ปัจจัยที่ส่งเสริมให้พนักงานในองค์กรแสดงออกถึงพฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ

อภิญญา รัตนาตรานุรักษ์*
บริษัท อีวาย คอร์ปอเรท เซอร์วิสเซส จำกัด

***Correspondence:** apinya.ara@gmail.com
doi: 10.14456/jisb.2018.15
วันที่รับบทความ: 22 ก.ค. 2560 วันแก้ไขบทความ: 22 ส.ค. 2560 วันตอบรับบทความ: 5 ก.ย. 2560

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาปัจจัยที่ส่งผลต่อการแสดงออกถึงพฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศของพนักงานในองค์กร ซึ่งเป็นงานวิจัยเชิงปริมาณ โดยทำการศึกษากลุ่มประชากรที่เป็นพนักงานในองค์กรที่มีนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศภายในองค์กรทั้งภาครัฐและเอกชน จำนวน 229 กลุ่มตัวอย่าง ด้วยวิธีการแจกแบบสอบถามทั้งรูปแบบกระดาษและอิเล็กทรอนิกส์ ผลการวิจัยพบว่า การรับรู้ภัยคุกคาม ความเชื่อในความสามารถของตนเอง การคล้อยตามกลุ่มอ้างอิง ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย การรับรู้ถึงความรับผิดรับชอบ และการตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยส่งอิทธิพลทางตรงต่อความตั้งใจที่จะปฏิบัตินโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศและยังส่งอิทธิพลทางอ้อมต่อพฤติกรรมในการรักษาความมั่นคงปลอดภัย หากพนักงานเกิดความตั้งใจที่จะปฏิบัติตามนโยบายและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยแล้วนั้นก็จะส่งผลโดยตรงทำให้เกิดการแสดงออกถึงพฤติกรรมในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศด้วย ทั้งนี้การรับรู้ภัยคุกคามที่เกิดขึ้นของพนักงานมีผลมาจากประสบการณ์ก่อนหน้าจากการเผชิญกับภัยคุกคามด้วยเช่นกัน ส่วนการให้รางวัลและความรู้สึกของการบีบบังคับโดยการลงโทษนั้นไม่ส่งผลกระทบต่อความตั้งใจที่จะปฏิบัติตามนโยบาย เนื่องจากการให้รางวัลและบทลงโทษอาจถูกตีความว่าเป็นเครื่องมือที่ใช้ในการควบคุมพฤติกรรม จึงทำให้พนักงานรู้สึกต่อต้าน และไม่อยากที่จะปฏิบัติตามนโยบาย ซึ่งผู้ที่เกี่ยวข้องหรือผู้ที่ต้องการสร้างสภาพแวดล้อมให้เกิดการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศสามารถนำไปปรับใช้เพื่อควบคุมให้พนักงานแสดงออกถึงพฤติกรรมในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศอย่างเหมาะสม

คำสำคัญ: พฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย ความตั้งใจที่จะปฏิบัติตามนโยบาย

Factors affecting the Employees' Behavior towards Information Security Policy Compliance

Apinya Rattanatranurak*

EY Corporate Services Co., Ltd.

***Correspondence:** apinya.ara@gmail.com

doi: 10.14456/jisb.2018.15

Received: 22 Jul 2017 Revised: 22 Aug 2017 Accepted: 5 Sep 2017

Abstract

The objective of this study is to examine the factors influencing behavioral information security policy compliance in employee. This research is quantitative research. The study was collected from 229 Thai participants, who was an employee in organizations with information security policy including both government and private sectors. Data was gathered by printed and online questionnaires. According to the results, this research found that factors - perceived threat, self-efficacy, subjective norms, attitude towards compliance with policy, perceived accountability and security awareness - are directly affect to the intention to information security policy compliance and also indirectly affects to security behavior. If participants intend to follow and aware of the security policy, they will conform to the information security behavior. In addition, participants perceived threat after they had prior experience with safety hazard. However, the results show that reward and perceived of constraint by punishment do not affect to the intention security policy compliance. The reason could be that participants interpreted rewards and punishment as a tool used to control behavior. Thus, the participants feel opposed and do not need to follow the information security policy compliance. This research introduces who involved or make environment to maintain information security can be implemented to control employees' behaviors under proper information security practice.

Keywords: Behavioral information security policy compliance, Security awareness, Intention to compliance policy

1. บทนำ

1.1 ความสำคัญและที่มาของปัญหา

เทคโนโลยีในปัจจุบันมีการเปลี่ยนแปลงไปอย่างรวดเร็ว ส่งผลให้องค์กรต่าง ๆ ต้องปรับตัวให้ทันกับเทคโนโลยีใหม่ ๆ ที่เกิดขึ้น จึงได้นำเทคโนโลยีสารสนเทศมาใช้เป็นพื้นฐานในการเปลี่ยนแปลงรูปแบบทางธุรกิจและกลยุทธ์ทางธุรกิจ (Stanciu & Tinca, 2016) ได้แก่ การจัดหา laptop ให้กับพนักงานได้ใช้พกพาไปทำงานนอกสถานที่ อุปกรณ์สื่อสารที่ทันสมัยขึ้น การใช้สื่อสังคมออนไลน์ (Social media) คลาวด์คอมพิวติ้ง (Cloud computing) หรือแนวคิดของการนำอุปกรณ์สื่อสารส่วนตัวมาใช้ในการทำงาน (Bring your own device: BYOD) เป็นต้น เพื่อที่จะสามารถตอบสนองและสร้างความพึงพอใจให้กับลูกค้าได้อย่างสะดวกและรวดเร็วที่สุด อย่างไรก็ตามการนำเทคโนโลยีมาใช้นั้นส่งผลให้เกิดความเสี่ยงทางธุรกิจจากการไม่ได้คำนึงถึงการรักษาความมั่นคงปลอดภัยของข้อมูลในระดับที่เพียงพอ (PwC, 2014) โดยจากผลการสำรวจของบริษัท PwC ในปี 2015 พบว่า เหตุการณ์การละเมิดการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศเพิ่มสูงขึ้นจากในอดีตถึงร้อยละ 48 และมีแนวโน้มที่จะขยายตัวสูงขึ้น จึงทำให้เทคโนโลยีด้านการรักษาความมั่นคงปลอดภัยกลายเป็นกลยุทธ์ที่สำคัญสำหรับธุรกิจในปัจจุบัน (Zaharia, 2015; PwC, 2015) ซึ่งนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศเป็นวิธีการในการจัดการเรื่องการรักษาความมั่นคงปลอดภัยที่สำคัญที่องค์กรส่วนใหญ่นิยมใช้ โดยจะช่วยให้มั่นใจว่าพนักงานทุกคนเข้าใจบทบาทและความรับผิดชอบของตนเองและทำให้ธุรกิจบรรลุเป้าหมายขององค์กรได้อย่างแท้จริง (Trustwave, 2014) แต่องค์กรอาจเกิดช่องโหว่ที่เป็นอันตรายจากการที่องค์กรมีนโยบายการรักษาความมั่นคงปลอดภัย แต่พฤติกรรมของพนักงานที่เกิดขึ้นจริงไม่ได้ปฏิบัติตามนโยบายเหล่านั้น จึงทำให้องค์กรตกเป็นเป้าหมายของการโจมตีของผู้ไม่ประสงค์ดี และเป็นเหตุให้นำมาซึ่งการสูญเสียทั้งค่าใช้จ่าย เวลา และทรัพยากรอื่น ๆ จำนวนมหาศาล (Jouini & Rabai, 2016) ซึ่งการที่พนักงานไม่ปฏิบัติตามนโยบายหรือมีการปฏิบัติที่บกพร่อง ไม่ครบถ้วน อาจเกิดจากความประมาท ความไม่รู้ หรือการละเลยนโยบายการรักษาความมั่นคงปลอดภัยขององค์กรซึ่งถือเป็นสาเหตุหลักของการละเมิดการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ จนทำให้กลุ่มผู้ใช้ข้อมูลภายใน (Insider) หรือพนักงานภายในองค์กรเป็นต้นเหตุสำคัญที่ทำให้เกิดอาชญากรรมคอมพิวเตอร์มากที่สุด และมีแนวโน้มเพิ่มขึ้นอีกร้อยละ 10 จากที่ผ่านมา (PwC, 2015) ซึ่งตัวเลขนี้เป็นสัญญาณเตือนสำคัญที่องค์กรควรเริ่มตระหนักถึงความสำคัญในการดูแลและส่งเสริมให้พนักงานในองค์กรปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศที่องค์กรกำหนดขึ้น เพราะพนักงานถือเป็นผู้ที่มีความใกล้ชิดและเกี่ยวข้องกับข้อมูลสารสนเทศขององค์กรเป็นอย่างมาก อีกทั้งองค์กรส่วนใหญ่มักให้ความสำคัญกับการป้องกันภัยคุกคามจากภายนอกองค์กร โดยละเลยการปกป้องภัยคุกคามที่เกิดขึ้นจากภายในองค์กรทำให้ในบางครั้งพนักงานสามารถเข้าถึงระบบได้โดยง่ายเพราะองค์กรให้ความไว้วางใจกับพนักงาน (จตุชัย แพงจันทร์, 2550) ทำให้พนักงานในองค์กรเป็นปัจจัยสำคัญที่ส่งผลต่อความมั่นคงปลอดภัยในระบบสารสนเทศขององค์กร หากพนักงานในองค์กรปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรอย่างสม่ำเสมอจะเป็นการช่วยให้องค์กรสามารถใช้เทคโนโลยีต่าง ๆ ได้อย่างมีประสิทธิภาพและไม่ต้องกังวลกับปัญหาภัยคุกคามต่าง ๆ ที่อาจเกิดขึ้น

