้องกัน นอกจากนี้ได้ศึกษาแนวคิดเกี่ยวกับความตระหนัก (Awareness) ได้แก่ ความรู้ความเข้าใจ ความตระหนัก และงานวิจัยในอดีตที่เกี่ยวข้องสามารถสรุปปัจจัยที่เกี่ยวข้องกับการศึกษาได้ดังนี้

การรับรู้ถึงจุดอ่อน (Perceived vulnerability) คือ การรับรู้ถึงข้อบกพร่อง หรือช่องโหว่ของระบบสารสนเทศที่ได้จากการประเมินความน่าจะเป็นในการถูกคุกคามจากภัยคุกคาม (Yoon et al., 2012) ซึ่งในงานวิจัยนี้หมายถึง การที่ผู้ประกอบการ SMEs ที่ใช้งานระบบ ERP ทราบว่าระบบ ERP มีช่องโหว่ที่อาจเป็นอันตรายต่อข้อมูลในระบบ โดยระบบ ERP ไม่สามารถรับมือกับผลที่เกิดขึ้นได้ด้วยตัวเองดังนั้นจึงเกิดช่องโหว่ที่นำมาซึ่งความสูญหายและถูกโจรกรรมข้อมูลบนระบบ ERP

การรับรู้ถึงความรุนแรง (Perceived severity) คือ การรับรู้ถึงผลกระทบและระดับความอันตรายของภัยคุกคามที่ส่งผลต่อความเสียหายของข้อมูล (Lee & Larsen, 2009) ในงานวิจัยนี้หมายถึงการที่ผู้ประกอบการ SMEs ที่ใช้งานระบบ ERP เชื่อว่าระดับความเสียหายของข้อมูลบนระบบ ERP ขึ้นอยู่กับระดับความรุนแรง ซึ่งมีความสำคัญอย่างยิ่งต่อระดับความถูกต้องของข้อมูล โดยบุคคลดังกล่าวจะเป็นผู้กำหนดขอบเขตในการรับรู้ถึงระดับความรุนแรงเพื่อยับยั้งความเสียหายที่อาจเกิดขึ้น

ความคาดหวังในประสิทธิผลของการตอบสนอง (Response efficacy) คือ ระดับการรับรู้ถึงการรักษาความปลอดภัย มาตรการ วิธีการหลีกเลี่ยงภัยคุกคามได้อย่างมีประสิทธิภาพ โดยผู้ใช้มีความเชื่อว่าหากได้ปฏิบัติตามมาตรการที่วางไว้ ผลลัพธ์ที่เกิดขึ้นจะช่วยปกป้องความเป็นส่วนตัวจากภัยคุกคามได้อย่างมาก (Bandura, 1982) ในงานวิจัยนี้หมายถึงการที่ผู้ประกอบการ SMEs ที่ใช้งานระบบ ERP เชื่อว่าหากได้ปฏิบัติตามมาตรการที่วางไว้จะสามารถช่วยปกป้องหรือลดทอนความเสียหายที่เกิดจากภัยคุกคามได้อย่างมาก

การรับรู้ความสามารถของตนเอง (Self-efficacy) คือ การที่บุคคลตัดสินใจภายใต้ความสามารถของตนเองที่จะจัดการและดำเนินการให้บรรลุเป้าหมายที่กำหนดไว้ (Bandura, 1982) ในงานวิจัยนี้หมายถึงการที่การที่ผู้ประกอบการ SMEs ที่ใช้งานระบบ ERP เชื่อว่าตนมีความสามารถในการจัดการกับภัยคุกคามที่เกิดขึ้นด้วยตนเองได้

ค่าใช้จ่ายการตอบสนอง (Response cost) คือ สิ่งที่บุคคลรับรู้ในการดำเนินกิจกรรมในการป้องกันและแก้ไขปัญหาที่เกิดขึ้น เช่น ความไม่สะดวก ความยาก และผลข้างเคียงของการปฏิบัติงาน รวมไปถึงค่าใช้จ่ายที่เป็นตัวเงินและเวลา เป็นต้น (Yoon et al., 2012) ในงานวิจัยนี้หมายถึงการที่ผู้ประกอบการ SMEs ที่ใช้งานระบบ ERP เชื่อว่าค่าใช้จ่ายในการตอบสนอง ได้แก่ ความยุ่งยากในการใช้งานการควบคุม และค่าใช้จ่ายในการติดตั้งการควบคุม ถือเป็นปัจจัยสำคัญต่อการป้องกันภัยคุกคาม ที่อาจส่งผลกระทบทางอ้อมต่อความปลอดภัยของข้อมูลภายในระบบ ERP

ความตั้งใจในการรับมือกับภัยคุกคาม (Behavior intention) คือ การแสดงออกถึงความกระตือรือร้น ความมุ่งมั่น ในการทำสิ่งใดสิ่งหนึ่ง (สำนักงานราชบัณฑิตยสภา, ม.ป.ป.) ดังนั้นเมื่อนำมาใช้กับการศึกษาในครั้งนี้ จึงหมายถึงการที่ผู้ประกอบการ SMEs ที่ใช้งานระบบ ERP แสดงออกถึงความตั้งใจ มุ่งมั่น ในการรับมือกับภัยคุกคามระบบ ERP ได้อย่างเหมาะสม

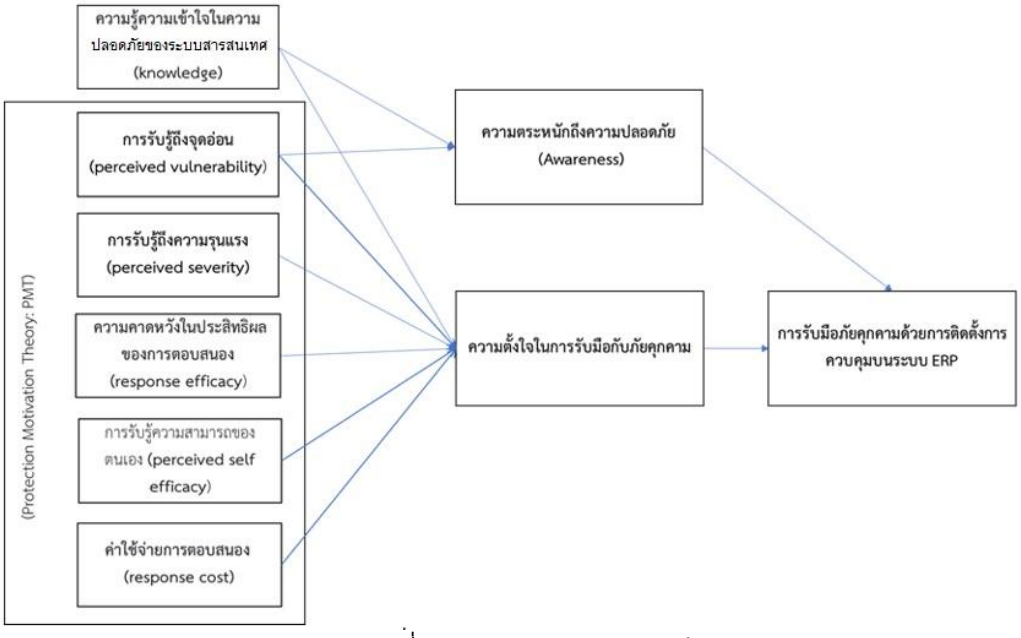
ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ (Knowledge) คือ สิ่งที่สั่งสมมาจากการศึกษาเล่าเรียน การค้นคว้า หรือประสบการณ์ รวมทั้งความสามารถเชิงทักษะและการปฏิบัติ หรือความเข้าใจ หรือสารสนเทศที่ได้รับมาจากประสบการณ์ หรือสิ่งที่ได้รับจากการได้ยิน การฟัง การคิด การปฏิบัติ (สำนักงานราชบัณฑิตยสภา, ม.ป.ป.) ดังนั้นเมื่อนำมาใช้กับการศึกษาในครั้งนี้ จึงหมายถึงการที่ผู้ประกอบการ SMEs ที่ใช้งานระบบ ERP มีความรู้ความเข้าใจในระบบความปลอดภัยของระบบสารสนเทศ ที่เกิดจากการศึกษาเล่าเรียน การค้นคว้า หรือประสบการณ์ รวมทั้งความสามารถเชิงทักษะและการปฏิบัติ หรือความเข้าใจ

