ปัจจัยที่กำหนดพฤติกรรมในการรับมือกับภัยคุกคามทางคอมพิวเตอร์ต่อการสูญเสียและถูกโจรกรรมข้อมูลทางการเงิน กรณีศึกษาโปรแกรมทางการบัญชีสำหรับธุรกิจขนาดเล็ก

อนุกูล นพคุณเจริญชัย*
บริษัท โชติธนวัฒน์ จำกัด (เครือ เค.กรุ๊ป)
นิตยา วงศ์ภินันท์วัฒนา
คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
สุรัตน์ โคอินทรางกูร
คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์

***Correspondence:** voyage.luckky@gmail.com
doi: 10.14456/jisb.2019.9
วันที่รับบทความ: 2 พ.ค. 2562 วันแก้ไขบทความ: 10 พ.ค. 2562 วันตอบรับบทความ: 16 พ.ค. 2562

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาปัจจัยที่กำหนดพฤติกรรมในการรับมือกับภัยคุกคามทางคอมพิวเตอร์ของโปรแกรมทางการบัญชีสำหรับธุรกิจขนาดเล็ก ซึ่งเป็นงานวิจัยเชิงปริมาณที่ศึกษากับกลุ่มตัวอย่างที่เป็นพนักงานของธุรกิจที่นำโปรแกรมทางการบัญชีสำหรับธุรกิจขนาดเล็กมาใช้งานจำนวน 167 ตัวอย่าง ผลการวิจัยพบว่า การรับรู้ถึงความรุนแรง การรับรู้ความสามารถของตนเอง การรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัว และแรงจูงใจในการเรียนรู้ทางสังคม ส่งอิทธิพลทางตรงต่อความตั้งใจในการรับมือกับภัยคุกคามและส่งอิทธิพลทางอ้อมต่อพฤติกรรมในการรับมือกับภัยคุกคาม แต่การรับรู้จุดอ่อน ความเชื่อเกี่ยวกับอำนาจควบคุม และการรับรู้ค่าใช้จ่ายจากการใช้เครื่องมือป้องกันภัยคุกคาม ไม่ส่งผลต่อความตั้งใจในการรับมือกับภัยคุกคาม นอกจากนี้ความตั้งใจในการรับมือกับภัยคุกคามและความตระหนักส่งอิทธิพลทางตรงต่อพฤติกรรมในการรับมือกับภัยคุกคาม

คำสำคัญ: การสูญเสียและถูกโจรกรรมข้อมูลทางการเงิน โปรแกรมทางการบัญชีสำหรับธุรกิจขนาดเล็ก ความตั้งใจในการรับมือกับภัยคุกคาม พฤติกรรมในการรับมือกับภัยคุกคาม

Factors that determine behavior in dealing with computer threats against loss and theft of financial information: Case studies of accounting programs for small business

Anukoon Noppakhuncharoenchai*

Chodthanawat Co.,Ltd. (K.Group Network)

Nitaya Wongpinunwatana

Thammasat Business School, Thammasat University

Surat Kointrangkul

Thammasat Business School, Thammasat University

***Correspondence:** voyage.luckky@gmail.com

doi: 10.14456/jisb.2019.9

Received: 2 May 2019 Revised: 10 May 2019 Accepted: 16 May 2019

Abstract

The objective of this study is to examine the factors influencing behavior in dealing with computer threats. This research is quantitative research. The data was collected from 167 participants, working in small business and have experience in using accounting software. The results of this research indicate that perceived severity, self-efficacy, perceived effectiveness, and social learning of motivation directly affect intention to deal with threats and also indirectly affect behavior in dealing with threats. However, perceived vulnerability, locus of control, and perceived cost do not affect intention to deal with treats. In addition, participants intend to follow and aware of deal with threats will directly affect to behavior in dealing with threats.

Keywords: Loss and theft of financial information, accounting software for small businesses, intention to deal with threats, behavior in dealing with threats

1. บทนำ

1.1 ความสำคัญและที่มาของปัญหา

ความก้าวหน้าทางเทคโนโลยีสารสนเทศส่งผลให้ธุรกิจต่างๆ นำเทคโนโลยีสารสนเทศมาช่วยในการดำเนินงานของธุรกิจมากขึ้น ปัจจุบันธุรกิจจำนวนมากหันมาใช้โปรแกรมทางการบัญชี เพื่อจัดเก็บข้อมูล และจัดทำรายงานทางการเงิน ซึ่งประกอบด้วย งบแสดงฐานะทางการเงิน งบกำไรขาดทุนเบ็ดเสร็จ งบกระแสเงินสด งบแสดงการเปลี่ยนแปลงส่วนของผู้ถือหุ้น และหมายเหตุประกอบงบการเงิน โดยโปรแกรมทางการบัญชีทำให้การจัดทำบัญชีมีประสิทธิภาพ มีความน่าเชื่อถือ และมีความถูกต้องตามมาตรฐานทางการบัญชี จะเห็นได้ว่าธุรกิจขนาดเล็กนำโปรแกรมทางบัญชี เช่น โปรแกรม Formula, Express, MyAccount, EasyWin, Daccount เป็นต้น ปกติโปรแกรมทางการบัญชีดังกล่าวมักจะถูกติดตั้งที่เครื่องไมโครคอมพิวเตอร์ซึ่งอาจถูกใช้โดยบุคคลเพียงคนเดียวหรือหลายคนแต่ต่างเวลาเพื่อใช้งานโปรแกรมทางการบัญชี เช่น ป้อนข้อมูลและประมวลผลโปรแกรมทางการบัญชี เป็นต้น เนื่องจากเครื่องไมโครคอมพิวเตอร์อาจถูกนำมาใช้ในลักษณะที่แตกต่างจากเทคโนโลยีสารสนเทศที่นำมาใช้โดยทั่วไป ดังนั้นการควบคุมและการรักษาความมั่นคงปลอดภัยซึ่งใช้กับเครื่องคอมพิวเตอร์ขนาดใหญ่อาจไม่เหมาะสมกับเครื่องไมโครคอมพิวเตอร์ นอกจากนี้การควบคุมบางประเภทยังอาจเหมาะสมมากกว่า เนื่องจากลักษณะของเครื่องไมโครคอมพิวเตอร์ที่มีลักษณะเล็กซึ่งเคลื่อนย้ายและติดตั้งเพื่อปฏิบัติงานได้สะดวก นอกจากนี้ผู้ใช้ที่มีทักษะพื้นฐานทางคอมพิวเตอร์สามารถเรียนรู้เพื่อใช้งานคอมพิวเตอร์ได้ง่ายเนื่องจากโปรแกรมระบบและโปรแกรมทางการบัญชีมีลักษณะง่ายต่อการใช้งานและมีคำสั่งเป็นขั้นเป็นตอน นอกจากนี้โปรแกรมระบบของเครื่องไมโครคอมพิวเตอร์ยังมีความซับซ้อนที่น้อยกว่าเครื่องคอมพิวเตอร์ขนาดใหญ่ ทำให้เครื่องไมโครคอมพิวเตอร์อาจมีระบบควบคุมน้อยกว่าเครื่องคอมพิวเตอร์ขนาดใหญ่

แม้ว่าโปรแกรมทางการบัญชีจะก่อให้เกิดความสะดวกสบาย เพิ่มประสิทธิภาพ และประสิทธิผลในการจัดทำรายงานทางการเงินดังกล่าวมาแล้วข้างต้นก็ตาม โปรแกรมทางการบัญชีก็มีความเสี่ยงทางด้านคอมพิวเตอร์ เช่น การปรับเปลี่ยน การสูญหาย และการถูกโจรกรรมข้อมูลทางการเงิน เป็นต้น เนื่องจากโปรแกรมทางการบัญชีสำหรับธุรกิจขนาดเล็กมักจะไม่มีการรักษาความมั่นคงปลอดภัยน้อยกว่าโปรแกรมทางการบัญชีสำหรับธุรกิจขนาดกลางและขนาดใหญ่ เช่น การกำหนดรหัสผ่าน และการกำหนดระดับชั้นของผู้ใช้งาน เป็นต้น นอกจากนี้ยังมีภัยคุกคามใหม่ๆ ทางด้านคอมพิวเตอร์เกิดขึ้นใหม่อยู่เสมอ ดังนั้นงานวิจัยนี้จะเน้นศึกษาพฤติกรรมของผู้ใช้ว่ามีการป้องกันหรือใช้เครื่องมือที่ช่วยป้องกันไม่ให้ผู้อื่นสามารถเข้าถึงข้อมูลโปรแกรมทางการบัญชีโดยเน้นที่โปรแกรมทางการบัญชีสำหรับธุรกิจขนาดเล็กเป็นหลัก