ดังนั้นการศึกษาปัจจัยที่ส่งเสริมให้พนักงานในองค์กรแสดงออกถึงพฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศในองค์กรจึงเป็นสิ่งที่จำเป็นอย่างยิ่งที่จะใช้เป็นแนวทางในการเสริมสร้างแรงจูงใจให้พนักงานในองค์กรให้ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยเพื่อให้เกิดความมั่นใจว่าข้อมูลสารสนเทศขององค์กรจะไม่รั่วไหลไปยังคู่แข่งหรือในสถานที่ ๆ ไม่พึงประสงค์ และลดช่องโหว่ที่สำคัญจากการใช้เทคโนโลยีใหม่ ๆ ที่นำมาใช้ภายในองค์กร เพื่อที่จะได้นำเทคโนโลยีมาใช้ให้เกิดประสิทธิภาพสูงสุดแก่องค์กรโดยไม่ก่อให้เกิดความเสียหายต่อข้อมูลสารสนเทศในองค์กร

1.2 วัตถุประสงค์ของการวิจัย

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาถึงปัจจัยต่าง ๆ ที่ส่งผลต่อการแสดงออกถึงพฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กร ประกอบด้วย ประสบการณ์ก่อนหน้าจากการเผชิญกับ

ภัยคุกคาม การรับรู้ภัยคุกคาม ความเชื่อในความสามารถของตนเอง การคล้อยตามกลุ่มอ้างอิง ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย การรับรู้ถึงความรับผิดรับชอบ การให้รางวัล ความรู้สึกของการบีบบังคับโดยการลงโทษ การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยที่ส่งผลต่อพฤติกรรมในการรักษาความมั่นคงปลอดภัยผ่านความตั้งใจที่จะปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

จากการศึกษาทฤษฎีทางจิตวิทยาสังคม (Social psychology) ได้แก่ ทฤษฎีแรงจูงใจเพื่อป้องกันโรค ทฤษฎีพฤติกรรมตามแผน ทฤษฎีความรับผิดรับชอบ ทฤษฎีการข่มขู่ยับยั้งทั่วไป ทฤษฎีการปฏิบัติตาม และงานวิจัยในอดีตที่เกี่ยวข้องสามารถสรุปปัจจัยที่เกี่ยวข้องกับการศึกษาได้ดังนี้

ประสบการณ์ก่อนหน้าจากการเผชิญกับภัยคุกคาม (Prior experience with safety hazard) หมายถึง ความรู้หรือการเรียนรู้ที่จะนำไปสู่ความคุ้นเคย ความสามารถ ทักษะและความเข้าใจเหตุการณ์ หรือการเรียนรู้ผ่านทางบุคคลอื่นที่เคยได้พบเจอกับเหตุการณ์หรือเป็นผู้เชี่ยวชาญในด้านที่เกี่ยวข้องกับอันตรายที่เกิดขึ้นกับระบบสารสนเทศขององค์กรของแต่ละบุคคลในอดีต ซึ่งมีส่วนช่วยในการตอบสนองและจัดการกับภัยคุกคามที่อาจเกิดขึ้น (สำนักงานราชบัณฑิตยสภา, 2532; Safa et al., 2016; Tsai et al., 2016)

การรับรู้ภัยคุกคาม (Perceived threats) หมายถึง การที่บุคคลประเมินระดับความเสี่ยงหรือรับรู้ถึงอันตรายจากเหตุการณ์ที่อาจก่อให้เกิดความเสียหายต่อระบบสารสนเทศขององค์กรจาก วัตถุ สิ่งของ หรือตัวบุคคล เพื่อหาวิธีในการปกป้องสารสนเทศขององค์กร ซึ่งประกอบด้วย การรับรู้ช่องโหว่ (perceived vulnerability) การรับรู้ความรุนแรง (perceived severity) และความกลัว (Fear) โดยภัยคุกคามทางด้านสารสนเทศนั้นสามารถสร้างความรู้สึกวิตกกังวลให้กับบุคคลในด้านความมั่นคงปลอดภัย และอาจสร้างความเสียหายกับข้อมูลที่เป็นความลับขององค์กรและทำให้สูญเสียทางด้านการเงินได้ (Liang & Xue, 2010; Ifinedo, 2012; Lee et al., 2016; Chen & Zahedi, 2016)

ความเชื่อในความสามารถของตนเอง (Self-efficacy) หมายถึง การที่บุคคลรับรู้ว่าตนสามารถที่จะตัดสินใจในการใช้ทักษะส่วนบุคคล หรือความรู้ของตนเอง เพื่อปกป้องสารสนเทศในองค์กรจากภัยคุกคามที่จะเข้ามาทำอันตรายได้อย่างเหมาะสม เช่น การใช้รหัสผ่าน การติดตั้งซอฟต์แวร์ป้องกันไวรัส การปิดการใช้ Cookies เป็นต้น (Ifinedo, 2012; Al-Omari et al., 2013)

การคล้อยตามกลุ่มอ้างอิง (Subjective norms) หมายถึง สิ่งที่สะท้อนให้เห็นถึงความเชื่อ การรับรู้ หรือแรงจูงใจของบุคคลที่จะปฏิบัติตามการกระทำหนึ่ง ๆ โดยการกระทำนั้นเป็นที่ยอมรับและได้รับการสนับสนุนจากบุคคลอื่นที่มีความสำคัญต่อบุคคลนั้น ซึ่งอาจมาจากการให้คำปรึกษาหรือสังเกตพฤติกรรมจากผู้อื่น เช่น ครอบครัว เพื่อน ผู้บังคับบัญชา ผู้ใต้บังคับบัญชา เป็นต้น เพื่อนำมาใช้ในการตัดสินใจที่จะปฏิบัติตามในแต่ละบุคคล (Ifinedo, 2012; Hu et al., 2012)

ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย (Attitude towards compliance with policy) หมายถึง การที่บุคคลมีความรู้สึกหรือความคิดทั้งในแง่บวกและแง่ลบต่อการมีส่วนร่วมในการแสดงออกถึงพฤติกรรมที่น่าสนใจ โดยบุคคลสามารถรับรู้ทัศนคติที่มีต่อสิ่ง ๆ หนึ่ง ได้จากสถานที่ บุคคล กิจกรรม หรือสิ่งต่าง ๆ ทั้งนี้ทัศนคติสามารถที่จะเปลี่ยนแปลงได้ผ่านการโน้มน้าวหรือชักจูงผ่านการตอบสนองจากการสื่อสารในหลาย ๆ ทาง เช่น การกำหนดนโยบาย เป็นต้น โดยทัศนคติที่ดีจะทำให้บุคคลมีแนวโน้มในการแสดงพฤติกรรมตามนโยบายมากขึ้น (Ajzen 1991; Fishbein & Ajzen, 1975; Dinev & Hu, 2007; Pahnila et al., 2007; Hu et al., 2012; Ifinedo, 2012; Hepler, 2015)

การรับรู้ถึงความรับผิดรับชอบ (Perceived accountability) หมายถึง การพร้อมรับผิดจากผลของการกระทำที่ส่งผลต่อตนเองและผู้อื่นทั้งในทางบวกและทางลบ เพื่อให้เป็นไปตามมาตรฐานที่กำหนดไว้ ทั้งในส่วนของภาระหน้าที่ ความคาดหวัง และค่าใช้จ่ายอื่น ๆ ซึ่งเป็นสิ่งที่จำเป็นในการดำเนินงานภายในองค์กรอย่างมีประสิทธิภาพ และเป็นการที่บุคคลมีความรู้สึกที่ต้องมีความรับผิดชอบซึ่งออกมาจากจิตสำนึกในการรักษาทรัพย์สินหรือปฏิบัติตามหน้าที่ที่ได้รับ

มอบหมายตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ (Schlenker et al., 1994; Hochwarter et al., 2005; Vance et al., 2015)

การให้รางวัล (Reward) หมายถึง แรงจูงใจที่จำเป็นสำหรับการให้บุคคลปฏิบัติตามสิ่งใด ๆ โดยบุคคลจะรับรู้ถึงความเป็นธรรมที่ได้รับจากผลตอบแทนทั้งที่เป็นตัวเงินและไม่เป็นตัวเงินว่ามีความเหมาะสมกับสิ่งที่ต้องกระทำหรือต้นทุนของบุคคลหรือไม่ และเพิ่มความเชื่อมั่นและความต้องการให้กับบุคคลในการกระทำตามสิ่งที่องค์กรอยากจะให้ปฏิบัติตาม เช่น การปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ เป็นต้น (Siponen et al., 2009; Bulgurcu et al., 2010; Cavallari, 2011; Chen et al., 2012)

ความรู้สึกของการบีบบังคับโดยการลงโทษ (Perceived of constraint by punishment) หมายถึง การที่บุคคลรับรู้ถึงมาตรการหรือกฎระเบียบที่ใช้ในการควบคุมพฤติกรรมของบุคคลในองค์กร เพื่อยับยั้งและต่อต้านพฤติกรรมที่เบี่ยงเบน ซึ่งเป็นวิธีการควบคุมให้มีการปฏิบัติตามและทำโทษบุคคลจากการไม่ปฏิบัติตามกฎระเบียบ ได้แก่ การลดตำแหน่งหรืออำนาจลง การถูกตำหนิหรือเสื่อมเสียชื่อเสียง การถูกหักเงินเดือน เป็นต้น ทั้งนี้การลงโทษจะต้องเกิดขึ้นอย่างรวดเร็ว สม่ำเสมอ และมีระดับความรุนแรงเพียงพอที่จะทำให้บุคคลเหล่านั้นไม่ฝ่าฝืนกฎระเบียบและยอมที่จะปฏิบัติตามกฎระเบียบ (Straub, 1990; Peace et al., 2003; Son, 2011; Chen et al., 2012)

การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย (Security awareness) หมายถึง การที่บุคคลรับรู้ มีสติต่อเหตุการณ์หรือทางความคิดอย่างใดอย่างหนึ่งที่เกิดขึ้น โดยนำมาซึ่งการตอบสนองทั้งในเชิงบวกและเชิงลบ ซึ่งพนักงานต้องมีความรู้ทั่วไปและความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ โดยพนักงานต้องเข้าใจเกี่ยวกับปัญหาที่อาจจะเกิดขึ้นหากไม่มีการปฏิบัติตาม รวมถึงความต้องการและจุดมุ่งหมายที่ถูกกำหนดไว้ในนโยบายการรักษาความมั่นคงปลอดภัย เพื่อให้บรรลุวัตถุประสงค์ของการรักษาความมั่นคงปลอดภัยขององค์กร (Siponen, 2000; Bulgurcu et. al., 2010; Cavallari, 2011; สุพิชญา อาชวจริดา, 2557)