ความตระหนัก (Awareness) คือ กระบวนการเกิดสภาวะการคำนึงถึง ซึ่งเกิดจากการที่บุคคลได้รับการกระตุ้นจากสิ่งเร้าในสภาพแวดล้อมแล้วเกิดการรับรู้ แล้วนำไปสู่การเรียนรู้ และความตระหนักตามลำดับ ซึ่งการเรียนรู้และเกิดความตระหนักจะนำไปสู่ความพร้อมที่จะแสดงการกระทำหรือแสดงพฤติกรรมต่อไป (Good & Merkel, 1973) ซึ่งในงานวิจัยนี้หมายถึง การที่ผู้ประกอบการ SMEs ที่ใช้งานระบบ ERP แสดงออกถึงความรู้สึกนึกคิดเมื่อเกิดภัยคุกคามที่ส่งผลกระทบต่อระบบ ERP บุคคลนั้นจะเกิดความตระหนักและหาวิธีการรับมือกับภัยคุกคามได้อย่างเหมาะสม

การรับมือภัยคุกคามในการติดตั้งการควบคุมบนระบบ ERP (Behavioral) คือ การแสดงออกถึงพฤติกรรมในการป้องกันภัยคุกคาม (Boss et al., 2015) ซึ่งในงานวิจัยนี้หมายถึง การที่ผู้ประกอบการ SMEs ที่ใช้งานระบบ ERP แสดงออกถึงการรับมือภัยคุกคามโดยนำการควบคุมบนระบบสารสนเทศเข้ามาใช้กับระบบ ERP

3. กรอบแนวคิดการวิจัยและสมมติฐานการวิจัย

กรอบแนวคิดการวิจัยนี้ มีปัจจัยที่เกี่ยข้อง 9 ปัจจัย โดยมี 7 ปัจจัยที่ได้นำมาจาก ทฤษฎี PMT ได้แก่ การรับรู้ถึงจุดอ่อน การับรู้ถึงความรุนแรง ความคาดหวังในประสิทธิผลของการตอบสนอง การรับรู้ความสามารถของตนเอง ค่าใช้จ่ายในการตอบสนอง ความตั้งใจในการรับมือภัยคุกคาม การรับมือด้วยการติดตั้งการควบคุม และอีก 2 ปัจจัยเป็นปัจจัยเพิ่มเติมที่ได้นำเพิ่มเข้าไปในกรอบแนวคิด ได้แก่ ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศและความตระหนักถึงความปลอดภัย โดยปัจจัยทางด้านความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ เป็นปัจจัยเฉพาะสำหรับกลุ่มตัวอย่าง SMEs ที่ใช้วัดความรู้ของผู้ประกอบการหรือผู้เกี่ยวข้องในแง่ความรู้ความเข้าใจต่อภัยคุกคาม ซึ่งการรับรู้ถึงจุดอ่อนส่งผลต่อความตั้งใจในการรับมือภัยคุกคาม การรับรู้ถึงความรุนแรงส่งผลต่อความตั้งใจในการรับมือภัยคุกคาม ความคาดหวังในประสิทธิผลของการตอบสนองส่งผลต่อความตั้งใจในการรับมือภัยคุกคาม การรับรู้ความสามารถของตนเองส่งผลต่อความตั้งใจในการรับมือภัยคุกคาม ค่าใช้จ่ายในการตอบสนองส่งผลต่อความตั้งใจในการรับมือภัยคุกคาม การรับรู้ถึงจุดอ่อนส่งผลต่อความตระหนักถึงความปลอดภัย ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศส่งผลต่อความตระหนักถึงความปลอดภัย ความตั้งใจในการรับมือภัยคุกคามส่งผลต่อการรับมือด้วยการติดตั้งการควบคุม และความตระหนักถึงความปลอดภัยส่งผลต่อการรับมือด้วยการติดตั้งการควบคุม ดังภาพที่ 1



ภาพที่ 1 แนวคิดเกิดความตระหนัก

งานวิจัยของ Williams et al. (2014) แสดงให้เห็นว่า การที่บุคคลรับรู้ถึงช่องโหว่ของระบบสารสนเทศที่อาจเป็นอันตรายต่อข้อมูลไม่ว่าจะเป็นข้อมูลระดับองค์กร หรือข้อมูลส่วนบุคคล ส่งผลให้บุคคลเกิดความตั้งใจในการรับมือภัยคุกคาม ดังนั้นสามารถตั้งสมมติฐานวิจัยได้ว่า

สมมติฐานที่ 1: การรับรู้ถึงจุดอ่อนส่งผลทางบวกต่อความตั้งใจในการรับมือกับภัยคุกคาม

จากงานวิจัยของ Boss et al. (2015) แสดงให้เห็นว่า การที่บุคคลได้รับรู้ถึงผลกระทบและระดับความรุนแรงที่เกิดขึ้นจากภัยคุกคามต่อระบบสารสนเทศของบุคคล ทำให้บุคคลมีความตั้งใจที่จะป้องกันภัยคุกคามที่จะเกิดขึ้น จึงนำไปสู่สมมติฐานในการวิจัยดังนี้

สมมติฐานที่ 2: การรับรู้ถึงความรุนแรงส่งผลทางบวกต่อความตั้งใจในการรับมือกับภัยคุกคาม

การที่บุคคลคาดหวังว่าการปฏิบัติตามข้อกำหนดในการใช้ระบบสารสนเทศ หรือการใช้ระบบรักษาความปลอดภัยทางสารสนเทศที่มีประสิทธิภาพสามารถช่วยลดทอนหรือป้องกันความเสี่ยงของภัยคุกคามที่จะเกิดขึ้นส่งผลให้บุคคลเกิดความตั้งใจทีจะรับมือกับภัยคุกคาม (Yoon et al., 2012) จึงนำไปสู่สมมติฐานในการวิจัยดังนี้

สมมติฐานที่ 3: ความคาดหวังในประสิทธิผลของการตอบสนองส่งผลทางบวกต่อความตั้งใจในการรับมือกับภัยคุกคาม

บุคคลเชื่อว่าตนเองมีความสามารถมากพอที่จะสามารถจัดการกับภัยคุกคามที่จะเกิดขึ้น เมื่อบุคคลมีความเชื่อมั่นในความสามารถของตนเองทำให้เกิดความตั้งใจที่จะป้องกันภัยคุกคาม (Johnston & Warkentin, 2010) จึงนำไปสู่สมมติฐานในการวิจัยดังนี้

สมมติฐานที่ 4: การรับรู้ความสามารถของตนเองส่งผลทางบวกต่อความตั้งใจในการรับมือกับภัยคุกคาม

การที่จะให้เกิดความตั้งใจในการป้องภัยคุกคามนั้น ระบบรักษาความปลอดภัยของระบบสารสนเทศต้องมีการใช้งานที่ไม่ซับซ้อนหรือไม่ยุ่งยาก รวมไปถึงค่าใช้จ่ายในติดตั้งระบบต้องมีความเหมาะสม (Yoon et al., 2012) จึงนำไปสู่สมมติฐานในการวิจัยดังนี้

สมมติฐานที่ 5: ค่าใช้จ่ายการตอบสนองส่งผลทางลบต่อความตั้งใจในการรับมือกับภัยคุกคาม

งานวิจัยของ Gusti (2016) แสดงให้เห็นว่า การที่บุคคลจะเกิดความตั้งใจได้นั้น บุคคลนั้นต้องมีความรู้ความเข้าใจในสิ่งนั้น จากการเรียนรู้ ประสบการณ์ หรือการวิจัยที่สะสมมาในอดีต ซึ่งจากผลการวิจัยพบว่าเมื่อเกิดการเพิ่มความรู้ความเข้าใจจะทำให้ความตั้งใจเพิ่มขึ้นตาม จึงนำไปสู่สมมติฐานในการวิจัยดังนี้

สมมติฐานที่ 6: ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศส่งผลทางบวกต่อความตั้งใจในการรับมือกับภัยคุกคาม

งานวิจัยของ Al-Saqer and Seliaman (2016) แสดงให้เห็นว่า การที่บุคคลรับรู้ถึงช่องโหว่และจุดอ่อนของข้อมูลส่วนบุคคลบนโซเชียลเน็ตเวิร์ค ทำให้บุคคลรู้สึกไม่ปลอดภัยในข้อมูลส่วนบุคคลของตนเอง ส่งผลให้บุคคลตระหนักถึงความปลอดภัยในข้อมูลส่วนบุคคล จึงนำไปสู่สมมติฐานในการวิจัยดังนี้

สมมติฐานที่ 7: การรับรู้ถึงจุดอ่อนส่งผลทางบวกต่อความตระหนักถึงความปลอดภัย

เมื่อบุคคลเกิดความรู้ความเข้าใจเกี่ยวกับความปลอดภัยของระบบสารสนเทศ จากการศึกษา ประสบการณ์ และจากการวิจัย ทำให้บุคคลเกิดความเข้าใจและตระหนักถึงความปลอดภัยของระบบสารสนเทศ (Mejias, 2012) จึงนำไปสู่สมมติฐานในการวิจัยดังนี้