1.2 วัตถุประสงค์ของการวิจัย

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาถึงปัจจัยต่างๆ ที่ส่งผลต่อกำหนดพฤติกรรมในการรับมือกับภัยคุกคามทางคอมพิวเตอร์สำหรับธุรกิจขนาดเล็ก ประกอบด้วย การรับรู้จุดอ่อน การรับรู้ความรุนแรง ความเชื่อเกี่ยวกับอำนาจการควบคุม การรับรู้ความสามารถของตนเอง การรับรู้ค่าใช้จ่ายจากการใช้เครื่องมือป้องกันภัยคุกคาม การรับรู้ประสิทธิผลในการป้องกันความเป็นส่วนตัว และแรงจูงใจในการเรียนรู้ทางสังคม ความตระหนักถึงการรับมือกับภัยคุกคามต่อการสูญเสียและถูกโจรกรรมข้อมูลทางการเงิน

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

จากการศึกษาทฤษฎีทางจิตวิทยาสังคม (Social psychology) ได้แก่ ทฤษฎีสัจนิยมคลาสสิกแนวใหม่ ทฤษฎีความรู้ความเข้าใจ ทฤษฎีแรงจูงใจในการเรียนรู้ทางสังคม ทฤษฎีพฤติกรรมตามแผน หรือทฤษฎีความตั้งใจเชิงพฤติกรรม ทฤษฎีความตระหนัก และงานวิจัยในอดีตที่เกี่ยวข้องสามารถสรุปปัจจัยที่เกี่ยวข้องกับการศึกษาได้ดังนี้

การรับรู้ถึงจุดอ่อน (Perceived vulnerability) คือ การที่ผู้ใช้งานโปรแกรมทางการบัญชีทราบว่าโปรแกรมทางการบัญชีมีช่องโหว่ที่อาจเป็นอันตรายต่อข้อมูลทางการบัญชี โดยโปรแกรมทางการบัญชีไม่สามารถรับมือกับภัยที่อาจเกิดขึ้นได้จึงเกิดช่องโหว่ซึ่งส่งผลให้ข้อมูลทางการเงินที่จัดเก็บในโปรแกรมทางการบัญชีถูกปรับเปลี่ยน สูญหาย หรือถูกโจรกรรมได้ (McCarthy et al., 2001)

การรับรู้ถึงความรุนแรง (Perceived severity) คือ การที่ผู้ใช้งานโปรแกรมทางการบัญชีเชื่อว่าภัยทางคอมพิวเตอร์จะส่งผลต่อระดับความถูกต้องของข้อมูลที่แตกต่างกันออกไป โดยผู้ใช้จะกำหนดว่าภัยคุกคามใดต้องใช้วิธีการยับยั้งความเสียหายที่อาจเกิดขึ้นใด (Davison, 1983)

ความเชื่อเกี่ยวกับอำนาจควบคุม (Locus of control) คือ การที่ผู้ใช้งานโปรแกรมทางการบัญชีเชื่อว่าตนเองสามารถควบคุมฟังก์ชันการใช้งานในโปรแกรมทางการบัญชีเพื่อยับยั้งไม่ให้เกิดความรุนแรงต่อข้อมูลที่จัดเก็บในโปรแกรมทางการบัญชีได้ (Rotter, 1975; Lefcourt, 1976 & 1981)

การรับรู้ความสามารถของตนเอง (Self-efficacy) คือ การที่ผู้ใช้งานโปรแกรมทางการบัญชีเชื่อว่าตนเป็นผู้กำหนดการใช้เครื่องมือทางการบัญชีได้ด้วยตนเอง โดยผู้ใช้งานมีระดับความเชี่ยวชาญเพียงพอที่สามารถประเมินและสอบทานข้อผิดพลาดได้ด้วยตนเอง (นิตยา วงศ์ภินันท์วัฒนา, 2561) ซึ่งถือเป็นการรับรู้ความสามารถที่มีอยู่ภายในตนต่อการปฏิบัติหน้าที่บนพื้นฐานตามที่กำหนดไว้ เพื่อเป็นการหลีกเลี่ยงภัยคุกคามที่อาจเกิดขึ้นต่อโปรแกรมทางการบัญชี (Bandura, 1977)

การรับรู้ค่าใช้จ่ายจากการใช้เครื่องมือป้องกันภัยคุกคาม (Perceived cost) คือ การที่ผู้ใช้งานโปรแกรมทางการบัญชีเชื่อว่าค่าใช้จ่ายโดยเฉพาะค่าบำรุงรักษา (Maintenance) ซอฟต์แวร์ให้มีความทันสมัยอยู่เสมอเพื่อปิดช่องว่างไม่ให้การโจมตีจากภัยคุกคามเข้าสู่โปรแกรมทางการบัญชีได้ (Liang & Xue, 2009; Lee & Larsen, 2009) นับเป็นสิ่งที่มีความสำคัญต่อการป้องกันภัยคุกคาม กล่าวคือจะช่วยให้เกิดความมั่นคงปลอดภัยต่อระบบคอมพิวเตอร์หรือซอฟต์แวร์ ซึ่งจะส่งผลกระทบทางอ้อมต่อข้อมูลภายในโปรแกรมทางการบัญชี

การรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัว (Perceived effectiveness) คือ การที่ผู้ใช้งานโปรแกรมทางการบัญชีเชื่อว่ามาตรการหลีกเลี่ยงภัยคุกคามที่มีประสิทธิผลเกิดจากมาตรการรักษาความมั่นคงปลอดภัยที่กำหนดไว้ เช่น การตั้งรหัสเข้าโปรแกรมทางการบัญชีที่มีความซับซ้อนเพียงพอเพื่อมิให้ผู้อื่นเข้าถึงข้อมูลที่ถูกบันทึกบนโปรแกรมทางการบัญชีมีความเป็นส่วนตัว เป็นต้น ซึ่งช่วยลดภัยคุกคามที่อาจเข้าถึงความเป็นส่วนตัวได้ (Bandura, 1982; Rogers, 1975)

แรงจูงใจในการเรียนรู้ทางสังคม (Social learning of motivation) คือ การที่ผู้ใช้งานโปรแกรมทางการบัญชีเชื่อว่าตนมีความเชื่อเกี่ยวกับอำนาจควบคุม รับรู้ถึงความสามารถของตนเอง และรับรู้ถึงประสิทธิผลในการป้องกันความเป็นส่วนตัวบุคคล โดยพื้นฐานของบุคคลนั้นเกิดจากความสนใจ หรือมีบุคคลต้นแบบคอยให้คำแนะนำเกี่ยวกับวิธีการป้องกันภัยคุกคามแล้วถ่ายทอดวิธีการนั้นออกมาโดยเกิดเป็นแรงจูงใจให้บุคคลนั้นเกิดความสนใจในการเรียนรู้ (Bandura, 1977)