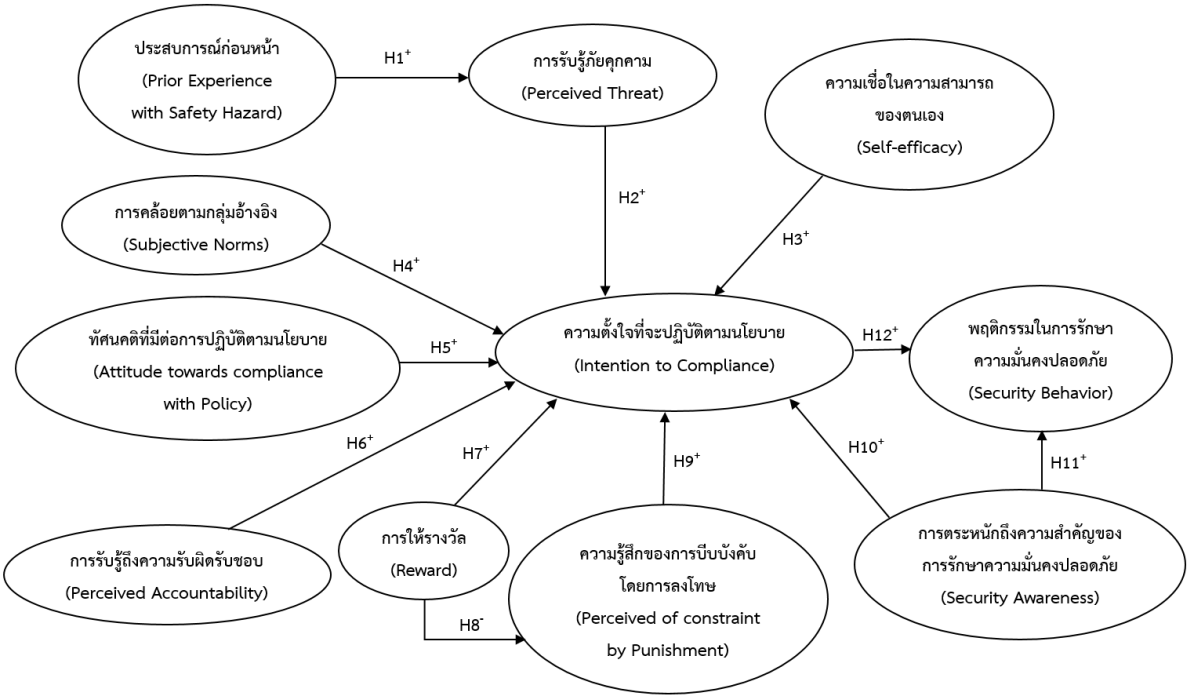
ความตั้งใจที่จะปฏิบัติตามนโยบาย (Intention to compliance) หมายถึง เจตนาหรือความพร้อมของแต่ละบุคคลที่จะแสดงออกถึงพฤติกรรมใดพฤติกรรมหนึ่ง ซึ่งถือเป็นความตั้งใจของพนักงานในการปกป้องเทคโนโลยีสารสนเทศขององค์กรและทรัพยากรขององค์กรจากการละเมิดความมั่นคงปลอดภัยจากการใช้งานที่อาจเกิดขึ้น โดยพร้อมที่จะแสดงออกถึงพฤติกรรมอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กร (Chan et al., 2005; Herath & Rao, 2009; Bulgurcu et al., 2010; Son, 2011; Ifinedo, 2012)

พฤติกรรมในการรักษาความมั่นคงปลอดภัย (Security behavior) หมายถึง การกระทำที่แสดงออกเพื่อตอบสนองต่อสิ่งแวดล้อมและเสริมสร้างความมั่นใจของแต่ละบุคคลในการที่จะปกป้องเทคโนโลยีสารสนเทศจากการละเมิดนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศได้อย่างมีประสิทธิภาพและสม่ำเสมอ โดยมีการใช้เครื่องมือหรือเพียงปฏิบัติตามกฎระเบียบที่องค์กรได้กำหนดเอาไว้ และหลีกเลี่ยงความเสี่ยงจากพฤติกรรมที่ไม่พึงประสงค์อันจะก่อให้เกิดความเสียหายทางด้านข้อมูลสารสนเทศขององค์กรขึ้น เช่น การเปิดไฟล์เอกสารหรือโปรแกรมที่น่าสงสัย การไม่เข้ารหัสผ่านหรือไม่ทำตามข้อกำหนดเกี่ยวกับการใช้รหัสผ่านเบื้องต้น เป็นต้น (Siponen et al., 2007; Siponen et al., 2010; Merriam-Webster Online Dictionary, 2010; Bulgurcu et al., 2010; Kaur & Mustafa, 2013; Hanus & Wu, 2016)

3. กรอบแนวคิดการวิจัยและสมมติฐานการวิจัย

การวิจัยนี้ได้ประยุกต์ใช้ทฤษฎีพฤติกรรมตามแผน ทฤษฎีแรงจูงใจเพื่อป้องกันโรค ทฤษฎีความรับผิดรับชอบ ทฤษฎีการปฏิบัติตาม ทฤษฎีการข่มขู่ยับยั้งทั่วไป โมเดลความรู้ ทัศนคติและพฤติกรรมและงานวิจัยในอดีตที่เกี่ยวข้อง ประกอบด้วยปัจจัยการรับรู้ภัยคุกคาม ความเชื่อในความสามารถของตนเอง การคล้อยตามกลุ่มอ้างอิง ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย ความตั้งใจที่จะปฏิบัติตามนโยบาย และพฤติกรรมในการรักษาความมั่นคงปลอดภัย กับปัจจัยใหม่อีก 4 ปัจจัยซึ่งงานวิจัยนี้เพิ่มเข้ามา คือ ปัจจัยการรับรู้ถึงความรับผิดรับชอบ การให้รางวัล ความรู้สึกของการบีบ

บังคับโดยการลงโทษ และประสบการณ์ก่อนหน้าจากการเผชิญกับภัยคุกคาม เพื่อใช้เป็นกรอบการศึกษาเพื่อหาคำตอบของการวิจัยดังแสดงในภาพที่ 1



ภาพที่ 1 กรอบแนวคิดการวิจัยเพื่อการแสดงออกถึงพฤติกรรมในการปฏิบัติตามนโยบาย
การรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศของพนักงานในองค์กร

Albrechtsen (2007) กล่าวว่า การขาดประสบการณ์ก่อนหน้าและความรู้ในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศของผู้ใช้งานยังคงเป็นปัญหาหลักในเรื่องของบทบาทและหน้าที่ที่ผู้ใช้ควรทราบในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ เนื่องจากการมีประสบการณ์ก่อนหน้าจะมีส่วนช่วยในการสร้างการรับรู้ถึงอันตรายที่อาจเกิดขึ้นและสร้างพฤติกรรมที่เหมาะสมในการรับมือกับสภาพแวดล้อมที่เกิดขึ้นจริงและมีการเปลี่ยนแปลงอยู่ตลอดเวลา ซึ่งสอดคล้องกับแนวคิดของ Lee et al. (2008) ที่กล่าวว่า เมื่อบุคคลมีประสบการณ์ก่อนหน้าจากการเผชิญหน้ากับภัยคุกคาม เช่น การติดไวรัสในคอมพิวเตอร์ บุคคลจะมีแนวโน้มที่จะรับรู้ถึงความรุนแรงของภัยคุกคามที่เกิดขึ้นและมีความตั้งใจที่จะหาวิธีป้องกันและรับมือกับภัยคุกคามที่เกิดขึ้นเพื่อไม่ให้ส่งผลกระทบร้ายแรงต่อองค์กร ดังนั้นจึงสามารถตั้งสมมติฐานได้ว่า

H1: ประสบการณ์ก่อนหน้าจากการเผชิญกับภัยคุกคามส่งผลทางบวกต่อการรับรู้ภัยคุกคาม

Ifinedo (2012) กล่าวว่า การรับรู้ภัยคุกคามที่เกิดขึ้นเป็นการที่บุคคลประเมินภัยคุกคามที่อาจเกิดขึ้นจากการรักษาความมั่นคงปลอดภัยและอันตรายที่เกิดจากการไม่ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ ซึ่งจะประเมินผลกระทบที่เกิดจากภัยคุกคามและความน่าจะเป็นที่ภัยคุกคามนั้นจะเกิดขึ้น โดยสอดคล้องกับแนวคิดของ Herath and Rao (2009) ที่กล่าวว่า หากพนักงานรับรู้ถึงภัยคุกคามด้านการรักษาความมั่นคงปลอดภัยและทราบว่าภัยคุกคามนั้นสามารถสร้างความเสียหายหรือรบกวนต่อการทำงานอย่างมีนัยสำคัญ บุคคลจะเริ่มมีความกังวลและมีแนวโน้มที่จะตั้งใจมีส่วนร่วมในกิจกรรมการรักษาความมั่นคงปลอดภัย เช่น นโยบายการรักษาความปลอดภัยทางด้านสารสนเทศภายในองค์กร ดังนั้นจึงสามารถตั้งสมมติฐานได้ว่า

H2: การรับรู้ภัยคุกคามส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย

Bandura (1980) กล่าวว่า บุคคลจะประเมินความสามารถของตนเองและกำหนดทางเลือกในสิ่งที่ตนสามารถทำได้ขึ้นมาและพยายามที่จะทำให้สอดคล้องกับสิ่งที่ได้เลือกไว้ และ Stajkovic and Luthans (1988) ได้ประเมินเกี่ยวกับบทบาทของความเชื่อในความสามารถของตนเองกับพฤติกรรมในองค์กรในหลาย ๆ งานวิจัย ทำให้สรุปได้ว่า ความเชื่อในความสามารถของตนเองและสมรรถนะในการปฏิบัติงานที่เกี่ยวข้องกันมีความสัมพันธ์กันอย่างมาก ซึ่งสอดคล้องกับแนวคิดของ Herath and Rao (2009) ที่กล่าวว่า หากพนักงานมีความเชื่อว่าตนมีความสามารถที่จะทำตามนโยบายการรักษาความมั่นคงปลอดภัยได้ พนักงานก็จะมีแนวโน้มที่จะมีความรู้สึกในเชิงบวกมากขึ้นต่อนโยบายและยังมีแนวโน้มที่จะปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยเหล่านั้นด้วย ดังนั้นจึงสามารถตั้งสมมติฐานได้ว่า