สมมติฐานที่ 8: ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศส่งผลทางบวกต่อความตระหนักถึงความปลอดภัย

งานวิจัยของ Boss et al. (2015) แสดงให้เห็นว่า การแสดงออกถึงพฤติกรรมในการป้องกันและรักษาความปลอดภัยของระบบสารสนเทศ เกิดจากบุคคลมีความตั้งใจที่จะรับมือกับภัยคุกคามด้วยวิธีการต่าง ๆ ซึ่งเมื่อบุคคลเกิดความตั้งใจแล้วจะเกิดการแสดงออกเชิงพฤติกกรรมตามมา จึงนำไปสู่สมมติฐานในการวิจัยดังนี้

สมมติฐานที่ 9: ความตั้งใจในการรับมือกับภัยคุกคามส่งผลทางบวกต่อการรับมือภัยคุกคามด้วยการติดตั้งการควบคุมบนระบบ ERP

จากงานวิจัยของ Mejias (2012) แสดงให้เห็นว่า เมื่อบุคคลตระหนักถึงความปลอดภัยในข้อมูลของตนเอง บุคคลเหล่านั้นจะแสดงออกถึงพฤติกรรมในการป้องกันและรักษาความปลอดภัยข้อมูลของตนเอง จึงนำไปสู่สมมติฐานในการวิจัยดังนี้

สมมติฐานที่ 10: ความตระหนักถึงความปลอดภัยส่งผลทางบวกต่อการรับมือภัยคุกคามด้วยการติดตั้งการควบคุมบนระบบ ERP

4. วิธีการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงปริมาณโดยเป็นการรวบรวมข้อมูลจากกลุ่มตัวอย่าง จากผู้ประกอบการ หรือพนักงานผู้ที่เกี่ยวข้องกับระบบ ERP ในธุรกิจขนาดกลางและขนาดย่อมที่นำระบบ ERP เข้ามาใช้งาน เป็นตัวแทนของสถานประกอบการแต่ละแห่ง จำนวน 160 ราย โดยได้จัดทำแบบสอบถามในรูปแบบอิเล็กทรอนิกส์ ซึ่งจัดสร้างขึ้นมาจากงานวิจัยที่เกี่ยวข้อง (ประกอบด้วย Ifinedo, 2012; Yoon et al., 2012; Chou and Chou, 2016; Klein and Luciano, 2016; Flores et al., 2014; Bulgurcu et al., 2010; Boss et al., 2015; Weiss, 2009; Workman et al., 2008; Ciampa, 2005)

5. ผลการวิจัยและอภิปรายผล

5.1 การทดสอบข้อตกลงเบื้องต้นทางสถิติ

ข้ออมูลที่จัดเก็บจากกลุ่มตัวอย่างมีการนำไปทดสอบข้อมูลขาดหายและการสอบทานการกระจายข้อมูล พบว่า ไม่มีข้อมูลใดขาดหาย หรือมีตัวแปรบางตัวแปรที่ไม่มีการกระจายค่าแบบปกติอีกทั้งมีค่า Error มีการแจกแจงแบบปกติ และมีค่า Standard residual อยู่ระหว่าง -3 ถึง +3 แสดงว่าตัวแปรมีการแจกแจงแบบปกติ และมีความสัมพันธ์เชิงเส้นตรงจึงสามารถนำไปวิเคราะห์ต่อได้

5.2 การประเมินความเที่ยงและความตรงของแบบสอบถาม

งานวิจัยนี้ได้ตรวจสอบความเที่ยงของแบบสอบถาม (Reliability) ด้วยค่าสัมประสิทธิ์ครอนบาคแอลฟา (Cronbach's alpha) และความตรงของแบบสอบถาม (Validity) และพบว่าปัจจัยความตระหนักถึงความปลอดภัยมีค่าสัมประสิทธิ์แอลฟาของครอนบาค เท่ากับ 0.569 ปัจจัยการรับรู้ถึงความรุนแรง ค่าสัมประสิทธิ์แอลฟาของครอนบาค เท่ากับ 0.507 ปัจจัยความคาดหวังในประสิทธิผลของการตอบสนอง ค่าสัมประสิทธิ์แอลฟาของครอนบาค เท่ากับ 0.671 และปัจจัยการรับมือภัยคุกคามด้วยการติดตั้งการควบคุมบนระบบ ERP ค่าสัมประสิทธิ์แอลฟาของครอนบาค เท่ากับ 0.647 ซึ่งต่ำกว่า 0.7 ทั้งนี้จากการค้นคว้าข้อมูลอ้างอิงเพิ่มเติม พบว่าค่าสัมประสิทธิ์แอลฟาของครอนบาค ระหว่าง 0.5 ถึง 0.75 ยังมีความน่าเชื่อถือในระดับปานกลาง (Hinton et al., 2014) ดังที่แสดงตามตารางที่ 1

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน น้ำหนักองค์ประกอบ และค่าสัมประสิทธิ์แอลฟาครอนบาค ของตัวแปรทั้งหมด

คำถาม	ค่าเฉลี่ย (Mean)	ค่าเบี่ยงเบนมาตรฐาน (S.D.)	น้ำหนักองค์ประกอบ (Factor loading)
ปัจจัยที่ 1: การรับรู้ถึงจุดอ่อน (Perceived vulnerability) (Cronbach's alpha = 0.798, % of variance = 63.970)			
ระบบ ERP ของท่านอาจมีจุดอ่อนที่จะถูกภัยคุกคาม เช่น ข้อมูลถูกนำเข้าระบบ ERP โดยไม่ได้รับอนุมัติ ส่งผลให้ข้อมูลไม่ถูกต้องและครบถ้วน เป็นต้น	3.61	1.017	0.714
ท่านเชื่อว่าระบบ ERP อาจมีความเสี่ยงต่อการถูกโจรกรรมข้อมูล	3.70	0.977	0.721
ท่านเชื่อว่าผู้ไม่ประสงค์ดีสามารถโจรกรรมข้อมูลจากระบบ ERP ของท่านได้	3.66	1.023	0.756
ท่านรู้สึกว่าระบบ ERP มีช่องโหว่ที่อาจถูกภัยคุกคามที่ส่งผลต่อความมั่นคงด้านข้อมูลขององค์กรท่าน	3.59	1.037	0.837
ปัจจัยที่ 2: การรับรู้ถึงความรุนแรง (Perceived severity) (Cronbach's alpha = 0.507, % of variance = 25.464)			
ท่านคิดว่าสปายแวร์หรือไวรัส ในระบบ ERP จะส่งผลต่อความถูกต้องของข้อมูล	3.87	0.765	0.621
ท่านคิดว่าสปายแวร์หรือไวรัส ในระบบ ERP จะส่งผลต่อการทำงานเป็นอย่างมากเช่นทำให้ท่านไม่สามารถเข้าถึงข้อมูลที่ใช้ในการทำงานได้	3.90	0.813	0.744
ท่านให้ความสำคัญในการจัดการสปายแวร์หรือไวรัสในระบบ ERP	4.07	0.769	0.661
ท่านคิดว่าการสูญเสียข้อมูลจากการถูกโจรกรรมเป็นปัญหาสำคัญ	4.17	0.828	0.636

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน น้ำหนักองค์ประกอบ และค่าสัมประสิทธิ์แอลฟาครอนบาค ของตัวแปรทั้งหมด (ต่อ)