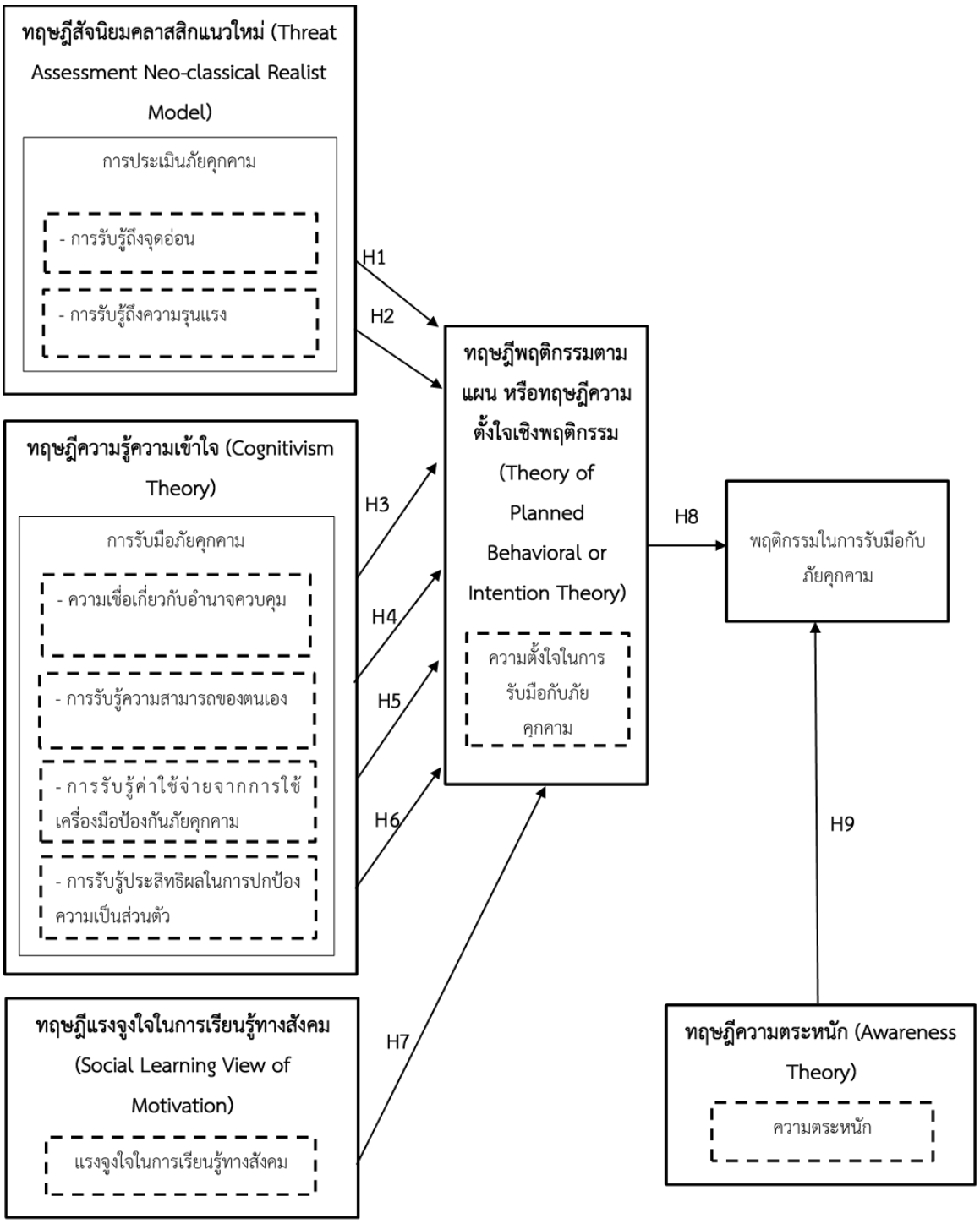
ความตั้งใจในการรับมือกับภัยคุกคาม (Behavior intention) คือ การที่ผู้ใช้งานบนโปรแกรมทางการบัญชีแสดงออกถึงความต้องการ มุ่งมั่น ที่จะรับมือกับภัยคุกคามบนโปรแกรมทางการบัญชีอย่างเหมาะสม (สำนักงานราชบัณฑิตยสภา, 2554) โดยความตั้งใจนั้นถือเป็นเครื่องชี้วัดว่าผู้ใช้โปรแกรมทางการบัญชีแสดงออกถึงวิธีการหลีกเลี่ยงภัยคุกคามซึ่งความตั้งใจสอดคล้องกับพฤติกรรมที่บุคคลตั้งไว้ตามวัตถุประสงค์ (Lee & Larsen, 2009)

ความตระหนัก (Awareness) คือ การที่ผู้ใช้งานบนโปรแกรมทางการบัญชีแสดงออกทางความคิดเห็น โดยบุคคลนั้นมีความรู้ความเข้าใจจากการใช้งาน รวมถึงการสะสมประสบการณ์ในอดีต และเมื่อเกิดภัยคุกคามที่ส่งผลกระทบต่อโปรแกรมทางการบัญชีบุคคลนั้นจะเกิดความตระหนักและหาวิธีการมารับมือกับภัยคุกคามได้อย่างถูกต้องเหมาะสม (Good, 1973; Koffka, 1973)

พฤติกรรมในการรับมือกับภัยคุกคาม (Threat coping behavioral) คือ การที่ผู้ใช้งานบนโปรแกรมทางการบัญชีแสดงออกเชิงพฤติกรรมในการรับมือกับภัยคุกคาม เพื่อหลีกเลี่ยงผลกระทบที่ก่อให้เกิดความรุนแรงต่อโปรแกรมทางการบัญชีโดยบุคคลนั้นพึงต้องปฏิบัติตามนโยบายด้านการใช้งานที่องค์กรจัดไว้ให้อย่างเคร่งครัด ดังนั้นพฤติกรรมในการรับมือกับภัยคุกคามมีส่วนช่วยบรรเทาความเสียหายที่อาจเกิดขึ้นต่อโปรแกรมทางการบัญชี (ธวัชชัย ชมศิริ, 2553)

3. กรอบแนวคิดการวิจัยและสมมติฐานการวิจัย

การวิจัยนี้ได้ประยุกต์ใช้ทฤษฎีสัจนิยมคลาสสิกแนวใหม่ ทฤษฎีความรู้ความเข้าใจ ทฤษฎีแรงจูงใจในการเรียนรู้ทางสังคม ทฤษฎีพฤติกรรมตามแผน หรือทฤษฎีความตั้งใจเชิงพฤติกรรม ทฤษฎีความตระหนัก และงานวิจัยในอดีตที่เกี่ยวข้อง เพื่อใช้เป็นกรอบการศึกษาเพื่อหาคำตอบของการวิจัยดังแสดงในภาพที่ 1



ภาพที่ 1 กรอบแนวคิดการวิจัยพฤติกรรมในการรับมือกับภัยคุกคามทางคอมพิวเตอร์ต่อการสูญเสียและถูกโจรกรรมข้อมูลทางการเงิน

Lee and Larsen (2009) แสดงให้เห็นว่า เมื่อบุคคลรับรู้ว่าเทคโนโลยีสารสนเทศที่ใช้งานมีจุดอ่อน หรือช่องว่างที่ก่อให้เกิดการรั่วไหลหรือสูญเสียหรือถูกโจรกรรมข้อมูลจากบุคคลภายนอกได้ บุคคลนั้นมีความตั้งใจในการรับมือกับภัยคุกคามมากขึ้น จึงนำไปสู่สมมติฐานในการวิจัยดังนี้

Hypothesis 1: การรับรู้ถึงจุดอ่อนส่งผลเชิงบวกต่อความตั้งใจในการรับมือกับภัยคุกคาม

Workman et al. (2008) แสดงให้เห็นว่า การที่บุคคลรับรู้ว่าเทคโนโลยีสารสนเทศที่ใช้งานมีระดับความรุนแรงที่อาจก่อให้เกิดการสูญเสียหรือถูกโจรกรรมข้อมูล บุคคลดังกล่าวจะกำหนดขอบเขตระดับความรุนแรงเพื่อยับยั้งความเสียหายที่อาจเกิดขึ้น บุคคลนั้นมีความตั้งใจในการรับมือกับภัยคุกคามมากขึ้น จึงนำไปสู่สมมติฐานในการวิจัยดังนี้

Hypothesis 2: การรับรู้ถึงความรุนแรงส่งผลเชิงบวกต่อความตั้งใจในการรับมือกับภัยคุกคาม

Rotter (1966) แสดงให้เห็นว่า การที่บุคคลมีความเชื่อเกี่ยวกับอำนาจควบคุมของตนเองจะส่งผลต่อการดำเนินการควบคุมฟังก์ชันของระบบงานที่ใช้งาน เช่น การควบคุมมิให้มีการเปลี่ยนแปลงแก้ไขข้อมูลที่สำคัญบนโปรแกรมทางการบัญชี รวมถึงการควบคุมการเข้าถึงระบบโดยการพิสูจน์ตัวตน การควบคุมสิทธิการเข้าใช้งานบนโปรแกรมทางการบัญชี เป็นต้น ซึ่งจะช่วยลดระดับความเสียหายที่อาจเกิดกับโปรแกรมได้ จึงนำไปสู่สมมติฐานในการวิจัยดังนี้

Hypothesis 3: การรับรู้ความเชื่อเกี่ยวกับอำนาจควบคุมส่งผลเชิงบวกต่อความตั้งใจในการรับมือกับภัยคุกคาม

Lee and Larsen (2009) แสดงให้เห็นว่า เมื่อบุคคลรับรู้ความสามารถในการใช้เครื่องมือป้องกันภัยคุกคามบนเทคโนโลยีสารสนเทศ บุคคลนั้นมีความตั้งใจในการรับมือกับภัยคุกคามมากขึ้น จึงนำไปสู่สมมติฐานในการวิจัยดังนี้

Hypothesis 4: การรับรู้ความสามารถของตนเองส่งผลเชิงบวกต่อความตั้งใจในการรับมือกับภัยคุกคาม

Bandura (1982) และ Herath and Rao (2010) แสดงให้เห็นว่า เมื่อบุคคลรับรู้ว่าเทคโนโลยีสารสนเทศที่ใช้งานมีมาตรการรักษาความมั่นคงปลอดภัยที่มีประสิทธิภาพและไว้วางใจได้ จะส่งผลให้ผู้ใช้งานโปรแกรมทางการบัญชีสามารถหลีกเลี่ยงภัยคุกคามที่อาจส่งผลต่อความเป็นส่วนตัวได้ และบุคคลนั้นจะมีความตั้งใจในการรับมือกับภัยคุกคามมากขึ้น จึงนำไปสู่สมมติฐานในการวิจัยดังนี้