H3: ความเชื่อในความสามารถของตนเองส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย

Venkatesh et al. (2003) และ Ifinedo (2014) กล่าวว่า การคล้อยตามกลุ่มอ้างอิงเป็นการรับรู้ถึงแรงกดดันทางสังคมที่มีผลต่อการกระทำพฤติกรรมนั้น ๆ โดยความตั้งใจของบุคคลในการแสดงออกถึงพฤติกรรมต่าง ๆ ได้รับอิทธิพลจากความคาดหวัง การให้คำปรึกษาหรือการสังเกตพฤติกรรมของบุคคลอื่นที่กระทำเป็นเรื่องปกติในสภาพแวดล้อมของบุคคลนั้น ซึ่งสอดคล้องกับแนวคิดของ Cheng et al. (2013), Chan et al. (2005) และ Herath and Rao (2009) ที่กล่าวว่า หากพนักงานได้รับแรงกดดัน แรงจูงใจหรือการสังเกตเห็นการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรจากบุคคลที่มีอิทธิพลต่อพนักงาน ได้แก่ ผู้บังคับบัญชา เพื่อนร่วมงาน ผู้ใต้บังคับบัญชา หรือได้รับความคาดหวังจากองค์กรแล้วนั้น พนักงานจะมีมุมมองเชิงบวกและมีแนวโน้มที่จะมีความตั้งใจในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ ดังนั้นจึงสามารถตั้งสมมติฐานได้ว่า

H4: การคล้อยตามกลุ่มอ้างอิงส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย

Karahanna et al. (1999) กล่าวว่า ทัศนคติของพนักงานต่อการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศเป็นการประเมินว่าหากพนักงานปฏิบัติหรือไม่ปฏิบัติตามพฤติกรรรมดังกล่าวจะนำไปสู่ผลกระทบต่อตนเองอย่างไรบ้าง เช่น ทำให้เกิดค่าใช้จ่ายหรือผลประโยชน์ที่ตามมาหรือไม่ โดยหากพนักงานมีทัศนคติที่ดีต่อการเปลี่ยนแปลงพฤติกรรมจะทำให้เกิดแรงผลักดันมากกว่าการต่อต้านการปฏิบัติตามนโยบายซึ่งนำไปสู่ความตั้งใจที่จะปฏิบัติตามนโยบายในที่สุด ทั้งนี้ Bulgurcu et al. (2010) ได้กล่าวว่า การเพิ่มการรับรู้ด้านการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศของพนักงานเป็นส่วนสำคัญที่ทำให้เกิดทัศนคติในเชิงบวกต่อการปฏิบัติตามนโยบาย ได้แก่ การสื่อสาร ฝึกอบรมหรือชี้แจงพนักงานเกี่ยวกับนโยบายที่มีการบังคับใช้ภายในองค์กร เพื่อให้พนักงานรับทราบและทำความเข้าใจเกี่ยวกับนโยบายดังกล่าว เมื่อพนักงานมีความรู้ความเข้าใจเกี่ยวกับนโยบายแล้วนั้น จะส่งผลให้พนักงานมีทัศนคติที่ดีต่อการปฏิบัติตามนโยบาย ซึ่งสอดคล้องกับแนวคิดของ Ifinedo (2014) ที่กล่าวว่า หากพนักงานมีความเชื่อและทัศนคติในเชิงบวกเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรแล้วนั้น จะมีแนวโน้มที่ดีในการปฏิบัติตามกฎระเบียบและแนวทางดังกล่าว ดังนั้นจึงสามารถตั้งสมมติฐานได้ว่า

H5: ทัศนคติที่มีต่อการปฏิบัติตามนโยบายส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย

Vance et al. (2015) กล่าวว่า ความรับผิดรับชอบเป็นการรับรู้ถึงภาระหน้าที่ที่ต้องทำจากจิตสำนึกของบุคคลในการตัดสินใจกระทำสิ่งต่าง ๆ พร้อมรับผิดชอบผลลัพธ์จากการกระทำที่ตามมาทั้งในทางบวกหรือทางลบ ดังนั้นหาก

พนักงานมีความรู้สึกถึงการเป็นเจ้าของสิ่งที่ได้รับมอบหมายมานั้น พนักงานจะรู้สึกว่าสิ่งที่ได้รับมอบหมายเป็นสิ่งที่ตนต้องทำและรับผิดชอบ เพื่อให้ตนได้รับการยกย่องจากบุคคลอื่นในองค์กร และหากมีภัยคุกคามหรือสิ่งที่อาจจะเป็นอันตราย พนักงานจะรับรู้ถึงความรับผิดรับชอบในการรักษาทรัพย์สินหรือมีความตั้งใจที่จะปฏิบัติตามหน้าที่ที่ได้รับมอบหมายเสมือนทุกสิ่งที่ได้รับมานั้นเป็นของตน ซึ่งทำให้พนักงานยอมปรับเปลี่ยนพฤติกรรมให้มีการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศขององค์กร ดังนั้นจึงสามารถตั้งสมมติฐานได้ว่า

H6: การรับรู้ถึงความรับผิดรับชอบส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย

Boss et al. (2009) กล่าวว่า การให้รางวัลเป็นการสร้างแรงจูงใจให้กับพนักงานที่ทำงานหรือมีพฤติกรรมที่ตอบสนองต่อความคาดหวังขององค์กร หรือเป็นสิ่งที่สามารถใช้แทนสัญญาที่องค์กรนำไปใช้ในการควบคุมการทำงานหรือการปฏิบัติตามกฎระเบียบของพนักงานภายในองค์กร โดยผ่านการให้รางวัลที่ไม่มีตัวตน เช่น การเลื่อนตำแหน่ง รางวัลพนักงานดีเด่นประจำเดือน เป็นต้น และการให้รางวัลที่มีตัวตน เช่น โบนัส หรือวันหยุด เป็นต้น การใช้วิธีการให้รางวัลอย่างเหมาะสมจะเป็นวิธีการควบคุมพฤติกรรมและประสิทธิภาพในการทำงานของพนักงานในองค์กรได้เป็นอย่างดี ได้แก่ การกำกับดูแลพฤติกรรมของพนักงาน การสร้างแรงจูงใจให้แก่พนักงาน การดึงดูดและรักษาความสามารถของพนักงาน อีกทั้งยังเพิ่มความพึงพอใจในการทำงานในตำแหน่งงานให้กับพนักงานด้วย ซึ่งสอดคล้องกับแนวคิดของ Bulgurcu et al. (2010) ที่กล่าวว่า การให้รางวัลสามารถช่วยในการบังคับให้พนักงานมีความตั้งใจที่จะปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศได้ หากพนักงานรับรู้ว่าได้รับสิ่งตอบแทนที่เหมาะสม ดังนั้นจึงสามารถตั้งสมมติฐานได้ว่า

H7: การให้รางวัลส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย

Chen et al. (2012) กล่าวว่า การควบคุมให้ปฏิบัติตามกฎระเบียบขององค์กรนั้น หลายองค์กรมักจะไม่ค่อยมีการควบคุมโดยการบีบบังคับหรือการควบคุมโดยการให้รางวัลเพียงอย่างใดอย่างหนึ่ง แต่จะใช้การควบคุมทั้งสองอย่างควบคู่กันในการควบคุมเพื่อเพิ่มการปฏิบัติตามของพนักงานในองค์กร เนื่องจากการบีบบังคับโดยการลงโทษหรือการให้รางวัลเพียงอย่างเดียวถือว่าเป็นปัจจัยที่มีอิทธิพลน้อยหรือไม่มีเลยในการให้ความร่วมมือของบุคคลในองค์กร แต่หากนำมาใช้ร่วมกันกลับมีผลกระทบอย่างมีนัยสำคัญในการบังคับใช้นโยบายซึ่งมีความสัมพันธ์กันอย่างมาก ซึ่งสอดคล้องกับแนวคิดของ Greitemeyer and Weiner (2008) ที่พบว่า ผลกระทบของการลงโทษขึ้นอยู่กับการให้รางวัล ซึ่งแสดงให้เห็นว่าการให้รางวัลและความรู้สึกของการบีบบังคับโดยการลงโทษไม่สมมาตรกัน เมื่อมีการให้รางวัลแก่บุคคลเพื่อเป็นแรงจูงใจให้มีการปฏิบัติตาม บุคคลจะมีการปฏิบัติตามมากกว่าการปฏิบัติตามเนื่องจากการถูกบีบบังคับโดยการลงโทษ เพราะการลงโทษจะถูกตีความจากพนักงานว่าเป็นการข่มขู่ ดังนั้นเพื่อให้การต่อต้านลดลง จึงควรที่จะมีการให้รางวัลเพื่อลดการตอบโต้หรือปฏิกิริยาต่อต้านทางอารมณ์ลง ซึ่งจะเห็นได้ว่าการให้รางวัลมีผลต่อการเปลี่ยนแปลงของความรู้สึกจากการถูกบีบบังคับโดยการลงโทษ ดังนั้นจึงสามารถตั้งสมมติฐานได้ว่า

H8: การให้รางวัลส่งผลทางลบต่อความรู้สึกของการบีบบังคับโดยการลงโทษ

Straub (1990) และ D'Arcy and Herath (2011) กล่าวว่า การลงโทษเป็นกลไกการยับยั้งและต่อต้านพฤติกรรมที่ไม่พึงประสงค์ เมื่อบุคคลทราบว่าองค์กรมีการควบคุมพฤติกรรมที่ไม่พึงประสงค์ ก็จะมีโอกาสน้อยลงที่จะกระทำความผิด การลงโทษมีตัวชี้วัดหลักอยู่ 3 องค์ประกอบ ประกอบด้วย ความรวดเร็วของการลงโทษ ความรุนแรงของการลงโทษและความสม่ำเสมอของการลงโทษ รวมถึงการรับรู้ถึงความเสี่ยงและค่าใช้จ่ายของการลงโทษ เพื่อช่วยบุคคลใน