คำถาม	ค่าเฉลี่ย (Mean)	ค่าเบี่ยงเบนมาตรฐาน (S.D.)	น้ำหนักองค์ประกอบ (Factor loading)
ปัจจัยที่ 3: ความคาดหวังในประสิทธิผลของการตอบสนอง (Response efficacy) (Cronbach's alpha = 0.671, % of variance = 41.312)			
ท่านคิดว่าการกำหนดนโยบายในการใช้งานเครือข่ายคอมพิวเตอร์ช่วยป้องกันภัยคุกคามได้	4.14	0.823	0.701
ท่านเชื่อว่าการปฏิบัติตามนโยบายที่ได้กำหนดไว้จะสามารถช่วยป้องกันภัยคุกคามได้	4.07	0.842	0.767
ท่านเชื่อว่าการเปิดใช้งานมาตรการรักษาความปลอดภัยบนคอมพิวเตอร์เป็นวิธีที่มีประสิทธิภาพในการป้องกันข้อมูลคอมพิวเตอร์จากการได้รับความเสียหายจากซอฟต์แวร์ที่เป็นอันตรายเช่น ไวรัส	4.05	0.818	0.734
ปัจจัยที่ 4: การรับรู้ความสามารถของตนเอง (Self-Efficacy) (Cronbach's alpha = 0.775, % of variance = 58.816)			
ท่านสามารถจัดการกับไวรัสได้	3.65	1.012	0.631
ท่านเชื่อว่าตนเองมีทักษะมากพอในการจัดการภัยคุกคามที่มีโอกาสเข้ามา	3.54	0.953	0.721
ท่านสามารถป้องกันข้อมูล บนระบบ ERP จากภัยคุกคามได้	3.67	0.997	0.754
เมื่อเครือข่ายในองค์กรของท่านติดไวรัส ท่านสามารถตัดสินใจและแก้ไขปัญหาได้อย่างรวดเร็ว	3.74	1.007	0.661
ปัจจัยที่ 5: ค่าใช้จ่ายการตอบสนอง (Response cost) (Cronbach's alpha = 0.862, % of variance = 115.064)			
ท่านคิดว่าการติดตั้งการควบคุมบนระบบ ERP เช่น การกำหนดรหัสผ่าน การใช้ลายนิ้วมือในการเข้าถึง การจำกัดสิทธิ์การเข้าถึง เป็นต้น ทำให้มีความยุ่งยากในการใช้งานระบบ	3.22	1.157	0.872
ท่านคิดว่าการติดตั้งการควบคุมบนระบบ ERP เช่น การกำหนดรหัสผ่าน การใช้ลายนิ้วมือในการเข้าถึง การจำกัดสิทธิ์การเข้าถึง เป็นต้น ทำให้เสียเวลาในการทำงาน	3.13	1.296	0.873
ท่านคิดว่าการติดตั้งการควบคุมบนระบบ ERP เช่น การกำหนดรหัสผ่าน การใช้ลายนิ้วมือในการเข้าถึง การจำกัดสิทธิ์การเข้าถึง เป็นต้น ทำให้เสียค่าใช้จ่ายเพิ่มมากขึ้น	3.24	1.179	0.800
ปัจจัยที่ 6: ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ (Knowledge) (Cronbach's Alpha = 0.743, % of variance = 71.550)			
ท่านทราบถึงวิธีการป้องกัน ไม่ให้เครือข่ายคอมพิวเตอร์ขององค์กรท่าน ถูกคุกคามจากโปรแกรมที่อาจเป็นไวรัสต่าง ๆ	3.72	0.927	0.722
ท่านสามารถระบุได้ว่าโปรแกรมใดเป็นไวรัส	3.60	1.123	0.718
ท่านสามารถแยกได้ว่าโปรแกรมใดที่เป็นไวรัสและเป็นอันตรายต่อระบบสารสนเทศ	3.56	1.063	0.726

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน น้ำหนักองค์ประกอบ และค่าสัมประสิทธิ์แอลฟาครอนบาค ของตัวแปรทั้งหมด (ต่อ)

คำถาม	ค่าเฉลี่ย (Mean)	ค่าเบี่ยงเบนมาตรฐาน (S.D.)	น้ำหนักองค์ประกอบ (Factor Loading)
ปัจจัยที่ 7: ความตระหนักถึงความปลอดภัย (Awareness) (Cronbach's alpha = 0.569, % of variance = 38.680)			
ท่านทราบถึงภัยคุกคามที่จะเกิดขึ้นต่อระบบ ERP	3.68	0.910	0.446
ท่านกังวลเกี่ยวกับความปลอดภัยของข้อมูลบนระบบ ERP	3.90	0.836	0.871
ท่างกังวลเกี่ยวกับผลกระทบต่อการถูกโจรกรรมข้อมูล	3.93	0.797	0.671
ปัจจัยที่ 8: ความตั้งใจในการรับมือกับภัยคุกคาม (Intention) (Cronbach's Alpha = 0.724, % of variance = 38.741)			
ท่านมีความตั้งใจที่จะดำเนินการเพื่อรับมือกับภัยคุกคามทางคอมพิวเตอร์อย่างสม่ำเสมอ	3.94	0.790	0.573
ท่านตั้งใจที่จะติดตั้งการควบคุมบนระบบ ERP เช่น การกำหนดรหัสผ่าน ระยะเวลาในการเปลี่ยนรหัส การใช้โทเค็น การใช้ลายนิ้วมือ การจำกัดสิทธิ์การเข้าถึง รวมไปถึงระบบการตรวจสอบประวัติการใช้งานย้อนหลัง	3.88	0.866	0.540
ท่านมีความตั้งใจที่จะปฏิบัติตามมาตรการรักษาความปลอดภัยตามที่กำหนดไว้	4.10	0.853	0.848
ท่านจะชักชวนและให้คำแนะนำแก่เพื่อนร่วมงานในการรับมือกับภัยคุกคามที่อำจเกิดขึ้นกับระบบ ERP	4.08	0.856	0.690
ปัจจัยที่ 9: การรับมือภัยคุกคามด้วยการติดตั้งการควบคุมบนระบบ ERP (Cronbach's Alpha = 0.647, % of variance = 43.788)			
องค์กรของท่านมีการพิสูจน์ตัวจริงในการเข้าใช้งานระบบ ERP เช่น การกำหนดรหัสผ่าน ระยะเวลาในการเปลี่ยนรหัส การใช้โทเค็น ลายนิ้วมือ เป็นต้น	4.00	0.912	0.461
องค์กรของท่านมีการกำหนดสิทธิ์การเข้าถึงระบบ ERP	4.10	0.836	0.846
องค์กรของท่านมีระบบที่สามารถใช้ตรวจสอบประวัติการใช้งานย้อนหลังบนระบบ ERP	4.07	0.842	0.748

5.3 ลักษณะทางประชากรศาสตร์ของกลุ่มตัวอย่าง

กลุ่มตัวอย่าง 162 คน ส่วนใหญ่เป็นเจ้าของกิจการ (ร้อยละ 39) โดยบทบาทในการตัดสินใจนำระบบ ERP มาใช้ส่วนใหญ่เป็นผู้ร่วมตัดสินใจ (ร้อยละ 46) อายุงานโดยส่วนใหญ่มีอายุงาน 6-10 ปี (ร้อยละ 28) โดยส่วนใหญ่มีความรู้เกี่ยวกับระบบ ERP (ร้อยละ 76) ซึ่งรู้ความหมายเป็นส่วนใหญ่ (ร้อยละ 25) เมื่อจำแนกตามลักษณะของธุรกิจกลุ่มตัวอย่างส่วนใหญ่ประกอบธุรกิจบริการ (ร้อยละ 43) และเมื่อจำแนกตามประเภทธุรกิจกลุ่มตัวอย่างส่วนใหญ่ประกอบธุรกิจประเภทสินค้าและบริการมากที่สุด (ร้อยละ 22) ซึ่งจำนวนพนักงานในองค์กรของกลุ่มตัวอย่างส่วนใหญ่คือ 10-30 คน (ร้อยละ 35) รูปแบบ ERP ที่ใช้ในองค์กรของกลุ่มตัวอย่างส่วนใหญ่เป็นแบบ On-premise (ร้อยละ 73) มีหน่วยงานที่รับผิดชอบเกี่ยวกับเทคโนโลยีสารสนเทศหรือระบบสารสนเทศ (ร้อยละ 56) และหน่วยงานที่รับผิดชอบเกี่ยวกับเทคโนโลยีสารสนเทศหรือระบบสารสนเทศมีความรู้ด้าน ERP (ร้อยละ 52)

5.4 การทดสอบสมมติฐานในการวิจัย

งานวิจัยนี้ทดสอบสมมติฐานการวิจัยจากกรอบแนวคิดการวิจัยด้วยการวิเคราะห์การถดถอยแบบเชิงชั้น (Hierarchical regression) ผลลัพธ์ที่ได้แสดงในตารางที่ 2 โดยสามารถวิเคราะห์ผลทางสถิติได้ดังนี้

5.4.1 อิทธิพลทางตรงต่อความตั้งใจในการรับมือกับภัยคุกคาม

ผลทางสถิติแสดงให้เห็นว่า ปัจจัยด้านการรับรู้ถึงจุดอ่อน ปัจจัยด้านการรับรู้ถึงความรุนแรง ปัจจัยด้านความคาดหวังในประสิทธิผลของการตอบสนอง ปัจจัยด้านการรับรู้ความสามารถของตนเอง ปัจจัยด้านค่าใช้จ่ายการตอบสนอง และปัจจัยด้านความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ สามารถร่วมกันอธิบายความแปรปรวนในตัวแปรความตั้งใจในการรับมือกับภัยคุกคามได้ ร้อยละ 39.1 (R^2 = 0.391) รายละเอียดอิทธิพลแต่ละปัจจัยมีดังนี้