Hypothesis 5: การรับรู้ประสิทธิผลในการป้องกันความเป็นส่วนตัวส่งผลเชิงบวกต่อความตั้งใจในการรับมือกับภัยคุกคาม

Workman et al. (2008) แสดงให้เห็นว่า เมื่อบุคคลรับรู้ว่าค่าใช้จ่ายที่เสียไปคุ้มค่ากับความเสียหายที่อาจเกิดกับเทคโนโลยีสารสนเทศ บุคคลนั้นจะมีความตั้งใจในการรับมือกับภัยคุกคามมากขึ้น จึงนำไปสู่สมมติฐานในการวิจัยดังนี้

Hypothesis 6: การรับรู้ค่าใช้จ่ายจากการใช้เครื่องมือป้องกันภัยคุกคามส่งผลเชิงบวกต่อความตั้งใจในการรับมือกับภัยคุกคาม

Liang and Xue (2009) แสดงให้เห็นว่า เมื่อบุคคลปรับเปลี่ยนพฤติกรรมในการหลีกเลี่ยงภัยคุกคามเพื่อสกัดกั้นไม่ให้ภัยคุกคามภายนอกเข้ามาคุกคามโปรแกรมทางการบัญชี บุคคลนั้นจะมีความตั้งใจในการรับมือกับภัยคุกคามมากขึ้น จึงนำไปสู่สมมติฐานในการวิจัยดังนี้

Hypothesis 7: แรงจูงใจในการเรียนรู้ทางสังคมส่งผลเชิงบวกต่อความตั้งใจในการรับมือกับภัยคุกคาม

Beaudry and Pinsonneault (2005) แสดงให้เห็นว่า เมื่อบุคคลรับรู้ว่าเทคโนโลยีสารสนเทศที่ใช้งานมีมาตรการรักษาความมั่นคงปลอดภัยเพื่อรับมือกับภัยคุกคามที่อาจเกิดขึ้น รวมทั้งมีการจัดการกับปัญหา บุคคลนั้นจะมีความตั้งใจในการรับมือกับภัยคุกคามมากขึ้น จึงนำไปสู่สมมติฐานในการวิจัยดังนี้

Hypothesis 8: ความตั้งใจในการรับมือกับภัยคุกคามส่งผลเชิงบวกต่อพฤติกรรมในการรับมือกับภัยคุกคาม

Humaidi and Balakrishnan (2012) แสดงให้เห็นว่า เมื่อบุคคลมีความตระหนักถึงภัยคุกคามที่เกิดขึ้นกับโปรแกรมทางการบัญชี บุคคลนั้นจะติดตามและเฝ้าระวังอย่างต่อเนื่องเพื่อให้การรับมือกับภัยคุกคามมีประสิทธิภาพและครอบคลุมมากยิ่งขึ้น จึงนำไปสู่สมมติฐานในการวิจัยดังนี้

Hypothesis 9: ความตระหนักส่งผลเชิงบวกต่อพฤติกรรมในการรับมือกับภัยคุกคาม

4. วิธีการวิจัย

งานวิจัยนี้จัดเก็บข้อมูลจากพนักงานของหน่วยงานเอกชน ตลอดจนธุรกิจที่เกี่ยวข้องกับการใช้โปรแกรมทางการบัญชีและสามารถนำมาวิเคราะห์ผลทางสถิติได้จำนวน 167 ตัวอย่าง ด้วยแบบสอบถามในรูปแบบอิเล็กทรอนิกส์และรูปแบบกระดาษ ซึ่งจัดสร้างขึ้นมาจากงานวิจัยที่เกี่ยวข้อง (ประกอบด้วย Lee and Larsen, 2009; Workman et al., 2008; Rotter, 1966; Bandura, 1982; Herath and Rao, 2010; Liang and Xue, 2009; Beaudry and Pinsonneault, 2005; Humaidi and Balakrishnan, 2012) โดยคณะผู้วิจัยจัดเก็บข้อมูลผ่านทางออนไลน์และผู้เข้ารับการอบรมที่สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์

5. ผลการวิจัย

5.1 การทดสอบข้อตกลงเบื้องต้นทางสถิติ

ข้อมูลที่จัดเก็บจากกลุ่มตัวอย่างถูกนำไปทดสอบข้อมูลขาดหาย (Missing data) ข้อมูลสุดโต่ง (Outliners) และการสอบทานการกระจายข้อมูล (Frequencies) พบว่าไม่มีข้อมูลใดขาดหาย และมีตัวแปรบางตัวแปรที่ไม่มีการกระจ่ายค่าแบบปกติ อีกทั้งมีการกระจายตัวของข้อมูลแบบเบ้ซ้ายหรือเบ้ทางด้านลบเพียงเล็กน้อยโดยความเบ้ไม่ต่างจากเกณฑ์มาตรฐานมากนัก นอกจากนี้ข้อมูลดังกล่าวยังมีค่า Skewness หารค่า Standard Error of Skewness ระหว่าง -3 ถึง +3 ดังนั้นผู้วิจัยจึงยังคงใช้ข้อมูลดังกล่าวมาวิเคราะห์ข้อมูลทางสถิติต่อไป

5.2 การประเมินความเที่ยงและความตรงของแบบสอบถาม

งานวิจัยนี้ได้ตรวจสอบความเที่ยงของแบบสอบถามด้วยค่าสัมประสิทธิ์แอลฟาของครอนบาซ (Cronbach's alpha) พบว่าทุกตัวแปรมีค่ามากกว่าหรือเท่ากับ 0.60 จึงถือว่ามีความเชื่อถือได้สำหรับงานวิจัยแบบ Basic research (Hair et al., 1998) นอกจากนี้ยังได้ทดสอบความตรงของแบบสอบถามด้วยการวิเคราะห์องค์ประกอบ (Factor analysis) โดยใช้เกณฑ์ที่ข้อคำถามที่จับกลุ่มกันเป็นแต่ละตัวแปรต้องมีค่า Factor loading ไม่น้อยกว่า 0.5 ผลการวิเคราะห์องค์ประกอบได้จำนวนปัจจัยทั้งหมด 10 องค์ประกอบและผ่านเกณฑ์ที่กำหนดไว้ ดังแสดงในตารางที่ 1

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน น้ำหนักองค์ประกอบและค่าสัมประสิทธิ์แอลฟา ของครอนบาซของตัวแปรทั้งหมด

ปัจจัย	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	น้ำหนักองค์ประกอบ
ปัจจัยที่ 1: การรับรู้ถึงจุดอ่อน (% of Variance = 22.05%, Cronbach's alpha = 0.859)			
โปรแกรมทางการบัญชีของท่านอาจมีจุดอ่อนที่จะถูกภัยคุกคาม เช่น ข้อมูลนำเข้าโปรแกรมทางการบัญชีโดยไม่ได้รับอนุมัติ ไม่ถูกต้องครบถ้วนก่อให้เกิดปัญหาข้อมูลไม่ครบถ้วน เป็นต้น	2.93	0.954	0.817
ท่านเชื่อว่าโปรแกรมทางการบัญชีที่ท่านใช้อาจมีความเสี่ยงต่อการถูกโจรกรรมข้อมูลทางการเงิน	2.90	0.952	0.866
ท่านรู้สึกว่าโปรแกรมทางการบัญชีมีช่องโหว่ที่อาจถูกภัยคุกคามที่ส่งผลต่อความมั่นคงด้านข้อมูลทางการเงินของท่าน	2.94	0.968	0.881
ปัจจัยที่ 2: การรับรู้ถึงความรุนแรง (% of Variance = 10.05%, Cronbach's alpha = 0.768)			
ท่านคิดว่าการขาดมาตรการการป้องกันภัยคุกคามที่ดีจะทำให้ภัยคุกคามทาง Cyber สามารถเข้าถึงข้อมูลผ่านโปรแกรมทางการบัญชีที่ท่านใช้งานได้	3.92	0.817	0.620
ท่านคิดว่าสปายแวร์หรือไวรัส สามารถเข้าถึงโปรแกรมทางการบัญชีได้และจะส่งผลกระทบต่อความถูกต้องของข้อมูลการบัญชีและการเงิน	3.82	0.940	0.687
ท่านมีความกังวลต่อพฤติกรรมของผู้ใช้งานที่ไม่มีความเคร่งครัดกับการรักษาความมั่นคงปลอดภัยในการใช้โปรแกรมทางการบัญชี	3.78	0.947	0.802
ความหวาดกลัวทำให้ท่านเกิดความวิตกกังวลและรับรู้ถึงความรุนแรงของภัยคุกคามที่อาจมีกับโปรแกรมทางการบัญชี	3.44	0.929	0.751
ปัจจัยที่ 3: ความเชื่อเกี่ยวกับอำนาจควบคุม (% of Variance = 7.23%, Cronbach's alpha = 0.571)			
ท่านเชื่อมั่นว่าโปรแกรมทางการบัญชีที่ใช้งานในปัจจุบันมีการป้องกันภัยคุกคามได้เป็นอย่างดีแล้ว	3.31	0.797	0.760
ท่านคิดว่าพนักงานทุกคนปฏิบัติงานตามมาตรการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์อย่างเคร่งครัด	3.34	0.882	0.790