การตัดสินใจว่าจะแสดงพฤติกรรมอย่างไร ซึ่งสอดคล้องกับแนวคิดของ Peace et al. (2003) ที่กล่าวว่า เมื่อพนักงานรับรู้ถึงบทลงโทษที่รุนแรง รวดเร็วและสม่ำเสมอแล้วนั้น พนักงานจะเกิดความรู้สึกถูกบีบบังคับให้ไม่ปฏิบัติตามในพฤติกรรมที่ไม่พึงประสงค์ต่อองค์กร และมีแนวโน้มที่จะหันมาตั้งใจที่จะปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ เพื่อหลีกเลี่ยงการถูกลงโทษ ดังนั้นจึงสามารถตั้งสมมติฐานได้ว่า

H9: ความรู้สึกของการบีบบังคับโดยการลงโทษส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย

Siponen (2000) กล่าวว่า การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศเป็นความรู้สึกนึกคิดของพนักงานที่รับรู้ถึงความสำคัญและเข้าใจถึงวัตถุประสงค์ของการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ ความเสี่ยงและภัยคุกคาม และแสวงหาความรู้ที่จำเป็นเกี่ยวกับหน้าที่ความรับผิดชอบในระบบสารสนเทศที่เกี่ยวข้อง ซึ่งสิ่งเหล่านี้เป็นส่วนสำคัญที่จะทำให้การรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศมีประสิทธิภาพมากขึ้น ทั้งนี้ Bulgurcu et al. (2010) กล่าวว่า การที่จะทำให้พนักงานในองค์กรปฏิบัติตามนโยบายที่จัดทำขึ้นนั้น ต้องทำให้เข้าใจง่ายและสามารถเข้าถึงได้ทุกที่ทุกเวลาที่พนักงานต้องการ ซึ่งสอดคล้องกับแนวคิดของ Dinev and Hu (2007) และ Haeussinger and Kranz (2013) ที่กล่าวว่า พนักงานจะมีการรับรู้และตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นและภัยคุกคามที่เป็นอันตรายจากการใช้เทคโนโลยีสารสนเทศในองค์กร เมื่อพนักงานมีความรู้และเข้าใจในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศมากขึ้น พนักงานจะมีแนวโน้มที่จะหาวิธีป้องกันโดยเกิดความตั้งใจที่จะปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศมากขึ้น ดังนั้นจึงสามารถตั้งสมมติฐานได้ว่า

H10: การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย

พฤติกรรมเป็นสิ่งที่เกิดจากการตระหนักโดยตรง ซึ่งการตระหนักถึงนั้นจะนำไปสู่พฤติกรรมที่ควรปฏิบัติ หากจะทำให้การตระหนักมีประสิทธิภาพนั้นต้องได้รับการสนับสนุนจากพนักงานและผู้มีส่วนได้เสียทุกคนที่ทำงานภายในองค์กร ซึ่งสอดคล้องกับแนวคิดของ Dinev and Hu (2007), D'Arcy et al. (2009) และ Bulgurcu et al. (2010) ที่กล่าวว่า หากบุคคลมีการตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศแล้วนั้น ย่อมส่งผลให้บุคคลนั้นมีแนวโน้มที่จะแสดงพฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศด้วย ดังนั้นจึงสามารถตั้งสมมติฐานได้ว่า

H11: การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยส่งผลทางบวกต่อพฤติกรรมในการรักษาความมั่นคงปลอดภัย

Shropshire et al. (2015) กล่าวว่า ความตั้งใจที่จะแสดงพฤติกรรมเป็นสิ่งที่ชี้วัดหรือทำนายการแสดงออกถึงพฤติกรรมที่แท้จริงทางด้านเทคโนโลยีสารสนเทศ โดยจากงานวิจัยต่าง ๆ ที่ทำการศึกษาในเรื่องนี้ได้ยอมรับว่า ความตั้งใจที่จะปฏิบัติตามนโยบายเป็นการที่บุคคลมีแรงจูงใจที่จะปกป้องทรัพย์สินทางด้านสารสนเทศขององค์กรจากภัยคุกคามต่างๆ ด้วยเครื่องมือที่องค์กรจัดทำขึ้น ได้แก่ นโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ ซึ่งส่งผลให้บุคคลนั้นเกิดความรู้สึกที่ดีและตั้งใจที่จะปฏิบัติตามนโยบายนั้น บุคคลก็จะมีแนวโน้มที่จะแสดงออกถึงพฤติกรรมการรักษาความปลอดภัยทางด้านสารสนเทศ ซึ่งสอดคล้องกับแนวคิดของ Yoon et al. (2012) ที่กล่าวว่า หากพนักงานมีความตั้งใจที่จะปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศแล้วนั้น พนักงาน

ก็จะมีแนวโน้มที่จะแสดงออกถึงพฤติกรรมในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศด้วย ดังนั้นจึงสามารถตั้งสมมติฐานได้ว่า

H12: ความตั้งใจที่จะปฏิบัติตามนโยบายส่งผลทางบวกต่อพฤติกรรมในการรักษาความมั่นคงปลอดภัย

4. วิธีการวิจัย

งานวิจัยนี้จัดเก็บข้อมูลจากกลุ่มตัวอย่างที่เป็นพนักงานในองค์กรทั้งภาครัฐบาลและภาคเอกชน โดยองค์กรดังกล่าวจะต้องมีนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ (Information security policy) จำนวน 229 กลุ่มตัวอย่าง ด้วยแบบสอบถามทั้งในรูปแบบกระดาษและอิเล็กทรอนิกส์ ซึ่งจัดสร้างขึ้นมาจากการค้นคว้าข้อมูลทางเอกสารและงานวิจัยที่เกี่ยวข้อง (ประกอบด้วย Tsai et al., 2016; Safa et al., 2016; Liang and Xue, 2010; Chen and Zahedi, 2016; Ifinedo, 2012; Lee et al., 2016; Al-Omari et al., 2013; Hu et al., 2012; Dinev and Hu, 2007; Hochwarter et al., 2005; Vance et al., 2015; Chen et al., 2012; Bulgurcu et al., 2010; Siponen et al., 2009; Cavallari, 2011; Peace et al., 2003; Son, 2011; Hanus and Wu, 2016; Siponen et al., 2007; Kaur and Mustafa, 2013; Siponen et al., 2010) นำไปทดสอบกับกลุ่มตัวอย่าง จำนวน 22 คน เพื่อวิเคราะห์แบบสอบถามเบื้องต้นและปรับปรุงข้อคำถามในแบบสอบถามให้มีความเหมาะสมก่อนนำไปจัดเก็บข้อมูลจริง โดยแจกแบบสอบถามอิเล็กทรอนิกส์ผ่านสื่อสังคมออนไลน์ และเริ่มจัดส่งแบบสอบถามตั้งแต่ต้นเดือนพฤษภาคมจนถึงสิ้นเดือนพฤษภาคม พ.ศ. 2560 พบว่า มีผู้ตอบแบบสอบถามไม่ครบตามจำนวนที่ต้องการ จึงแจกแบบสอบถามในรูปแบบกระดาษด้วยการส่งผ่านคนรู้จักที่ทำงานในองค์กรต่าง ๆ ที่มีนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ จนถึงวันที่ 10 มิถุนายน พ.ศ. 2560 รวมระยะเวลาในการจัดเก็บข้อมูลประมาณ 1 เดือน

5. ผลการวิจัย

5.1 การทดสอบข้อตกลงเบื้องต้นทางสถิติ

ข้อมูลที่จัดเก็บจากกลุ่มตัวอย่างถูกนำไปทดสอบข้อมูลขาดหาย (Missing data) ข้อมูลสุดโต่ง (Outliners) การกระจายแบบปกติ (Normal) ความสัมพันธ์เชิงเส้นตรง (Linearity) ภาวะร่วมเส้นตรงพหุ (Multicollinearity) และภาวะร่วมเส้นตรง (Singularity) ซึ่งจากการทดสอบพบว่า ข้อมูลไม่มีส่วนใดขาดหาย มีความสัมพันธ์เชิงเส้นตรง และไม่มีปัญหาภาวะร่วมเส้นตรงพหุและภาวะร่วมเส้นตรง ซึ่งถือว่าผ่านเกณฑ์ตามที่กำหนดทั้งหมด มีเพียงบางตัวแปรเท่านั้นที่ไม่ได้มีการกระจายแบบปกติ โดยมีการกระจายข้อมูลแบบเบ้ซ้าย แต่มีความเบ้ต่างจากเกณฑ์มาตรฐานไม่มากนัก ทางผู้วิจัยจึงยังคงใช้ข้อมูลดังกล่าววิเคราะห์ข้อมูลทางสถิติต่อไป

5.2 การประเมินความเที่ยงและความตรงของแบบสอบถาม

งานวิจัยนี้ทดสอบความเชื่อถือได้ของแบบสอบถาม โดยใช้การทดสอบความเที่ยงของแบบสอบถาม (Reliability) จากการวิเคราะห์ค่าประสิทธิ์แอลฟาของครอนบาซ (Cronbach's alpha) ที่มีค่ามากกว่า 0.70 ซึ่งถือว่ามีความเชื่อถือได้สำหรับงานวิจัยแบบ Basic research และได้ทดสอบความตรงของแบบสอบถาม (Validity) ด้วยการวิเคราะห์องค์ประกอบ (Factor analysis) โดยต้องมีค่าน้ำหนักองค์ประกอบ (Factor loading) มากกว่า 0.5 (สุพิชญา อาชวจิรดา, 2557) ดังแสดงค่าสถิติของแต่ละข้อคำถามที่ผ่านเกณฑ์ตามตารางที่ 1

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน น้ำหนักองค์ประกอบและค่าสัมประสิทธิ์แอลฟา ของครอนบาซของตัวแปรทั้งหมด