5.4.1.1 การรับรู้ถึงจุดอ่อน ไม่ส่งผลต่อความตั้งใจในการรับมือกับภัยคุกคาม ที่การถดถอยที่ปรับมาตรฐานแล้ว (Beta) เท่ากับ -0.109 มีระดับนัยสำคัญ p = 0.120 ซึ่งไม่สนับสนุนสมมติฐานที่ 1 ที่กล่าวว่า การรับรู้ถึงจุดอ่อนส่งผลทางบวกต่อความตั้งใจในการรับมือกับภัยคุกคามและไม่สอดคล้องกับงานวิจัยของ Williams et al. (2014) แต่สอดคล้องกับงานวิจัยของ Yoon et al. (2012) ซึ่งกล่าวว่า กลุ่มตัวอย่างบางรายอาจจะมีประสบการณ์ในการประเมินความเป็นไปได้ของการเกิดภัยคุกคามน้อยทำให้ไม่รับรู้ถึงจุดอ่อนหรือภัยคุกคามที่อาจเกิดขึ้นกับระบบ นอกจากนี้กลุ่มตัวอย่างส่วนใหญ่เป็นเจ้าของกิจการอาจไม่ได้มีความชำนาญในการประเมินความน่าจะเป็นในการเกิดภัยคุกคามต่อระบบ

5.4.1.2 การรับรู้ถึงความรุนแรง ส่งผลต่อความตั้งใจในการรับมือกับภัยคุกคาม ที่การถดถอยที่ปรับมาตรฐานแล้ว (Beta) เท่ากับ 0.282 มีระดับนัยสำคัญ p = 0.000 ซึ่งสนับสนุนสมมติฐานที่ 2 ที่กล่าวว่า การรับรู้ถึงความรุนแรงส่งผลทาง บวกต่อความตั้งใจในการรับมือกับภัยคุกคาม เนื่องจากค่าสัมประสิทธิ์อิทธิพลมีเครื่องหมายบวกไปในทิศทางเดียวกับสมมติฐานการวิจัยที่ตั้งไว้ และสอดคล้องกับงานวิจัยของ Boss et al. (2015) ที่กล่าวว่าเมื่อบุคคลรับรู้ถึงความรุนแรงและความเสียหายที่จะเกิดขึ้นกับข้อมูลจะเกิดความตั้งใจในการสำรองข้อมูล

5.4.1.3 ความคาดหวังในประสิทธิผลของการตอบสนอง ส่งผลต่อความตั้งใจในการรับมือกับภัยคุกคาม ที่การถดถอยที่ปรับมาตรฐานแล้ว (Beta) เท่ากับ 0.392 มีระดับนัยสำคัญ p = 0.000 ซึ่งสนับสนุนสมมติฐานที่ 3 ที่กล่าวว่า ความคาดหวังในประสิทธิผลของการตอบสนองส่งผลทางบวกต่อความตั้งใจในการรับมือกับภัยคุกคาม เนื่องจากค่าสัมประสิทธิ์อิทธิพลมีเครื่องหมายบวกไปในทิศทางเดียวกับสมมติฐานการวิจัยที่ตั้งไว้ และสอดคล้องกับงานวิจัยของ Yoon et al. (2012) ที่กล่าวว่าเมื่อบุคคลเกิดความเชื่อในกระบวนการในการดำเนินการเพื่อการป้องกันภัยคุกคามจะทำให้เกิดความตั้งใจในการป้องกันภัยคุกคาม

5.4.1.4 การรับรู้ความสามารถของตนเอง ไม่ส่งผลต่อความตั้งใจในการรับมือกับภัยคุกคาม ที่การถดถอยที่ปรับมาตรฐานแล้ว (Beta) เท่ากับ 0.042 มีระดับนัยสำคัญ p = 0.645 ซึ่งไม่สนับสนุนสมมติฐานที่ 4 ที่กล่าวว่า การรับรู้ความสามารถของตนเองส่งผลทางบวกต่อความตั้งใจในการรับมือกับภัยคุกคาม และไม่สอดคล้องกับงานวิจัยของ (Johnston & Warkentin, 2010) แต่สอดคล้องกับงานวิจัยของ Williams et al. (2014) ที่กล่าวว่ากลุ่มตัวอย่างมีความแตกต่างกันเกี่ยวกับความเชื่อมั่นในความสามารถของตนเองที่จะป้องกันภัยคุกคาม ซึ่งกลุ่มตัวอย่างที่ได้จากการสำรวจในครั้งนี้ค่อนข้างมีความหลายหลาย อาทิตำแหน่งในบริษัทซึ่งส่วนใหญ่เป็นเจ้าของกิจการ ซึ่งเจ้าของกิจการอาจมีความรู้ความสามารถเกี่ยวกับการป้องกันภัยคุกคามในภาพกว้างซึ่งอาจส่งผลให้เจ้าของกิจการไม่มีความเชื่อมั่นว่าตนเองสามารถรับมือกับภัยคุกคามที่จะเกิดขึ้นได้

5.4.1.5 ค่าใช้จ่ายการตอบสนอง ไม่ส่งผลต่อความตั้งใจในการรับมือกับภัยคุกคาม ที่การถดถอยที่ปรับมาตรฐานแล้ว (Beta) เท่ากับ -0.029 มีระดับนัยสำคัญ p = 0.671 ซึ่งไม่สนับสนุนสมมติฐานที่ 5 ที่กล่าวว่า ค่าใช้จ่ายการตอบสนองส่งผลทางลบต่อความตั้งใจในการรับมือกับภัยคุกคาม และไม่สอดคล้องกับงานวิจัยของ Yoon et al. (2012) แต่สอดคล้องกับงานวิจัยของ Ifinedo (2012) ที่ศึกษาเรื่องการทำความเข้าใจนโยบายการรักษาความปลอดภัย

ระบบของสารสนเทศด้วยทฤษฎีพฤติกรรมตามแผน และทฤษฎีแรงจูงใจในการป้องกัน ที่กล่าวว่า ผู้ตอบแบบสอบถามบางคนมีความเป็นไปได้ที่มีความคิดเห็นต่อค่าใช้จ่ายในการตอบสนองในเชิงบวกเพราะกลุ่มตัวอย่างบางคนเชื่อว่า เมื่อนำระบบรักษาความปลอดภัยเข้ามาปรับใช้กับองค์กร ระบบรักษาความปลอดภัยเหล่านั้นไม่ได้ทำให้กลุ่มตัวอย่างรู้สึกว่า การใช้เวลาในการทำงานมากขึ้น รู้สึกไม่สะดวกในการทำการหรือรู้สึกว่าค่าใช้จ่ายในการนำระบบรักษาความปลอดภัยเข้ามาใช้ไม่สมเหตุสมผลซึ่งอาจจะมาจากกลุ่มตัวอย่างที่เป็นผู้ตัดสินใจ ผู้ร่วมตัดสินใจ หรือผู้ให้ข้อมูลประกอบตัดสินใจในการนำระบบเข้ามาใช้ซึ่งอาจไม่ได้เป็นผู้ใช้งานเองทำให้บุคคลเหล่านั้นเห็นประโยชน์ของการควบคุม

5.4.1.6 ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ ส่งผลต่อความตั้งใจในการรับมือกับภัยคุกคาม ที่การถดถอยที่ปรับมาตรฐานแล้ว (Beta) เท่ากับ 0.196 มีระดับนัยสำคัญ p = 0.025 ซึ่งสนับสนุนสมมติฐานที่ 6 ที่กล่าวว่า ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศส่งผลทางบวกต่อความตั้งใจในการรับมือกับภัยคุกคาม เนื่องจากค่าสัมประสิทธิ์อิทธิพลมีเครื่องหมายบวกไปในทิศทางเดียวกับสมมติฐานการวิจัยที่ตั้งไว้ และสอดคล้องกับงานวิจัยของ Gusti (2016) ที่กล่าวว่าเมื่อมีความรู้เพิ่มมากขึ้นความตั้งใจที่ก่อให้เกิดพฤติกรรมก็จะเพิ่มตาม

5.4.2 อิทธิพลทางตรงต่อความตระหนักถึงความปลอดภัย

ผลทางสถิติแสดงให้เห็นว่า ปัจจัยด้านการับรู้ถึงจุดอ่อน และความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ สามารถร่วมกันอธิบายความแปรปรวนในตัวแปรความตระหนักถึงความปลอดภัยได้ ร้อยละ 20.3 (R Square = 0.203) รายละเอียดอิทธิพลแต่ละปัจจัยมีดังนี้