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน น้ำหนักองค์ประกอบและค่าสัมประสิทธิ์แอลฟา ของครอนบาซของตัวแปรทั้งหมด (ต่อ)

ปัจจัย	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	น้ำหนักองค์ประกอบ
ปัจจัยที่ 4: การรับรู้ความสามารถของตนเอง (% of Variance = 6.58%, Cronbach's alpha = 0.790)			
ท่านมั่นใจว่าตนเองมีทักษะในการปกป้องโปรแกรมทางการบัญชีจากภัยคุกคามได้ตามนโยบายที่กำหนดไว้ในคู่มือการปฏิบัติงาน	3.38	0.758	0.708
ท่านมีความเชี่ยวชาญเพียงพอที่จะสามารถประเมินความเหมาะสมของการจัดการกับข้อผิดพลาดเพื่อป้องกันภัยคุกคามในโปรแกรมทางการบัญชี	3.03	0.846	0.752
ท่านคิดว่าท่านมีความสามารถในการสอบทานข้อมูลทางการเงินอย่างสมเหตุสมผลก่อนนำไปคีย์บนโปรแกรมทางการบัญชี	3.78	0.748	0.521
ท่านมีความรู้ความชำนาญทางด้านโปรแกรมทางการบัญชีที่เกิดจากการสะสมข้อมูล หรือมีประสบการณ์ในอดีตที่สามารถนำมาประยุกต์ใช้ด้วยกันได้	3.59	0.762	0.734
ท่านคิดว่าท่านมีทักษะในการเรียนรู้การอัพเดทโปรแกรมทางการบัญชีได้ตลอดเวลาซึ่งเป็นการอัพเดทเพื่อป้องกันภัยคุกคามหรือความเสี่ยงรายใหม่ได้	3.34	0.917	0.734
ปัจจัยที่ 5: การรับรู้ค่าใช้จ่ายจากการใช้เครื่องมือป้องกันภัยคุกคาม (% of Variance = 5.27%, Cronbach's alpha =0.743)			
ท่านมีการเปรียบเทียบผลประโยชน์ กับค่าใช้จ่ายก่อนตัดสินใจเลือกใช้งานโปรแกรมทางการบัญชี	3.96	0.768	0.747
ท่านรับรู้ถึงประโยชน์ที่จะได้รับและยอมรับค่าใช้จ่ายในการเลือกใช้โปรแกรมทางการบัญชีสำหรับธุรกิจขนาดเล็ก	3.95	0.718	0.803
ท่านคิดว่าราคาโปรแกรมทางการบัญชีสำหรับธุรกิจขนาดเล็กที่ท่านเลือกใช้งานมีความเหมาะสมคุ้มค่ากับที่การลงทุน	3.71	0.872	0.586

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน น้ำหนักองค์ประกอบและค่าสัมประสิทธิ์แอลฟา ของครอนบาซของตัวแปรทั้งหมด (ต่อ)

ปัจจัย (Factor)	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	น้ำหนักองค์ประกอบ
ปัจจัยที่ 6: การรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัว (% of Variance = 4.74%, Cronbach's alpha =0.809)			
ท่านคิดว่าการป้องกันความเป็นส่วนตัวจะมีประสิทธิภาพได้ เนื่องจากผู้ขายโปรแกรมทางการบัญชีมีบริการหลังการขายที่ดี	3.53	0.870	0.832
ท่านคิดว่าโปรแกรมทางการบัญชีที่เลือกใช้มีการป้องกันความเป็นส่วนตัวได้ เนื่องจากสามารถกำหนดสิทธิการเข้าถึงข้อมูลทางการเงินได้อย่างปลอดภัย	3.63	0.867	0.866
การจำกัดสิทธิไม่ให้บุคคลภายนอกเข้าสู่ภายในโปรแกรมทางการบัญชีได้จะช่วยป้องกันความเป็นส่วนตัวได้อย่างมีประสิทธิผล	4.01	0.768	0.568
ปัจจัยที่ 7: แรงจูงใจในการเรียนรู้ทางสังคม (% of Variance = 4.34%, Cronbach's alpha =0.761)			
ท่านได้รับคำแนะนำจากผู้อื่นจึงเป็นแรงจูงใจต่อพฤติกรรมทางด้านความคิดของท่านว่าควรเลือกใช้โปรแกรมทางการบัญชีสำหรับธุรกิจขนาดเล็กประเภทไหน	3.56	0.804	0.648
โปรแกรมทางการบัญชีที่ท่านเลือกใช้สามารถใช้งานได้ง่ายและเป็นที่นิยมใช้กันอย่างแพร่หลายในแวดวงธุรกิจขนาดเล็ก	3.64	0.907	0.607
ท่านรับรู้ถึงถึงประโยชน์และข้อดีของโปรแกรมทางการบัญชีว่ามีอะไรบ้าง จากบุคคลใกล้ชิดและผู้ที่เคยใช้งาน	3.71	0.786	0.817
บุคคลที่ท่านรู้จักใกล้ชิด หรือสังคมรอบข้างได้กล่าวถึงคุณสมบัติที่ดีของโปรแกรมทางการบัญชีสำหรับธุรกิจขนาดเล็ก ทำให้ท่านมีความมั่นใจและเชื่อถือในตัวโปรแกรมทางการบัญชีนี้ยิ่งขึ้น	3.56	0.868	0.794

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน น้ำหนักองค์ประกอบและค่าสัมประสิทธิ์แอลฟา ของครอนบาซของตัวแปรทั้งหมด (ต่อ)

ปัจจัย (Factor)	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	น้ำหนักองค์ประกอบ
ปัจจัยที่ 8: ความตั้งใจในการรับมือกับภัยคุกคาม (% of Variance =4.13%, Cronbach's alpha =0.890)			
ท่านจะชักชวนและให้คำแนะนำแก่เพื่อนร่วมงานในการรับมือกับภัยคุกคามที่อาจเกิดขึ้นกับโปรแกรมทางการบัญชีสำหรับธุรกิจขนาดเล็ก	3.80	0.707	0.688
ท่านมีความตั้งใจที่จะปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยตามที่กำหนดไว้เพื่อช่วยให้การใช้งานโปรแกรมทางการบัญชีไม่มีปัญหาที่อาจส่งผลต่อข้อมูลทางการบัญชี	4.02	0.728	0.815
ท่านจะรับมือกับภัยคุกคามทางคอมพิวเตอร์ตลอดเวลาแม้จะมีการปรับเปลี่ยนทางด้านเทคนิคของโปรแกรมทางการบัญชีในอนาคตก็ตาม	3.91	0.775	0.758
ท่านมีความตั้งใจที่จะดำเนินการเพื่อรับมือกับภัยคุกคามทางคอมพิวเตอร์อย่างสม่ำเสมอ	4.01	0.724	0.801
ปัจจัยที่ 9: ความตระหนัก (% of Variance = 3.35%, Cronbach's alpha =0.838)			
ข้อมูลทางการเงินมีบทบาทที่สำคัญต่อการขับเคลื่อนองค์กรไปข้างหน้าจึงควรปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยอย่างเคร่งครัดเพื่อให้ข้อมูลทางการบัญชีถูกต้องครบถ้วน	4.17	0.725	0.623
ท่านมีความเข้าใจและเห็นด้วยกับนโยบายในการรักษาความมั่นคงปลอดภัยเพื่อหลีกเลี่ยงภัยคุกคามที่อาจเกิดขึ้นกับโปรแกรมทางการบัญชีซึ่งจะมีผลกระทบต่อการสูญเสียและถูกโจรกรรมข้อมูลทางการเงินได้	4.09	0.684	0.667
ปัจจัยที่ 10: พฤติกรรมในการรับมือกับภัยคุกคาม (% of Variance = 3.11%, Cronbach's alpha = 0.729)			
ท่านเปลี่ยนรหัสผ่านเพื่อเข้าสู่โปรแกรมทางการบัญชีเป็นประจำ เช่น ทุกเดือน หรือ สามเดือน เป็นต้น	3.71	0.951	0.682
ท่านค้นคว้าหาข้อมูลหรือเข้ารับการอบรมเพิ่มเติมเกี่ยวกับการดำเนินการรับมือกับภัยคุกคามในรูปแบบต่างๆ ของโปรแกรมทางการบัญชีอย่างสม่ำเสมอ	3.49	0.856	0.789
องค์กรของท่านมีการเตรียมตัวรับมือหรือมีมาตรการในการป้องกันภัยคุกคาม เช่น ติดตั้งโปรแกรม antivirus และปรับ virus definition ในเครื่องคอมพิวเตอร์ให้เป็นปัจจุบันอยู่เสมอ	3.86	0.852	0.676