ปัจจัย	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	น้ำหนักองค์ประกอบ
ปัจจัย 1: ประสบการณ์ก่อนหน้าจากการเผชิญกับภัยคุกคาม (% of variance = 83.222, Cronbach's alpha = 0.896)			
ท่านสามารถประเมินได้ว่าเหตุการณ์ใดเป็นภัยคุกคาม โดยใช้ประสบการณ์ของท่าน	3.900	0.6444	0.929
ท่านเชื่อว่าท่านสามารถใช้ประสบการณ์ที่ผ่านมาเพื่อจัดการกับเหตุการณ์ที่ท่านรู้สึกว่าจะเป็นภัยอันตรายต่อความมั่นคงปลอดภัยทางสารสนเทศที่อาจเกิดขึ้นในปัจจุบัน	3.917	0.5902	0.920
การเผชิญกับภัยคุกคามมาแล้ว ทำให้ท่านมีความระมัดระวังและช่วยทำให้ท่านหาวิธีป้องกันได้ง่ายขึ้น	4.083	0.6800	0.887
ปัจจัย 2: การรับรู้ภัยคุกคาม (% of variance = 52.212, Cronbach's alpha = 0.757)			
ท่านเชื่อว่าการพยายามที่จะปกป้องข้อมูลสารสนเทศขององค์กร จะช่วยลดการเข้าถึงที่ไม่ได้รับอนุญาตได้	3.860	0.6473	0.837
ท่านกังวลว่า ข้อมูลสารสนเทศและทรัพยากรขององค์กรจะได้รับความเสียหายจากการถูกบุกรุกที่เกิดจากช่องโหว่ของระบบสารสนเทศ	3.926	0.5687	0.780
ท่านมีความกังวลว่า ท่านจะตกเป็นเหยื่อและเกิดความสูญเสียจากการโจมตีที่เป็นอันตรายต่อความมั่นคงปลอดภัยทางด้านสารสนเทศ จากการใช้งานคอมพิวเตอร์ที่ไม่ถูกวิธีของท่าน	3.812	0.6975	0.748
หากคอมพิวเตอร์ของท่านติดไวรัส สปายแวร์ ท่านมีความรู้สึกเสี่ยงและไม่สบายใจในการใช้คอมพิวเตอร์ของท่าน	3.786	0.6899	0.687
ท่านเชื่อว่า องค์กรของท่านอาจเกิดความเสี่ยงต่อระบบสารสนเทศ เมื่อท่านฝ่าฝืนกฎระเบียบที่องค์กรกำหนด	3.965	0.7000	0.521

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน น้ำหนักองค์ประกอบและค่าสัมประสิทธิ์แอลฟา ของครอนบาซของตัวแปรทั้งหมด (ต่อ)

ปัจจัย	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	น้ำหนักองค์ประกอบ
ปัจจัย 3: ความเชื่อในความสามารถของตนเอง (% of variance = 67.335, Cronbach's alpha = 0.879)			
ท่านมีทักษะในการใช้มาตรการป้องกันเพื่อหยุดผู้ที่จะเข้ามาโจมตีคอมพิวเตอร์ที่ท่านใช้ในการทำงาน เช่น การติดตั้งซอฟต์แวร์ป้องกันไวรัส การใช้รหัสผ่านอย่างเหมาะสม การปิดการใช้ cookies เป็นต้น	3.511	0.8915	0.863
การใช้งานโปรแกรมต่าง ๆ ทางด้านการรักษาความมั่นคงปลอดภัยบนคอมพิวเตอร์ที่ใช้ในการทำงานเป็นเรื่องง่ายสำหรับท่าน	3.563	0.8438	0.843
ท่านเชื่อว่า ท่านสามารถที่จะควบคุมและป้องกันตนเองจากการโจมตีระบบสารสนเทศขององค์กรได้	3.541	0.8399	0.809
ท่านเชื่อว่า ท่านมีทักษะที่เพียงพอสำหรับจัดการกับภัยคุกคาม ต่าง ๆ ที่องค์กรต้องจำกัดได้	3.389	0.7735	0.800
ท่านมีความเชี่ยวชาญในการดำเนินการตามมาตรการป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าถึงข้อมูลที่เป็นความลับของท่านได้	3.371	0.7987	0.786
ปัจจัย 4: การคล้อยตามกลุ่มอ้างอิง (% of variance = 68.235, Cronbach's alpha = 0.878)			
ท่านทำในสิ่งที่เพื่อนร่วมงานของท่านคิดว่าท่านควรจะทำ	3.886	0.6249	0.900
ท่านทำในสิ่งที่ผู้บังคับบัญชาของท่านคิดว่าท่านควรจะทำ	4.017	0.5995	0.877
ท่านทำในสิ่งที่ผู้ใต้บังคับบัญชาของท่านคิดว่าท่านควรจะทำ	3.825	0.6590	0.862
ท่านทำในสิ่งที่แผนกเทคโนโลยีสารสนเทศขององค์กรของท่านคิดว่าท่านควรจะทำ	4.004	0.6589	0.799
ท่านมีแนวโน้มที่จะทำตามพฤติกรรมที่บุคคลที่มีอิทธิพลและมีความสำคัญกับท่านแสดงออกมา	3.782	0.6724	0.672

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน น้ำหนักองค์ประกอบและค่าสัมประสิทธิ์แอลฟา ของครอนบาซของตัวแปรทั้งหมด (ต่อ)

ปัจจัย	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	น้ำหนักองค์ประกอบ
ปัจจัย 5: ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย (% of variance = 76.347, Cronbach's alpha = 0.922)			
ท่านเชื่อว่า การกำหนดนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศที่ชัดเจนขององค์กร จะเป็นประโยชน์ต่อการปฏิบัติตามและการใช้เทคโนโลยีของท่าน	4.293	0.6191	0.778
ท่านเชื่อว่า การบังคับใช้นโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ จะเป็นประโยชน์ต่อการปฏิบัติตามและการใช้เทคโนโลยีของท่าน	4.223	0.6270	0.768
ท่านคิดว่า การปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศเป็นความคิดที่ดี	4.367	0.6254	0.770
ท่านคิดว่า การปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศเป็นสิ่งที่จำเป็น	4.362	0.6520	0.784
สำหรับท่านแล้ว การจำกัดและปกป้องเครื่องคอมพิวเตอร์จากสปายแวร์หรือ ไวรัส เป็นความคิดที่ดี	4.393	0.6092	0.718
ปัจจัย 6: การรับรู้ถึงความรับผิดรับชอบ (% of variance = 53.632, Cronbach's alpha = 0.710)			
ท่านคิดว่า การใช้งานระบบสารสนเทศขององค์กรอย่างระมัดระวัง คือสิ่งที่ท่านควรทำ	4.371	0.6670	0.775
ท่านมีส่วนสำคัญในการทำให้เกิดความสำเร็จหรือความล้มเหลวของงานที่ได้รับมอบหมาย	3.978	0.6451	0.757
ท่านคิดว่า ท่านสามารถดูแลและรักษาทรัพย์สินในองค์กรของท่านเสมือนกับเป็นทรัพย์สินของท่านเอง	4.170	0.6700	0.752
องค์กรของท่านให้ท่านรับผิดชอบต่อการกระทำทั้งหมดของท่านในการใช้งานระบบสารสนเทศขององค์กร	3.716	0.6302	0.637
ปัจจัย 7: การให้รางวัล (% of variance = 59.711, Cronbach's alpha = 0.864)			
เมื่อท่านทำตามกฎระเบียบที่องค์กรกำหนด ท่านจะได้รับการ ชื่นชม	3.590	0.7707	0.802
เมื่อท่านทำตามสิ่งที่องค์กรต้องการ ท่านจะได้รับรางวัลที่เป็นตัวเงิน เช่น การขึ้นเงินเดือน เป็นต้น	3.555	0.8444	0.790
เมื่อท่านกระทำสิ่งที่เป็นประโยชน์หรือสร้างชื่อเสียงให้กับองค์กร ท่านจะได้รับรางวัลจากองค์กร เช่น เลื่อนตำแหน่ง รางวัลพนักงานดีเด่น เป็นต้น	3.690	0.8403	0.787

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน น้ำหนักองค์ประกอบและค่าสัมประสิทธิ์แอลฟา ของครอนบาซของตัวแปรทั้งหมด (ต่อ)

ปัจจัย	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	น้ำหนักองค์ประกอบ
ปัจจัย 7: การให้รางวัล (ต่อ)			
ท่านรู้สึกว่า รางวัลทำให้ท่านเต็มใจที่จะทำสิ่งใด ๆ มากกว่าการถูกบีบบังคับให้ทำสิ่งนั้น	3.769	0.8903	0.785
เมื่อท่านทำตามสิ่งที่องค์กรต้องการ ท่านจะได้รับรางวัลที่ไม่เป็นตัวเงิน เช่น คำชมเชย ชื่อเสียง เป็นต้น	3.537	0.7693	0.772
ท่านคิดว่า องค์กรมีการให้รางวัลกับท่านอย่างเหมาะสม เมื่อเปรียบเทียบกับสิ่งที่ท่านกระทำ	3.402	0.8085	0.696
ปัจจัย 8: ความรู้สึกของการบีบบังคับโดยการลงโทษ (% of variance = 59.128, Cronbach's alpha = 0.826)			
เมื่อท่านไม่ทำในสิ่งที่กำหนดไว้ในกฎระเบียบขององค์กร ท่านมีแนวโน้มที่จะได้รับการลงโทษ	3.821	0.6807	0.849
องค์กรของท่านจะลงโทษบุคคลที่นำทรัพยากรทางคอมพิวเตอร์ขององค์กรไปใช้เพื่อประโยชน์ส่วนตัว	3.852	0.6785	0.773
ผู้บังคับบัญชาของท่านจะว่ากล่าวตักเตือนหรือกระทำการใด ๆ ซึ่งแสดงให้เห็นถึงความเข้มงวดในกฎระเบียบที่องค์กรกำหนดขึ้น	3.882	0.5990	0.772
หากท่านฝ่าฝืนกฎระเบียบที่องค์กรกำหนดและถูกจับได้ ท่านจะได้รับการลงโทษอย่างรุนแรงทันที	3.939	0.5966	0.722
ท่านรู้สึกว่า การลงโทษเป็นปัญหาใหญ่สำหรับท่าน	3.943	0.6361	0.722
ปัจจัย 9: การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย (% of variance = 69.032, Cronbach's alpha = 0.887)			
ท่านรู้และเข้าใจเหตุผลว่าทำไมองค์กรของท่านต้องมีการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ	4.437	0.6567	0.873
ท่านรู้ว่าท่านต้องรับผิดชอบตามที่กำหนดในนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรของท่าน เพื่อเพิ่มการรักษาความมั่นคงปลอดภัยขององค์กรของท่าน	4.362	0.6587	0.860
ท่านทราบเกี่ยวกับผลกระทบที่ตามมาจากการที่ท่านไม่ปฏิบัติตามระเบียบที่องค์กรกำหนด	4.249	0.6908	0.845
เมื่อท่านเข้าใช้งานระบบสารสนเทศขององค์กร ท่านจะคิดถึงกฎระเบียบและข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยเสมอ	4.297	0.6616	0.823
การปกป้องข้อมูลของลูกค้า พนักงาน และคู่ค้า มีความสำคัญมากสำหรับองค์กรของท่าน	4.607	0.6020	0.747