5.4.2.1 การรับรู้ถึงจุดอ่อน ส่งผลต่อความตระหนักถึงความปลอดภัย ที่การถดถอยที่ปรับมาตรฐานแล้ว (Beta) เท่ากับ 0.189 มีระดับนัยสำคัญ p = 0.012 ซึ่งสนับสนุนสมมติฐานที่ 7 ที่กล่าวว่า การรับรู้ถึงจุดอ่อนส่งผลทางบวกต่อความตระหนักถึงความปลอดภัย เนื่องจากค่าสัมประสิทธิ์อิทธิพลมีเครื่องหมายบวกไปในทิศทางเดียวกับสมมติฐานการวิจัยที่ตั้งไว้ และสอดคล้องกับงานวิจัยของ Al-Saqer and Seliaman (2016) ที่กล่าวว่าการรับรู้ถึงความเสี่ยงต่อความเป็นส่วนตัวในเครือข่ายสังคมส่งผลในเชิงบวกต่อระดับการรับรู้ถึงเนื้อหาของนโยบายความเป็นส่วนตัวของ SNS

5.6.2.2 ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ ส่งผลต่อความตระหนักถึงความปลอดภัย ที่การถดถอยที่ปรับมาตรฐานแล้ว (Beta) เท่ากับ 0.355 มีระดับนัยสำคัญ p = 0.000 ซึ่งสนับสนุนสมมติฐานที่ 8 ที่กล่าวว่า ความรู้ความเข้าใจในความปลอดภัยของระบบส่งผลทางบวกต่อความตระหนักถึงความปลอดภัย เนื่องจากค่าสัมประสิทธิ์อิทธิพลมีเครื่องหมายบวกไปในทิศทางเดียวกับสมมติฐานการวิจัยที่ตั้งไว้ และสอดคล้องกับงานวิจัยของ Mejias (2012) ที่กล่าวว่า การมีความรู้ทางเทคโนโลยีสามารถพยากรณ์ความตระหนักต่อความปลอดภัยของสารสนเทศ

5.4.3 อิทธิพลทางตรงต่อการรับมือภัยคุกคามด้วยการติดตั้งการควบคุมบนระบบ ERP

ผลทางสถิติแสดงให้เห็นว่า ปัจจัยด้านความตั้งใจในการรับมือกับภัยคุกคาม และปัจจัยด้านความตระหนักถึงความปลอดภัย สามารถร่วมกันอธิบายความแปรปรวนในตัวแปรความตั้งใจในการรับมือกับภัยคุกคามได้ ร้อยละ 28.2 (R Square = 0.282) รายละเอียดอิทธิพลแต่ละปัจจัยมีดังนี้

5.4.3.1 ความตั้งใจในการรับมือกับภัยคุกคาม ส่งผลต่อการรับมือภัยคุกคามด้วยการติดตั้งการควบคุมบนระบบ ERP ที่การถดถอยที่ปรับมาตรฐานแล้ว (Beta) เท่ากับ 0.381 มีระดับนัยสำคัญ p = 0.000 ซึ่งสนับสนุนสมมติฐานที่ 9 ที่กล่าวว่า ความตั้งใจในการรับมือกับภัยคุกคามส่งผลทางบวกต่อการรับมือภัยคุกคามด้วยการติดตั้งการควบคุมบนระบบ ERP เนื่องจากค่าสัมประสิทธิ์อิทธิพลมีเครื่องหมายบวกไปในทิศทางเดียวกับสมมติฐานการวิจัยที่ตั้งไว้ และสอดคล้องกับงานวิจัยของ Boss et al. (2015) ที่กล่าวว่าเมื่อเกิดความตั้งใจแล้วจะนำไปสู่การแสดงออกเชิงพฤติกรรม

5.4.3.2 ความตระหนักถึงความปลอดภัย ส่งผลต่อการรับมือภัยคุกคามด้วยการติดตั้งการควบคุมบนระบบ ERP ที่การถดถอยที่ปรับมาตรฐานแล้ว (Beta) เท่ากับ 0.222 มีระดับนัยสำคัญ p = 0.005 ซึ่งสนับสนุนสมมติฐานที่ 10 ที่กล่าวว่า ความตระหนักถึงความปลอดภัยส่งผลทางบวกต่อการรับมือภัยคุกคามด้วยการติดตั้งการควบคุมบนระบบ ERP เนื่องจากค่าสัมประสิทธิ์อิทธิพลมีเครื่องหมายบวกไปในทิศทางเดียวกับสมมติฐานการวิจัยที่ตั้งไว้ และสอดคล้องกับงานวิจัยของ Mejias (2012) ที่กล่าวว่า เมื่อบุคคลเกิดความตระหนักถึงความปลอดภัยของข้อมูลนำไปสู่การแสดงออกเชิงพฤติกรรม

5.4.4 อิทธิพลทางอ้อมต่อการรับมือภัยคุกคามด้วยการติดตั้งตัวควบคุมบนระบบ ERP

ผลทางสถิติแสดงให้เห็นว่า ปัจจัยด้านการรับรู้ถึงความรุนแรง ปัจจัยด้านความคาดหวังในประสิทธิผลของการตอบสนอง และปัจจัยด้านความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ ส่งผลอิทธิพลทางอ้อมผ่านความตั้งใจในการรับมือกับภัยคุกคามไปยังการรับมือภัยคุกคามด้วยการติดตั้งตัวควบคุมบนระบบ ERP และปัจจัยด้านการรับรู้ถึงจุดอ่อน ปัจจัยด้านความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศส่งอิทธิพลทางอ้อมผ่านความตระหนักถึงความปลอดภัยไปยังการรับมือภัยคุกคามด้วยการติดตั้งตัวควบคุมบนระบบ ERP รายละเอียดอิทธิพลแต่ละปัจจัยมีดังนี้

5.4.4.1 การรับรู้ถึงความรุนแรง ส่งอิทธิพลทางอ้อมผ่านความตั้งใจในการรับมือกับภัยคุกคามไปยังการรับมือภัยคุกคามด้วยการติดตั้งตัวควบคุมบนระบบ ERP ที่ค่าสัมประสิทธิ์อิทธิพล เท่ากับ 0.107 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

5.4.4.2 ความคาดหวังในประสิทธิผลของการตอบสนอง ส่งอิทธิพลทางอ้อมผ่านความตั้งใจในการรับมือกับภัยคุกคามไปยังการรับมือภัยคุกคามด้วยการติดตั้งตัวควบคุมบนระบบ ERP ที่ค่าสัมประสิทธิ์อิทธิพล เท่ากับ 0.149 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

5.4.4.3 ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ ส่งอิทธิพลทางอ้อมผ่านความตั้งใจในการรับมือกับภัยคุกคามไปยังการรับมือภัยคุกคามด้วยการติดตั้งตัวควบคุมบนระบบ ERP ที่ค่าสัมประสิทธิ์อิทธิพล เท่ากับ 0.074 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

5.4.4.4 การรับรู้ถึงจุดอ่อน ส่งอิทธิพลทางอ้อมผ่านความตระหนักถึงความปลอดภัยไปยังการรับมือภัยคุกคามด้วยการติดตั้งตัวควบคุมบนระบบ ERP ที่ค่าสัมประสิทธิ์อิทธิพล เท่ากับ 0.042 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

5.4.4.5 ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ ส่งอิทธิพลทางอ้อมผ่านความตระหนักถึงความปลอดภัยไปยังการรับมือภัยคุกคามด้วยการติดตั้งตัวควบคุมบนระบบ ERP ที่ค่าสัมประสิทธิ์อิทธิพล เท่ากับ 0.079 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

ตารางที่ 2 ค่าสัมประสิทธิ์อิทธิพลทางตรง ทางอ้อม และอิทธิพลโดยรวมของตัวแปรแฝงในกรอบแนวคิดการวิจัย (แสดงเป็นคะแนนมาตรฐาน)

ตัวแปรตาม	R^2	อิทธิพล	ตัวแปรอิสระ							
			การรับรู้ถึงจุดอ่อน	การรับรู้ถึงความรุนแรง	ความคาดหวังในประสิทธิผลของการตอบสนอง	การรับรู้ความสามารถของตนเอง	ค่าใช้จ่ายการตอบสนอง	ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ	ความตั้งใจในการรับมือกับภัยคุกคาม	ความตระหนักถึงความปลอดภัย
ความตั้งใจในการรับมือกับภัยคุกคาม	0.391	ทางตรง	-0.109	0.282*	0.392*	0.042	-0.029	0.196*	-	-
		ทางอ้อม	-	-	-	-	-	-	-	-
		โดยรวม	-0.109	0.282*	0.392*	0.042	-0.029	0.196*	-	-
ความตระหนักถึงความปลอดภัย	0.203	ทางตรง	0.189*	-	-	-	-	0.355*	-	-
		ทางอ้อม	-	-	-	-	-	-	-	-
		โดยรวม	0.189*	-	-	-	-	0.355*	-	-
การรับมือภัยคุกคามด้วยการติดตั้งตัวควบคุมบนระบบ ERP	0.282	ทางตรง	-	-	-	-	-	-	0.381*	0.222*
		ทางอ้อม (IN)	-	0.107*	0.149*	-	-	0.074*	-	-
		ทางอ้อม (AW)	0.042*	-	-	-	-	0.079*	-	-
		โดยรวม	0.042*	0.107*	0.149*	-	-	0.153*	0.381*	0.222*