5.3 ลักษณะทางประชากรศาสตร์ของกลุ่มตัวอย่าง

กลุ่มตัวอย่างจำนวน 127 คน ส่วนใหญ่เป็นเพศหญิงมากกว่าเพศชาย คิดเป็นร้อยละ 76.00 ช่วงอายุที่ตอบแบบสอบถามมากที่สุดอยู่ระหว่าง 36-40 ปีคิดเป็นร้อยละ 19.00 ระดับการศึกษาสูงสุดส่วนใหญ่อยู่ในระดับปริญญาตรี คิดเป็นร้อยละ 58.68 ระดับตำแหน่งงานในปัจจุบันส่วนใหญ่ที่ตอบแบบสอบถามอยู่ในระดับผู้จัดการ คิดเป็นร้อยละ 30.54 ผู้ตอบแบบสอบถามส่วนใหญ่มีอายุการทำงานในหน่วยงานตั้งแต่ 10 ปีขึ้นไป คิดเป็นร้อยละ 50.30 ผู้ตอบแบบสอบถามส่วนใหญ่มีความรู้เกี่ยวกับคอมพิวเตอร์และเทคโนโลยีในระดับปานกลาง คิดเป็นร้อยละ 64.07 และผู้ตอบแบบสอบถามส่วนใหญ่ใช้โปรแกรมทางการบัญชี Express คิดเป็นร้อยละ 41.32 ส่วนโปรแกรมทางการบัญชีขนาดเล็กอื่นๆ ประกอบด้วย ประกอบไปด้วย ACCPAC Plus, Sun System, Easy-Acc, Easy wins, SME Move และ Prosoft WinSpeed มีการนำมาใช้งานรวมทั้งสิ้น คิดเป็นร้อยละ 32.93

5.4 การทดสอบสมมติฐานการวิจัย

งานวิจัยนี้ทดสอบสมมติฐานการวิจัยจากกรอบแนวคิดการวิจัยด้วยการวิเคราะห์การถดถอยแบบเชิงชั้น (Hierarchical regression) ผลลัพธ์ที่ได้แสดงในตารางที่ 2 โดยสามารถวิเคราะห์ผลทางสถิติได้ดังนี้

5.4.1 ความตั้งใจในการรับมือกับภัยคุกคาม ผลทางสถิติแสดงให้เห็นว่า การรับรู้ถึงความรุนแรง การรับรู้ความสามารถของตนเอง การรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัว และแรงจูงใจในการเรียนรู้ทางสังคม ส่งอิทธิพลต่อความตั้งใจในการรับมือกับภัยคุกคาม โดยความผันแปรของตัวแปรตามเท่ากับร้อยละ 38.20 (R^2 = 0.382) แต่การรับรู้จุดอ่อน ความเชื่อเกี่ยวกับอำนาจควบคุม และการรับรู้ค่าใช้จ่ายจากการใช้เครื่องมือป้องกันภัยคุกคาม ไม่ส่งผลต่อความตั้งใจในการรับมือกับภัยคุกคาม ตามรายละเอียดดังนี้

5.4.1.1 การรับรู้ถึงความรุนแรง ส่งอิทธิพลทางตรงต่อความตั้งใจในการรับมือกับภัยคุกคาม ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.194 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ซึ่งสอดคล้องกับสมมติฐานที่ 2 ที่กล่าวว่า การรับรู้ถึงความรุนแรงส่งผลเชิงบวกต่อความตั้งใจในการรับมือกับภัยคุกคาม ซึ่งสอดคล้องกับงานวิจัยของ Workman et al. (2008) ที่กล่าวว่า เมื่อพนักงานบัญชีรับรู้ถึงความรุนแรง พนักงานเหล่านั้นจะเป็นส่วนหนึ่งของทางฝ่ายไอทีที่คอยสอดส่องดูแล เมื่อเกิดความรุนแรงต่อโปรแกรมทางการบัญชีก็จะแจ้งไปยังหน่วยงานเพื่อแก้ไขปัญหาได้อย่างตรงจุด

5.4.1.2 การรับรู้ความสามารถของตนเอง ส่งอิทธิพลทางตรงต่อความตั้งใจในการรับมือกับภัยคุกคาม ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.215 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ซึ่งสอดคล้องกับสมมติฐานที่ 4 ที่กล่าวว่า การรับรู้ความสามารถของตนเองส่งผลเชิงบวกต่อความตั้งใจในการรับมือกับภัยคุกคาม ซึ่งสอดคล้องกับงานวิจัยของ Bandura (1977) ที่กล่าวว่า เมื่อพนักงานรับรู้ถึงความสามารถของตนในการใช้งานสิ่งใดสิ่งหนึ่ง พนักงานจะปฏิบัติตามวัตถุประสงค์ที่กำหนดไว้ได้อย่างเหมาะสม กล่าวคือ เมื่อพนักงานบัญชีสามารถใช้เครื่องมือเพื่อปกป้องภัยที่อาจเกิดขึ้น พนักงานดังกล่าวจะช่วยปกป้องภัยที่อาจเกิดกับโปรแกรมทางการบัญชีได้

5.4.1.3การรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัว ส่งอิทธิพลทางตรงต่อความตั้งใจในการรับมือกับภัยคุกคาม ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.263 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ซึ่งสอดคล้องกับสมมติฐานที่ 5 ที่กล่าวว่า การรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัวส่งผลเชิงบวกต่อความตั้งใจในการรับมือกับภัยคุกคาม ซึ่งสอดคล้องกับงานวิจัยของ Bandura (1982) ที่กล่าวว่า การที่หน่วยงานรับรู้ถึงประสิทธิผลในการป้องกันภัย หน่วยงานจะมีการปกป้องภัย หรือกล่าวอีกนัยหนึ่งว่าหน่วยงานจะรักษาความเป็นส่วนตัวของข้อมูลในโปรแกรมทางการบัญชี เมื่อหน่วยงานรับรู้ถึงประสิทธิภาพของโปรแกรมที่สามารถปกป้องภัยนั้น

5.4.1.4 แรงจูงใจในการเรียนรู้ทางสังคม ส่งอิทธิพลทางตรงต่อความตั้งใจในการรับมือกับภัยคุกคาม ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.180 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ซึ่งสอดคล้องกับสมมติฐานที่ 7 ที่กล่าวว่า แรงจูงใจในการเรียนรู้ทางสังคมส่งผลต่อความตั้งใจในการรับมือกับภัยคุกคาม ซึ่งสอดคล้องกับงานวิจัยของ Liang and Xue (2009) ที่กล่าวว่า ผู้ใช้งานโปรแกรมทางการบัญชีจะเกิดแรงกระตุ้นจากบุคคลต้นแบบที่มีความเชี่ยวชาญในการ

รับมือกับภัยคุกคามที่เกิดกับโปรแกรมทางการบัญชี ถ้าหากผู้ใช้งานไม่มีการเรียนรู้จากตัวต้นแบบก็ยากที่จะหลีกเลี่ยงภัยคุกคามที่อาจเกิดขึ้นกับโปรแกรมทางการบัญชีได้ เนื่องจากขาดความรู้ความเข้าใจในการรักษาความมั่นคงปลอดภัย

5.4.1.5 การรับรู้ถึงจุดอ่อน ไม่ส่งอิทธิพลทางตรงต่อความตั้งใจในการรับมือกับภัยคุกคาม โดยมีค่าสัมประสิทธิ์อิทธิพลเท่ากับ -0.025, p = 0.713 ซึ่งไม่สนับสนุนสมมติฐานที่ 1 ที่กล่าวว่า การรับรู้ถึงจุดอ่อนส่งผลเชิงบวกต่อความตั้งใจในการรับมือกับภัยคุกคาม ที่เป็นดังนี้ อาจมีสาเหตุมาจากพนักงานที่ใช้โปรแกรมทางการบัญชีไม่ให้ความสำคัญต่อจุดอ่อนของโปรแกรมทางการบัญชีที่อาจถูกโจมตี หรือไม่ทราบถึงจุดอ่อนที่เกิดจากโปรแกรมทางการบัญชี ซึ่งสอดคล้องกับงานวิจัยของ Lee and Larsen (2009) ที่พบว่าการรับรู้จุดอ่อนจะส่งผลกระทบเชิงลบได้ถ้าผู้ใช้งานโปรแกรมทางการบัญชีให้ความสำคัญกับโปรแกรมน้อย เนื่องจากผู้ใช้งานคิดว่าการควบคุมจุดอ่อนของโปรแกรมทางการบัญชีเป็นหน้าที่ของฝ่ายไอที

5.4.1.6 ความเชื่อเกี่ยวกับอำนาจควบคุม ไม่ส่งอิทธิพลทางตรงต่อความตั้งใจในการรับมือกับภัยคุกคาม ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.097, p = 0.149 ซึ่งไม่สนับสนุนสมมติฐานที่ 3 ที่กล่าวว่า การรับรู้ความเชื่อเกี่ยวกับอำนาจควบคุมส่งผลเชิงบวกต่อความตั้งใจในการรับมือกับภัยคุกคาม ที่เป็นดังนี้ อาจมีสาเหตุมาจากผู้ใช้งานโปรแกรมทางการบัญชีคิดว่าการควบคุมจุดอ่อนของโปรแกรมทางการบัญชีเป็นหน้าที่ของฝ่ายไอทีมากกว่า (Lee & Larsen, 2009)

5.4.1.7 การรับรู้ค่าใช้จ่ายจากการใช้เครื่องมือป้องกันภัยคุกคาม ไม่ส่งอิทธิพลทางตรงต่อความตั้งใจในการรับมือกับภัยคุกคาม ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.098, p = 0.179 ซึ่งไม่สนับสนุนสมมติฐานที่ 6 ที่กล่าวว่า การรับรู้ค่าใช้จ่ายจากการใช้เครื่องมือป้องกันภัยคุกคามส่งผลกระทบเชิงบวกต่อความตั้งใจในการรับมือกับภัยคุกคาม ที่เป็นดังนี้ อาจมีสาเหตุมาจากผู้ใช้งานโปรแกรมทางการบัญชีคิดว่าการควบคุมจุดอ่อนของโปรแกรมทางการบัญชีเป็นหน้าที่ของฝ่ายไอทีมากกว่า (Lee & Larsen, 2009)

5.4.2 พฤติกรรมในการรับมือกับภัยคุกคาม ผลทางสถิติแสดงให้เห็นว่า ความตั้งใจในการรับมือกับภัยคุกคามส่งอิทธิพลต่อพฤติกรรมในการรับมือกับภัยคุกคาม ที่ค่าสัมประสิทธิ์อิทธิพล เท่ากับ 0.371 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 และมีความผันแปรของตัวแปรตามเท่ากับ 20.8 (R^2 = 0.208) ซึ่งสนับสนุนสมมติฐานการวิจัยที่ 8 ที่กล่าวว่า ความตั้งใจในการรับมือกับภัยคุกคามส่งผลกระทบเชิงบวกต่อพฤติกรรมในการรับมือกับภัยคุกคาม สอดคล้องกับ Ajzen and Fishbein (1977) ที่กล่าวว่าความตั้งใจส่งผลทางตรงต่อพฤติกรรม กล่าวคือ ผู้ใช้โปรแกรมทางการบัญชีมักจะมีความตั้งใจในการหามาตรการมาดำเนินการรับมือกับภัยคุกคาม อีกทั้งผู้ใช้โปรแกรมทางการบัญชีที่มีทักษะจะจัดการกับปัญหาที่เกิดขึ้นกับโปรแกรมคอมพิวเตอร์เพื่อไม่ให้ส่งผลกระทบร้ายแรงต่อโปรแกรมทางการบัญชี

นอกจากนี้ผลทางสถิติแสดงให้เห็นว่าความตระหนักส่งอิทธิพลต่อพฤติกรรมในการรับมือกับภัยคุกคาม ที่ค่าสัมประสิทธิ์อิทธิพล เท่ากับ 0.138 อย่างมีนัยสำคัญส่วนเพิ่มทางสถิติที่ระดับ 0.088 ซึ่งสนับสนุนสมมติฐานการวิจัยที่ 9 บางส่วน ที่กล่าวว่า ความตระหนักส่งผลเชิงบวกต่อความตั้งใจในการรับมือกับภัยคุกคาม ที่เป็นดังนี้ อาจมีสาเหตุมาจากผู้ใช้โปรแกรมอาจไม่เคยประสบกับภัยคุกคามทางคอมพิวเตอร์ด้วยตนเองจึงยังไม่ให้ความระมัดระวังกับภัยคุกคามทางคอมพิวเตอร์มากนัก

นอกเหนือจากอิทธิพลทางตรงของความตั้งใจในการรับมือกับภัยคุกคามและความตระหนักต่อพฤติกรรมในการรับมือกับภัยคุกคามดังกล่าวข้างต้นแล้ว พฤติกรรมในการรับมือกับภัยคุกคามยังได้รับอิทธิพลทางอ้อมจากปัจจัยการรับรู้ถึงความรุนแรง การรับรู้ความสามารถของตนเอง การรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัว และแรงจูงใจในการเรียนรู้ทางสังคม ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.012, 0.018, 0.003 และ 0.025 ตามลำดับ

ตารางที่ 2 ค่าสัมประสิทธิ์อิทธิพลทางตรง ทางอ้อม อิทธิพลโดยรวมของตัวแปรแฝง และอิทธิพลร่วม ในกรอบแนวคิดการวิจัย (แสดงเป็นคะแนนมาตรฐาน)

ตัวแปรตาม	R^2	อิทธิพล	ตัวแปรอิสระ								
			การรับรู้ถึงความรุนแรง	การรับรู้ถึงจุดอ่อน	ความเชื่อเกี่ยวกับอำนาจควบคุม	การรับรู้ความสามารถของตนเอง	การรับรู้ค่าใช้จ่ายจากการใช้เครื่องมือป้องกันภัยคุกคาม	การรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัว	แรงจูงใจในการเรียนรู้ทางสังคม	ความตระหนัก	ความตั้งใจในการรับมือกับภัยคุกคาม
ความตั้งใจในการรับมือกับภัยคุกคาม	0.382	ทางตรง	0.194*	-0.025	0.097	0.215*	0.098	0.263*	0.180*	-	-
		ทางอ้อม	-	-	-	-	-	-	-	-	-
		รวม	0.194	-0.025	0.097	0.215	0.098	0.263	0.180	-	-
พฤติกรรมในการรับมือกับภัยคุกคาม	0.208	ทางตรง	-	-	-	-	-	-	-	0.138**	0.371*
		ทางอ้อม	0.012*	-	-	0.018*	-	0.003*	0.025*	-	-
		รวม	0.012	-	-	0.018	-	0.003	0.025	0.138	0.371

* $p < 0.05$, ** $p = 0.05$-0.10

6. สรุปผลการวิจัย

6.1 อภิปรายผลการวิจัย

ผลการวิจัยแสดงให้เห็นว่ากรอบแนวคิดการวิจัยพฤติกรรมในการรับมือกับภัยคุกคามทางคอมพิวเตอร์ต่อการสูญเสียและถูกโจรกรรมข้อมูลทางการเงินมีความสอดคล้องกับข้อมูลเชิงประจักษ์ ดังนี้

(1) การรับรู้ถึงความรุนแรง การรับรู้ความสามารถของตนเอง การรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัว และแรงจูงใจในการเรียนรู้ทางสังคม ส่งผลต่อความตั้งใจในการรับมือกับภัยคุกคาม แต่ข้อมูลเชิงประจักษ์ไม่แสดงให้เห็นว่า การรับรู้จุดอ่อน ความเชื่อเกี่ยวกับอำนาจควบคุม และการรับรู้ค่าใช้จ่ายจากการใช้เครื่องมือป้องกันภัยคุกคามไม่ส่งผลต่อความตั้งใจในการรับมือกับภัยคุกคาม ที่เป็นดังนี้อาจเนื่องจากผู้ใช้งานโปรแกรมทางการบัญชีมีความเห็นว่าการรักษาความมั่นคงปลอดภัยของโปรแกรมเป็นหน้าที่ของฝ่ายคอมพิวเตอร์เท่านั้น

(2) ความตั้งใจในการรับมือกับภัยคุกคามจะส่งผลต่อพฤติกรรมในการรับมือกับภัยคุกคาม ส่วนความตระหนักส่งผลต่อพฤติกรรมในการรับมือกับภัยคุกคามบางส่วนเท่านั้น