*P<0.05

6. สรุปผลการวิจัยและข้อเสนอแนะ

6.1 สรุปผลการวิจัย

ผลการวิเคราะห์ทางสถิติเกี่ยวกับปัจจัยที่กำหนดพฤติกรรมในการติดตั้งการควบคุมในระบบการบริหารทรัพยากรขององค์กร สำหรับธุรกิจขนาดกลางและขนาดย่อม พบว่า ปัจจัยที่ส่งผลต่อความตั้งใจในการรับมือกับภัยคุกคาม คือ ปัจจัยด้านความคาดหวังในประสิทธิผลของการตอบสนอง ปัจจัยด้านการรับรู้ถึงความรุนแรง ปัจจัยด้านความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ ตามลำดับ ส่วนปัจจัยที่ไม่ส่งผลต่อความตั้งใจในการรับมือกับภัยคุกคาม คือ ปัจจัยด้านการรับรู้ถึงจุดอ่อน ปัจจัยด้านการรับรู้ความสามารถของตนเอง และปัจจัยด้านค่าใช้จ่ายตอบสนอง ส่วนปัจจัยที่ส่งผลต่อความตระหนัก คือ ปัจจัยด้านความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ และปัจจัยด้านการรับรู้ถึงจุดอ่อน ตามลำดับ นอกจากนี้ยังพบว่า ปัจจัยที่ส่งผลต่อการรับมือภัยคุกคามด้วยการติดตั้งการควบคุมบนระบบ ERP คือ ปัจจัยด้านความตั้งใจในการรับมือกับภัยคุกคาม และความตระหนักถึงความปลอดภัย ตามลำดับ

6.2 ประโยชน์ของงานวิจัย

6.2.1 ประโยชน์ของงานวิจัยด้านทฤษฎี

ผลของงานวิจัยนี้ทำให้เกิดการสร้างกรอบแนวคิดที่ใช้อธิบายปัจจัยที่กำหนดพฤติกรรมในการติดตั้งการควบคุมในระบบการบริหารทรัพยากรขององค์กร สำหรับธุรกิจขนาดกลางและขนาดย่อม โดยพัฒนากรอบแนวคิดมาจากทฤษฎีโมเดลแรงจูงใจในการป้องกัน (Protection Motivation Theory) ของ Boss et al. (2015) ทำให้เกิดกรอบแนวคิดใหม่ในการศึกษาปัจจัยที่กำหนดพฤติกรรมในการติดตั้งการควบคุมในระบบการบริหารทรัพยากรขององค์กร สำหรับธุรกิจขนาดกลางและขนาดย่อม โดยมีข้อแตกต่างจากกรอบแนวคิดงานวิจัยในอดีตคือ มีการเพิ่ม แนวคิดความตระหนัก (Awareness) ที่ประกอบด้วยปัจจัยความรู้ความเข้าในความปลอดภัยของระบบสารสนเทศ และความตระหนักเข้ามาเพิ่มในการศึกษาเพิ่มเติม เพื่อเป็นแนวทางสำหรับงานวิจัยที่ต้องการศึกษาเกี่ยวกับปัจจัยที่กำหนดพฤติกรรมในการติดตั้งการควบคุมในระบบการบริหารทรัพยากรขององค์กร สำหรับธุรกิจขนาดกลางและขนาดย่อมโดยอาจทำการศึกษาเปรียบเทียบกันในแต่ลักษณะของธุรกิจที่ส่งผลต่อพฤติกรรมในการติดตั้งการควบคุมในระบบการบริหารทรัพยากรขององค์กร สำหรับธุรกิจขนาดกลางและขนาดย่อม รวมไปถึงสามารถนำกรอบแนวคิดของงานวิจัยนี้ไปศึกษาต่อยอดสำหรับงานวิจัยในอนาคต โดยอาจจะเพิ่มตัวแปรใหม่ ๆ เพิ่มเข้าไปในงานวิจัยด้วยอาทิ อิทธิพลทางสังคม เป็นต้น

6.2.2 ประโยชน์ของงานวิจัยทางภาคปฏิบัติ

จากการศึกษาปัจจัยที่ส่งผลต่อความตั้งใจในการรับมือกับภัยคุกคามพบว่า ความตั้งใจในการรับมือกับภัยคุกคามขึ้นอยู่กับ การรับรู้ถึงความรุนแรง ความคาดหวังในประสิทธิผลของการตอบสนอง และความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ โดยปัจจัยที่ส่งผลต่อความตั้งใจในการรับมือกับภัยคุกคามมากที่สุดคือ ปัจจัยด้านความคาดหวังในประสิทธิผลของการตอบสนอง สะท้อนให้เห็นว่าการที่บุคคลจะมีความตั้งใจในการรับมือกับภัยคุกคามนั้นเกิดจากความเชื่อของการกำหนดนโยบายในการใช้งานเครือข่ายคอมพิวเตอร์และออกมาตรการในการปฏิบัติตามนโยบายที่ช่วยป้องกันภัยคุกคาม ซึ่งผู้เกี่ยวข้องกับความปลอดภัยของระบบสารสนเทศ สามารถนำผลการวิจัยในส่วนนี้ไปช่วยในกระตุ้นและการตัดสินใจกำหนดนโยบายในการใช้งานเครือข่ายคอมพิวเตอร์ และออกมาตรการในการปฏิบัติตามนโยบายที่ช่วยป้องกันภัยคุกคาม ตามด้วยปัจจัยด้านการรับรู้ถึงความรุนแรง สะท้อนให้เห็นว่าเมื่อบุคคลทราบถึงผลกระทบและความรุนแรงของสปายแวร์ ไวรัส หรือภัยคุกคามในรูปแบบต่าง ๆ จะทำให้บุคคลเกิดความตั้งใจในการรับมือกับภัยคุกคามซึ่งผู้เกี่ยวข้องกับความปลอดภัยของระบบสารสนเทศ สามารถนำผลการวิจัยในส่วนนี้ไปช่วยในการสร้างความรู้เกี่ยวกับความรุนแรงของภัยคุกคามที่อาจขึ้นได้ทุกเมื่อให้แก่กิจการหรือบุคลกรภายในองค์กร และตามด้วยปัจจัยด้านความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศสะท้อนให้เห็นว่า เมื่อบุคคลมีความรู้และความเข้าใจในการป้องกันภัยคุกคามจะส่งผลให้เกิดความตั้งใจในการรับมือกับภัยคุกคาม บุคคลที่เกี่ยวข้องกับความปลอดภัยของระบบสารสนเทศสามารถนำผลการวิจัยในส่วนนี้นำไปสร้างความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์และวิธีป้องกันเบื้องต้น ให้กิจการหรือบุคลากรได้มีความรู้เพื่อที่จะได้เกิดความตั้งใจในการรับมือกับภัยคุกคาม

ในส่วนของปัจจัยที่ส่งผลต่อความตระหนักถึงความปลอดภัย พบว่า ความตระหนักถึงความปลอดภัยขึ้นอยู่กับปัจจัยด้านความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศมากที่สุดสะท้อนให้เห็นว่า ความตระหนักเกิดจากการความรู้ความเข้าใจตามแนวคิดของ Good and Merkel (1973) ซึ่งผู้เกี่ยวข้องกับความปลอดภัยของระบบสารสนเทศ สามารถนำผลการวิจัยในส่วนนี้ นำไปสร้างความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์และวิธีป้องกันเบื้องต้นเพื่อที่กิจการและบุคลากรจะเกิดความตระหนักจากความรู้ที่ได้รับ ตามด้วยปัจจัยด้านการรับรู้ถึงจุดอ่อน สะท้อนให้เห็นว่าเมื่อบุคคลทราบถึงข้อบกพร่อง หรือช่องโหว่ของระบบสารสนเทศจะทำให้เกิดความตระหนักในความปลอดภัยของระบบ โดยผู้เกี่ยวข้องกับความปลอดภัยของระบบสารสนเทศ สามารถนำผลการวิจัยในส่วนนี้ไปให้ความรู้เกี่ยวกับการประเมินความน่าจะเป็นในการเกิดภัยคุกคามให้แก่ กิจการและบุคลากรที่เกี่ยวข้อง เพื่อให้ทราบถึงข้อบกพร่องของระบบของตนเอง