6.2 ข้อเสนอแนะในเชิงปฏิบัติ

การที่จะให้ผู้ใช้งานโปรแกรมทางการบัญชีตั้งใจที่จะปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัย รับมือและชักชวนให้เพื่อนร่วมงานรับมือกับภัยคุกคามที่อาจเกิดขึ้นกับโปรแกรมทางการบัญชีนั้นธุรกิจควรดำเนินการดังนี้

(1) ให้ข้อมูลและสร้างการรับรู้ถึงความรุนแรงกับผู้ใช้โปรแกรมทางการบัญชี เกี่ยวกับภัยคุกคามทาง Cyber เช่น สปายแวร์หรือไวรัส เป็นต้น

(2) จัดทำคู่มือการปฏิบัติงานที่ให้ข้อมูลเกี่ยวกับโปรแกรมทางการบัญชี และข้อมูลที่เกี่ยวกับความมั่นคงปลอดภัยของโปรแกรมทางการบัญชี เช่น การปกป้อง การจัดการข้อผิดพลาด และการสอบทานข้อมูลทางการเงิน เป็นต้น นอกจากนี้ควรสร้างความมั่นใจและทักษะในการจัดการกับโปรแกรมทางการบัญชีให้กับผู้ใช้โปรแกรมทางการบัญชี เพื่อให้มีทักษะในการปกป้องโปรแกรมทางการบัญชีจากภัยคุกคามตามที่กำหนดไว้ในคู่มือการปฏิบัติงาน

(3) กำหนดให้โปรแกรมทางการบัญชีมีการรักษาความมั่นคงปลอดภัย เช่น การป้องกันความเป็นส่วนตัว การกำหนดสิทธิในการใช้งานโปรแกรมทางการบัญชี และจำกัดสิทธิไม่ให้บุคคลภายนอกเข้าสู่ภายในโปรแกรมทางการบัญชีได้ เป็นต้น

(4) เลือกใช้สามารถใช้งานได้ง่ายและเป็นที่นิยมใช้กันอย่างแพร่หลายในแวดวงธุรกิจขนาดเล็ก

นอกจากนี้การที่จะให้ผู้ใช้งานโปรแกรมทางการบัญชีมีพฤติกรรมในการรับมือกับภัยคุกคาม เช่น เปลี่ยนรหัสผ่านเพื่อเข้าสู่โปรแกรมทางการบัญชีเป็นประจำ ค้นคว้าหาข้อมูลหรือเข้ารับการอบรมเพิ่มเติมเกี่ยวกับการดำเนินการรับมือกับภัยคุกคามในรูปแบบต่างๆ ของโปรแกรมทางการบัญชีอย่างสม่ำเสมอ และเตรียมตัวรับมือหรือมีมาตรการในการป้องกันภัยคุกคาม ไม่ว่าจะเป็นติดตั้งโปรแกรม antivirus และปรับ virus definition ในเครื่องคอมพิวเตอร์ให้เป็นปัจจุบันอยู่เสมอนั้น ธุรกิจควรดำเนินการดังนี้

(1) สร้างความตั้งใจที่จะปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยที่ธุรกิจกำหนดไว้ดังกล่าวมาแล้วข้างต้น

(2) สร้างความตระหนักให้ผู้ใช้งานโปรแกรมทางการบัญชีให้เข้าใจและเห็นด้วยกับนโยบายในการรักษาความมั่นคงปลอดภัย ซึ่งอาจกระทำด้วยการให้ผู้ใช้งานโปรแกรมทางการบัญชีมีส่วนร่วมในการกำหนดนโยบายดังกล่าวด้วย

6.3 ข้อเสนอแนะสำหรับงานวิจัยต่อเนื่อง

คณะผู้วิจัยขอเสนอแนะการทำวิจัยครั้งต่อไปดังนี้

(1) งานวิจัยนี้จัดเก็บข้อมูลจากกลุ่มตัวอย่างเฉพาะในเขตพื้นที่กรุงเทพมหานครเท่านั้น งานวิจัยต่อเนื่องอาจขยายขอบเขตไปยังภูมิภาคอื่นๆ ซึ่งอาจมีลักษณะของการรักษาความมั่นคงปลอดภัยของโปรแกรมทางการบัญชีที่แตกต่างกันออกไปได้

(2) ผลการวิจัยในครั้งนี้ พบว่า ปัจจัยการรับรู้จุดอ่อน ความเชื่อเกี่ยวกับอำนาจควบคุม และการรับรู้ค่าใช้จ่ายจากการใช้เครื่องมือป้องกันภัยคุกคาม ไม่ส่งผลต่อความตั้งใจในการรับมือกับภัยคุกคาม งานวิจัยต่อเนื่องอาจพิจารณาถึงปัจจัยการกำหนดหน้าที่งานด้านการรักษาความมั่นคงปลอดภัยที่เฉพาะเจาะจงมากขึ้น

นอกจากนี้ผลการวิจัยยังแสดงให้เห็นว่าความตระหนักส่งผลต่อพฤติกรรมในการรับมือกับภัยคุกคามเพียงเล็กน้อยเท่านั้น งานวิจัยต่อเนื่องอาจพิจารณาหาปัจจัยอื่นหรือจะทดสอบปัจจัยดังกล่าวอีกครั้งกับกลุ่มตัวอย่างอื่นๆ เพื่อค้นหาความสัมพันธ์ที่เหมาะสมต่อไป

บรรณานุกรม

ธวัชชัย ชมศิริ. (2553). *ความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์.* กรุงเทพฯ: โปรวิชั่น.

นิตยา วงศ์ภินันท์วัฒนา. (2561). *การตรวจสอบระบบสารสนเทศ.* กรุงเทพฯ: สำนักพิมพ์ มหาวิทยาลัยธรรมศาสตร์.

สำนักงานราชบัณฑิตยสภา. (2554). ความหมายคำว่าตั้งใจ. ดึงข้อมูลวันที่ 1 เมษายน 2562, จาก http://www.royin.go.th/ dictionary/.

Ajzen, I., & Fishbein, M. (1977). Attitude-behavior relations: A theoretical analysis and review of empirical research. *Psychological Bulletin, 84*, 888–918.

Bandura, A. (1977). Self-Efficacy: Toward a Unifying Theory of Behavior Change. *Psychological Review, 84*, 191-215.

Bandura, A. (1982). Self-Efficacy Mechanism in Human Agency. *American Psychologist, 37*, 122-147.

Beaudry, A.., & Pinsonneault, A. (2005). Understand User Responses to Information Technology: A Coping Model of User Adaption. *MIS Quarterly*, *29* (3), 493-534.

Davison, W. P. (1983). The third-person effect in communication. *Public Opinion Quarterly, 47*, 1-13.

Good, C. V. (1973). *Dictionary of Education*. New York: McGraw-Hill.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., and Tatham, R. L. (1998). Construct Validity and Reliability. Retrieved January 12, 2016, from http://wallaby.vu.edu.au/adt-VVUT/uploads/approved/adtVVUT20080416/115505/public/05Chapter4.pdf.

Herath, T., & Rao, H. R. (2010). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations. *European Journal of Information Systems*, *18*, 106–125.

Humaidi, N., & Balakrishnan, V. (2012). The Influence of Security Awareness and Security Technology on Users' Behavior towards the Implementation of Health Information System: A Conceptual Framework. *2nd International Conference on Management and Artificial Intelligence*, Hawaii, 35.

Koffka, K. (1978). *Encyclopedia of the Social Sciences*. New York: The Macmillan Company.

Lee, Y., & Larsen, K. R. (2009). Threat or Coping Appraisal: Determinants of SMB Executives' Decision to Adopt Antimalware Software. *European Journal of Information Systems*, *18*, 177–187.

Lefcourt, H. M. (1976). *Locus of Control Current Trends*: Theory and Research. New York: Wiley.

Lefcourt, H. M. (1981). *Research with the Locus of Control Construct*: *vol. 1. Assessment Methods*. New York: Academic Press.

Liang, H., & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly*, 33(1), 71-90.

McCarthy, J. J., Canziani, O. F., Leary, N. A., Dokken, D. J., & White, K. S. (2001). *Climate Change 2001: Impacts, Adaptation and Vulnerability.* Cambridge: Cambridge University Press.

Rotter, J. (1966). Generalized Expectancies for Internal Versus External Control of Reinforcement. *Psychological Monographs, 1*, 1–28.

Rotter, J. B. (1975). Some problems and misconceptions related to the construct of internal vs. external control of reinforcement. *Journal of Consulting and Clinical Psychology,* 43, 56-67.

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(18), 2799–2816.