ในส่วนของปัจจัยที่ส่งผลต่อการรับมือภัยคุกคามด้วยการติดตั้งการควบคุมบนระบบ ERP พบว่า การรับมือภัยคุกคามด้วยการติดตั้งการควบคุมบนระบบ ERP ขึ้นอยู่กับปัจจัยด้านความตั้งใจในการรับมือกับภัยคุกคาม และความตระหนักถึงความปลอดภัยะท้อนให้เห็นว่า เมื่อบุคคลเกิดความตั้งใจและความตระหนักจะนำไปสู่การแสดงออกทางพฤติกรรมในที่สุด

6.3 ข้อจำกัดในการวิจัย และข้อเสนอแนะสำหรับวิจัยต่อเนื่อง

งานวิจัยครั้งนี้เป็นการศึกษาจากกลุ่มตัวอย่าง ผู้ประกอบการหรือผู้มีส่วนเกี่ยวข้องกับระบบ ERP ขององค์กร ผลการวิจัยอาจไม่สามารถนำไปใช้ได้กับทุกกลุ่มคน ประกอบกับเป็นการวิจัยเชิงปริมาณที่เป็นการสื่อสารทางเดียว จึงอาจจะไม่ได้รับข้อมูลเชิงลึกมากเท่าที่ควร

จากผลการวิจัยพบว่าปัจจัยการรับรู้จุดอ่อน ปัจจัยการรับรู้ความสามารถของตนเอง และปัจจัยค่าใช้จ่ายในการตอบสนอง ไม่มีอิทธิพลต่อความตั้งใจในการรับมือกับภัยคุกคามดังนั้นหากจะทำงานวิจัยในอนาคตสามารถนำข้อมูลไปประกอบการวิจัยบริบทอื่นๆ ที่เกี่ยวข้องกันได้ เช่น กลุ่มตัวอย่างในมุมมองของผู้ใช้งานระบบ เป็นต้น นอกจากนี้การวิจัยครั้งนี้พบว่า ตัวแปรอิสระความตระหนักถึงความปลอดภัย ปัจจัยการรับรู้ถึงความรุนแรง ปัจจัยความคาดหวังในประสิทธิผลของการตอบสนอง และปัจจัยการรับมือภัยคุกคามด้วยการติดตั้งการควบคุมบนระบบ ERP ค่าสัมประสิทธิ์แอลฟาของครอนบาค ที่ต่ำกว่า 0.7 แต่ยังคงมีความน่าเชื่อถือในระดับปานกลาง จึงควรพิจารณาข้อคำถามให้เหมาะสมกับบริบทกลุ่มตัวอย่าง และการวิจัยครั้งนี้ พบว่า ตัวแปรอิสระ ได้แก่การรับรู้จุดอ่อน ปัจจัยด้านความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศมีความสัมพันธ์กับตัวแปรตามความตระหนัก โดยมีความผันแปรของตัวแปรตาม (R^2) ค่อนข้างน้อยซึ่งเท่ากับร้อยละ 20.3 (R^2 = 0.203) จึงควรศึกษาว่ามีปัจจัยใดอีกบ้างที่ส่งผลต่อ ความตระหนัก อีกทั้งยังสามารถนำกรอบแนวคิดของงานวิจัยมาทำการศึกษาปัจจัยอื่นๆ เพิ่มเติมจากปัจจัยที่ยังไม่ได้ศึกษาในงานวิจัยนี้ เช่นปัจจัย อิทธิพลจากสภาพแวดล้อม รวมไปถึงกรอบแนวคิดของ Boss et al. (2015) ที่ไม่ได้นำมาใช้ในงานวิจัยนี้ เพื่อต่อยอดงานวิจัยและนำมาประยุกต์ใช้ได้อย่างเหมาะสม เพื่อให้ได้กรอบแนวคิดที่มีความสมบูรณ์และมีประสิทธิผลมากยิ่งขึ้นในอนาคต ซึ่งจะช่วยเพิ่มความเข้าใจต่อพฤติกรรมการติดตั้งการควบคุมในระบบการบริหารทรัพยากรขององค์กร สำหรับธุรกิจขนาดกลางและขนาดย่อมหรือทำการต่อยอดด้วยการสัมภาษณ์เชิงลึก (In-depth Interview) เพื่อให้ทราบถึงการติดตั้งการควบคุมในเชิงลึกมากยิ่งขึ้น

บรรณานุกรม

คิวเอดี. (ม.ป.ป.). *ERP คืออะไรและเหตุใดองค์กรจึงจำเป็นต้องใช้.* สืบค้นเมื่อวันที่ 1 พฤศจิกายน 2564, จาก https://www.qad.com/th-TH/what-is-erp.

ณชญาภัส รอดประยูร. (2560). การเตรียมความพร้อมก่อนการตัดสินใจนำระบบการวางแผนทรัพยากรในองค์กรมาใช้สำหรับธุรกิจขนาดกลางและขนาดย่อมในเขตกรุงเทพมหานคร. *วารสารบัณฑิตศึกษา มหาวิทยาลัยราชภัฏวไลยอลงกรณ์ ในพระบรมราชูปถัมภ์, 11*(พิเศษ), 41-53.

ดิจิทเดย์. (28 กันยายน 2564). *Cisco เผยรายงาน SME ไทยกว่า 76% สูญเสียข้อมูลลูกค้าจากการถูกโจมตีทางไซเบอร์.* https://www.digitday.com/cisco-reports-76-of-thai-SMEs-losing-customer-data-from-cyber-attacks/.

สำนักงานราชบัณฑิตยสภา (ม.ป.ป.). *พจนานุกรม ฉบับราชบัณฑิตยสถาน 2554.* สืบค้นเมื่อวันที่ 1 พฤศจิกายน 2564, จาก https://dictionary.orst.go.th/.

สำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม (สสว.). (ม.ป.ป.). *ภาพรวม SME แยกรายจังหวัด หรืออุตสาหกรรม*. สืบค้นเมื่อวันที่ 1 พฤศจิกายน 2564, จาก https://sme.go.th/th/page.php?modulekey=468.

นิตยา วงศ์ภินันท์วัฒนา. (2563). *ความมั่นคงปลอดภัยและการควบคุมระบบสารสนเทศ* (พิมพ์ครั้งที่ 2). กรุงเทพฯ: สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์.

Al-Saqer, N. S., & Seliaman, M. E. (2016). The Impact of Privacy Concerns and Perceived Vulnerability to Risks on Users Privacy Protection Behaviors on SNS: A Structural Equation Model. *International Journal of Advanced Computer Science and Applications, 7*(5), 142-147.

Bandura, A. (1982). Self-efficacy mechanism in human agency. *American psychologist, 37*(2), 122.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS quarterly, 39*(4), 837-864.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 523-548.

Ciampa, M. (2005). Security+ Guide to Network Security Fundamentals Second. *Thomson Course Technology*.

Chou, H.-L., & Chou, C. (2016). An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in human behavior, 65*, 334-345.

ENISA. (2020). *SME Cybersecurity*. Retrieved 24 November, 2020, from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/sme_cybersecurity.

Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security, 43*, 90-110.

Good, C. V., & Merkel, W. R. (1973). *Dictionary of education*. McGraw-Hill.

Gusti, A. (2016). The relationship of knowledge, attitudes, and behavioral intentions of sustainable waste management on primary school students in city of Padang, Indonesia. *International Journal of Applied Environmental Sciences, 11*(5), 1323-1332.

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

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS quarterly*, 549-566.

Klein, R. H., & Luciano, E. M. (2016). What influences information security behavior? A study with Brazilian users. *JISTEM-Journal of Information Systems and Technology Management, 13*, 479-496.

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems, 18*(2), 177-187.

Mejias, R. J. (2012). An integrative model of information security awareness for assessing information systems security risk. *Hawaii International Conference on System Sciences, 45*, 3258-3267.

Romney, M., Steinbart, P., Mula, J., McNamara, R., & Tonkin, T. (2012). *Accounting Information Systems Australasian Edition*. Pearson Higher Education AU.

Weiss, S. (2009). Privacy threat model for data portability in social network applications. *International journal of information management, 29*(4), 249-254.

Williams, C. K., Wynn, D., Madupalli, R., Karahanna, E., & Duncan, B. K. (2014). Explaining users' security behaviors with the security belief model. *Journal of Organizational and End User Computing (JOEUC), 26*(3), 23-46.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in human behavior, 24*(6), 2799-2816.

Yoon, C., Hwang, J. W., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of information systems education, 23*(4), 407-416.