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน น้ำหนักองค์ประกอบและค่าประสิทธิ์แอลฟา ของครอนบาซของตัวแปรทั้งหมด (ต่อ)

ปัจจัย	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	น้ำหนักองค์ประกอบ
ปัจจัย 10: ความตั้งใจที่จะปฏิบัติตามนโยบาย (% of variance = 76.508, Cronbach's alpha = 0.923)			
ท่านตั้งใจที่จะทำหน้าที่ของท่านตามที่ได้กำหนดไว้ในนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรของท่าน เมื่อท่านใช้ข้อมูลสารสนเทศและเทคโนโลยีในอนาคต	4.293	0.6400	0.909
ท่านตั้งใจที่จะปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรของท่านในอนาคต	4.288	0.6176	0.881
ท่านตั้งใจที่จะปกป้องข้อมูลสารสนเทศและทรัพยากรทางด้านเทคโนโลยีตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรของท่านในอนาคต	4.332	0.6310	0.877
ท่านมั่นใจว่า ท่านจะปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กร เมื่อเป็นไปได้	4.271	0.6113	0.861
สำหรับท่านแล้ว การปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศอย่างต่อเนื่องเป็นความตั้งใจของท่าน	4.227	0.6495	0.845
ปัจจัย 11: พฤติกรรมในการรักษาความมั่นคงปลอดภัย (% of variance = 61.074, Cronbach's alpha = 0.832)			
ท่านปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศทุกครั้ง เมื่อท่านทำงานประจำวัน	4.192	0.7180	0.851
ท่านมีพฤติกรรมในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศตามที่นโยบายขององค์กรแนะนำ มากเท่าที่จะเป็นไปได้	4.205	0.7296	0.815
ท่านแนะนำและช่วยเหลือให้ผู้อื่นในองค์กร ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศเช่นเดียวกับท่าน	3.882	0.8579	0.805
ท่านมีโปรแกรมสแกนไวรัสติดตั้งไว้ที่เครื่องคอมพิวเตอร์ของท่าน และมีการอัปเดตอยู่ตลอดเวลา	4.192	0.9213	0.725
ท่านจะไม่เปิดอ่านไฟล์เอกสารที่แนบมากับอีเมล หากเนื้อหาในอีเมลนั้นดูน่าสงสัย	4.258	0.8319	0.701

5.3 ลักษณะทางประชากรศาสตร์ของกลุ่มตัวอย่าง

กลุ่มตัวอย่างส่วนใหญ่เป็นเพศหญิงมากกว่าเพศชาย (ร้อยละ 63.80) โดยอยู่ในช่วงอายุ 26-30 ปี (ร้อยละ 45.40) ระดับการศึกษาสูงสุดอยู่ในระดับปริญญาตรีและทำงานในองค์กรด้านธุรกิจบริการ (ร้อยละ 17.00) และธุรกิจการเงินและการธนาคาร (ร้อยละ 14.90) ทั้งนี้อายุการทำงานในหน่วยงานยังอยู่ในช่วงน้อยกว่า 3 ปี (ร้อยละ 36.20) ระดับความรู้เกี่ยวกับคอมพิวเตอร์และเทคโนโลยีอยู่ในระดับปานกลาง (ร้อยละ 53.30) ทั้งนี้องค์กรของกลุ่มตัวอย่างยังมีการให้ยืมเครื่องคอมพิวเตอร์พกพา (Laptop) หรืออนุญาตให้ใช้อุปกรณ์ Smart device ส่วนบุคคลในการทำงานด้วย (ร้อยละ 79.50)

5.4 การทดสอบสมมติฐานการวิจัย

งานวิจัยนี้ทดสอบสมมติฐานการวิจัยจากกรอบแนวคิดการวิจัยด้วยการวิเคราะห์การถดถอยแบบเชิงชั้น (Hierarchical regression) ผลลัพธ์ที่ได้แสดงในภาพที่ 2 และตารางที่ 2 โดยใช้ค่า p-value ที่น้อยกว่าหรือเท่ากับ 0.05 เป็นตัวกำหนดนัยสำคัญทางสถิติ ซึ่งแสดงคะแนนมาตรฐาน (Standardized score) โดยสามารถวิเคราะห์ผลทางสถิติได้ดังนี้

5.4.1 ความรู้สึกของการบีบบังคับโดยการลงโทษ ผลทางสถิติแสดงให้เห็นว่า การให้รางวัลส่งอิทธิพลทางตรงต่อความรู้สึกของการบีบบังคับโดยการลงโทษ ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.135 และมีความผันแปรของตัวแปรตามเท่ากับร้อยละ 1.8 (R^2 = 0.018) ซึ่งจากการวิเคราะห์ข้อมูลพบว่า การให้รางวัลไม่สนับสนุนสมมติฐานการวิจัยที่ 8 ที่กล่าวว่า การให้รางวัลส่งผลทางลบต่อความรู้สึกของการบีบบังคับโดยการลงโทษ เนื่องจากค่าสัมประสิทธิ์อิทธิพลมีเครื่องหมายบวก ซึ่งมีทิศทางตรงกันข้ามกับสมมติฐานการวิจัยที่ตั้งไว้ โดยอาจมีสาเหตุจากบริบทของกลุ่มตัวอย่างในองค์กรของไทยมักจะปฏิเสธหรือหลีกเลี่ยงความเป็นจริง เพื่อให้ตนเองปลอดภัยและลดความเสี่ยงที่อาจเกิดขึ้น เพราะคำถามเกี่ยวกับเรื่องการให้รางวัลและความรู้สึกของการบีบบังคับโดยการลงโทษค่อนข้างเป็นเรื่องลึกซึ้งในความคิดของคนไทย ที่จะไม่ยอมให้ความไม่แน่นอนหรือภัยเกิดขึ้นกับตนเองและพยายามที่จะหาทางลดความไม่แน่นอนหรือความเสี่ยงที่เกิดขึ้นกับตน จึงอาจทำให้มีการตอบไม่ตรงกับความเป็นจริงทั้งหมด (สุธีรา เดชนครินทร์ และ สุธินี ฤกษ์ขำ, 2558) จึงส่งผลให้ข้อมูลที่ได้ไม่สนับสนุนสมมติฐานดังกล่าว

5.4.2 การรับรู้ภัยคุกคาม ผลทางสถิติแสดงให้เห็นว่า ประสบการณ์ก่อนหน้าจากการเผชิญกับภัยคุกคามส่งอิทธิพลทางตรงต่อการรับรู้ภัยคุกคาม ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.272 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 และมีความผันแปรของตัวแปรตามเท่ากับร้อยละ 7.4 (R^2 = 0.074) ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 1 ที่กล่าวว่า ประสบการณ์ก่อนหน้าจากการเผชิญกับภัยคุกคามส่งผลทางบวกต่อการรับรู้ภัยคุกคาม ซึ่งสอดคล้องกับงานวิจัยของ Albrechtsen (2007) และ Lee et al. (2008) ที่กล่าวว่า ประสบการณ์ก่อนหน้าจะเกิดจากความคุ้นเคยหรือการรับรู้ถึงเหตุการณ์หรือภัยคุกคามที่เกิดขึ้นจากการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศในอดีตของแต่ละบุคคล ซึ่งมีส่วนช่วยในการตอบสนองและรับรู้ถึงภัยคุกคามที่เกิดขึ้น ทั้งนี้จะมีความตั้งใจที่จะพยายามจัดการ หาทางป้องกันและลดความเสี่ยงจากภัยคุกคามที่อาจเกิดขึ้น เพื่อไม่ให้ส่งผลกระทบร้ายแรงต่อองค์กร

5.4.3 ความตั้งใจที่จะปฏิบัติตามนโยบาย ผลทางสถิติแสดงให้เห็นว่า การรับรู้ภัยคุกคาม ความเชื่อในความสามารถของตนเอง การคล้อยตามกลุ่มอ้างอิง ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย การรับรู้ถึงความรับผิดรับชอบ การให้รางวัล ความรู้สึกของการบีบบังคับโดยการลงโทษ การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย และประสบการณ์ก่อนหน้าจากการเผชิญกับภัยคุกคาม ส่งอิทธิพลต่อความตั้งใจที่จะปฏิบัติตามนโยบาย โดยมีความผันแปรของตัวแปรตามเท่ากับร้อยละ 65.70 (R^2 = 0.657) รายละเอียดของอิทธิพลแต่ละปัจจัยมีดังนี้

5.4.3.1 การรับรู้ภัยคุกคาม ส่งอิทธิพลทางตรงต่อความตั้งใจที่จะปฏิบัติตามนโยบายที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.228 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 2 ที่กล่าวว่า การรับรู้ภัยคุกคามส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ซึ่งสอดคล้องกับงานวิจัยของ Ifinedo (2012); Herath and Rao (2009) และ Yoon et al. (2012) ที่กล่าวว่า การรับรู้ภัยคุกคามทางด้านความปลอดภัยจะเกิดขึ้น เมื่อบุคคลมีการประเมินภัยคุกคามและอันตรายจากการไม่ปฏิบัติตามหรือรับรู้ช่องโหว่ที่เกิดขึ้น จะทำให้บุคคลมีความตั้งใจที่จะมีส่วนร่วมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ

5.4.3.2 ความเชื่อในความสามารถของตนเอง ส่งอิทธิพลทางตรงต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.138 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 3 ที่กล่าวว่า ความเชื่อในความสามารถของตนเองส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ซึ่งสอดคล้องกับงานวิจัยของ Stajkovic and Luthans (1988) และ Herath and Rao (2009) ที่กล่าวว่า ความเชื่อในความสามารถของตนเองได้รับการแสดงให้เป็นปัจจัยที่มีผลกระทบต่อการใช้งานด้านเทคโนโลยีสารสนเทศด้วย หากบุคคลมีความมั่นใจ

ว่าตนมีทักษะและความสามารถเพียงพอในการดำเนินกิจกรรมต่างๆ บุคคลก็จะมีแนวโน้มที่จะตั้งใจที่จะกระทำกิจกรรมต่างๆ นั้น

5.4.3.3 การคล้อยตามกลุ่มอ้างอิง ส่งอิทธิพลทางตรงต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.155 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 4 ที่กล่าวว่า การคล้อยตามกลุ่มอ้างอิงส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ซึ่งสอดคล้องกับงานวิจัยของ Pahnila et al. (2007); Herath and Rao (2009); Bulgurcu et al. (2010) และ Ifinedo (2014) ที่กล่าวว่า การคล้อยตามกลุ่มอ้างอิงเป็นที่ยอมรับกันอย่างกว้างขวางในการทบทวนวรรณกรรมที่เกี่ยวข้องกับความตั้งใจที่จะแสดงออกถึงพฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศอย่างมีนัยสำคัญ เมื่อพนักงานได้เห็นหรือรับรู้ว่าบุคคลรอบข้างหรือมีความใกล้ชิดมีการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ พนักงานเหล่านี้ก็มีแนวโน้มที่จะปฏิบัติตามด้วย

5.4.3.4 ทัศนคติที่มีต่อการปฏิบัตินโยบาย ส่งอิทธิพลทางตรงต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.121 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 5 ที่กล่าวว่า ทัศนคติที่มีต่อการปฏิบัติตามนโยบายส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ซึ่งสอดคล้องกับงานวิจัยของ Bulgurcu et al. (2010) และ Ifinedo (2014) ที่กล่าวว่า หากพนักงานมีความเชื่อและทัศนคติในเชิงบวกเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรแล้วนั้น ก็จะมีแนวโน้มที่ดีในการปฏิบัติตามกฎระเบียบและแนวทางดังกล่าว

5.4.3.5 การรับรู้ถึงความรับผิดรับชอบ ส่งอิทธิพลทางตรงต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.193 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 6 ที่กล่าวว่า การรับรู้ถึงความรับผิดรับชอบส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ซึ่งสอดคล้องกับงานวิจัยของ Vance et al. (2015) ที่กล่าวว่า หากพนักงานมีความรับผิดรับชอบเพิ่มขึ้นจะทำให้พนักงานลดความคิดที่จะละเมิดนโยบายฯ และหันมามีความตั้งใจที่จะปฏิบัติตามนโยบายเพิ่มขึ้น ซึ่งแสดงให้เห็นถึงการรับรู้ถึงความรับผิดรับชอบต่อการปฏิบัติตามนโยบายนั้น

5.4.3.6 การให้รางวัล ส่งอิทธิพลทางตรงต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ -0.123 และส่งอิทธิพลทางอ้อมผ่านความรู้สึกของการบีบบังคับโดยการลงโทษไปยังความตั้งใจที่จะปฏิบัติตามนโยบาย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ -0.026 จากการวิเคราะห์ข้อมูลพบว่า การให้รางวัลไม่สนับสนุนสมมติฐานการวิจัยที่ 7 ที่กล่าวว่า การให้รางวัลส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย เนื่องจากค่าสัมประสิทธิ์อิทธิพลมีเครื่องหมายลบ ซึ่งมีทิศทางตรงกันข้ามกับสมมติฐานการวิจัยที่ตั้งไว้ อาจมีสาเหตุเนื่องจากกลุ่มตัวอย่างตีความว่าการให้รางวัลเป็นเสมือนเครื่องมือในการควบคุมพฤติกรรมและรู้สึกว่าได้รับสิ่งตอบแทนไม่คุ้มค่ากับสิ่งที่ตนจะต้องปฏิบัติตาม

5.4.3.7 ความรู้สึกของการบีบบังคับโดยการลงโทษ ส่งอิทธิพลทางตรงต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ -0.195 จากการวิเคราะห์ข้อมูลพบว่า ความรู้สึกของการบีบบังคับโดยการลงโทษไม่สนับสนุนสมมติฐานการวิจัยที่ 9 ที่กล่าวว่า ความรู้สึกของการบีบบังคับโดยการลงโทษส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย เนื่องจากค่าสัมประสิทธิ์อิทธิพลมีเครื่องหมายลบ ซึ่งมีทิศทางตรงกันข้ามกับสมมติฐานการวิจัยที่ตั้งไว้ โดยอาจมีสาเหตุมาจากการวัดความรู้สึกของการบีบบังคับโดยการลงโทษเป็นเรื่องที่วัดค่อนข้างยากในบริบทของกลุ่มตัวอย่างองค์กรในประเทศไทยซึ่งพนักงานส่วนใหญ่ไม่มีการรับรู้ถึงบทลงโทษอย่างแน่ชัด ว่าหากตนกระทำความผิด ไม่ปฏิบัติตามหรือละเมิดนโยบายฯ แล้วนั้น จะส่งผลอย่างไรต่อตนเองบ้าง และรูปแบบการลงโทษที่รุนแรงอาจไม่ก่อให้เกิดความกลัวต่อผู้ใช้งานระบบสารสนเทศ แต่อาจเป็นการเพิ่มความรู้สึกต่อต้านของบุคคล จนนำไปสู่การไม่สนใจที่จะปฏิบัติตามนโยบายด้วย ซึ่งสอดคล้องกับงานวิจัยของ Herath and Rao (2009) ที่พบว่า ในการศึกษางานวิจัยต่างๆ ที่มีปัจจัยเรื่องของการยับยั้งการละเมิดนโยบายฯ โดยการลงโทษนั้น มีผลการวิจัยที่

แตกต่างกันออกไป ซึ่งมีทั้งทางบวกและทางลบ โดยสามารถชี้ให้เห็นว่า การลงโทษอาจไม่จำเป็นต้องรุนแรง แต่องค์กรควรควบคุมพนักงานโดยการติดตั้งระบบควบคุมในคอมพิวเตอร์ เพื่อเป็นการเฝ้าระวังและชดเชยการควบคุมด้วยวิธีการสังเกตการณ์หรือการสอบถามจะเหมาะสมกว่า

5.4.3.8 การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย ส่งอิทธิพลทางตรงต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.474 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 10 ที่กล่าวว่า การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ซึ่งสอดคล้องกับงานวิจัยของ Dinev and Hu (2007), Bulgurcu et al. (2010) และ Haeussinger and Kranz (2013) ที่กล่าวว่า การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของพนักงานเป็นส่วนสำคัญที่จะทำให้การจัดการเกี่ยวกับการรักษาความมั่นคงปลอดภัยมีประสิทธิภาพ

5.4.3.9 ประสบการณ์ก่อนหน้าจากการเผชิญกับภัยคุกคาม ส่งอิทธิพลทางอ้อมผ่านการรับรู้ภัยคุกคามไปยังความตั้งใจที่จะปฏิบัติตามนโยบาย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.062 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

5.4.4 พฤติกรรมในการรักษาความมั่นคงปลอดภัย ผลทางสถิติแสดงให้เห็นว่า การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย ความตั้งใจที่จะปฏิบัติตามนโยบาย การรับรู้ภัยคุกคาม ความเชื่อในความสามารถของตนเอง การคล้อยตามกลุ่มอ้างอิง ทัศนคติที่มีต่อการปฏิบัตินโยบาย การรับรู้ถึงความรับผิดรับชอบ การให้รางวัล ความรู้สึกของการบีบบังคับโดยการลงโทษ ส่งอิทธิพลต่อพฤติกรรมในการรักษาความมั่นคงปลอดภัย โดยมีความผันแปรของตัวแปรตามเท่ากับร้อยละ 36.40 (R^2 = 0.364) รายละเอียดของอิทธิพลแต่ละปัจจัยมีดังนี้

5.4.4.1 การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย ส่งอิทธิพลทางตรงต่อพฤติกรรมในการรักษาความมั่นคงปลอดภัย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.283 และส่งอิทธิพลทางอ้อมผ่านความตั้งใจที่จะปฏิบัติตามนโยบายไปยังพฤติกรรมในการรักษาความมั่นคงปลอดภัย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.175 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 11 ที่กล่าวว่า การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยส่งผลทางบวกต่อพฤติกรรมในการรักษาความมั่นคงปลอดภัย ซึ่งสอดคล้องกับงานวิจัยของ Bulgurcu et al. (2010) ที่กล่าวว่า พฤติกรรมเป็นสิ่งที่เกิดจากการตระหนักโดยตรง ซึ่งการตระหนักถึงนั้นจะนำไปสู่พฤติกรรมที่ควรปฏิบัติตาม

5.4.4.2 ความตั้งใจที่จะปฏิบัติตามนโยบาย ส่งอิทธิพลทางตรงต่อพฤติกรรมในการรักษาความมั่นคงปลอดภัย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.369 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 12 ที่กล่าวว่า ความตั้งใจที่จะปฏิบัติตามนโยบายส่งผลทางบวกต่อพฤติกรรมในการรักษาความมั่นคงปลอดภัย ซึ่งสอดคล้องกับงานวิจัยของ Yoon et al. (2012) ที่กล่าวว่า พนักงานที่มีความตั้งใจที่จะปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ จะมีแนวโน้มที่จะแสดงออกถึงพฤติกรรมในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศด้วย

5.4.4.3 การรับรู้ภัยคุกคาม ส่งอิทธิพลทางอ้อมผ่านความตั้งใจที่จะปฏิบัติตามนโยบายไปยังพฤติกรรมในการรักษาความมั่นคงปลอดภัย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.084 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

5.4.4.4 ความเชื่อในความสามารถของตนเอง ส่งอิทธิพลทางอ้อมผ่านความตั้งใจที่จะปฏิบัติตามนโยบายไปยังพฤติกรรมในการรักษาความมั่นคงปลอดภัย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.051 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

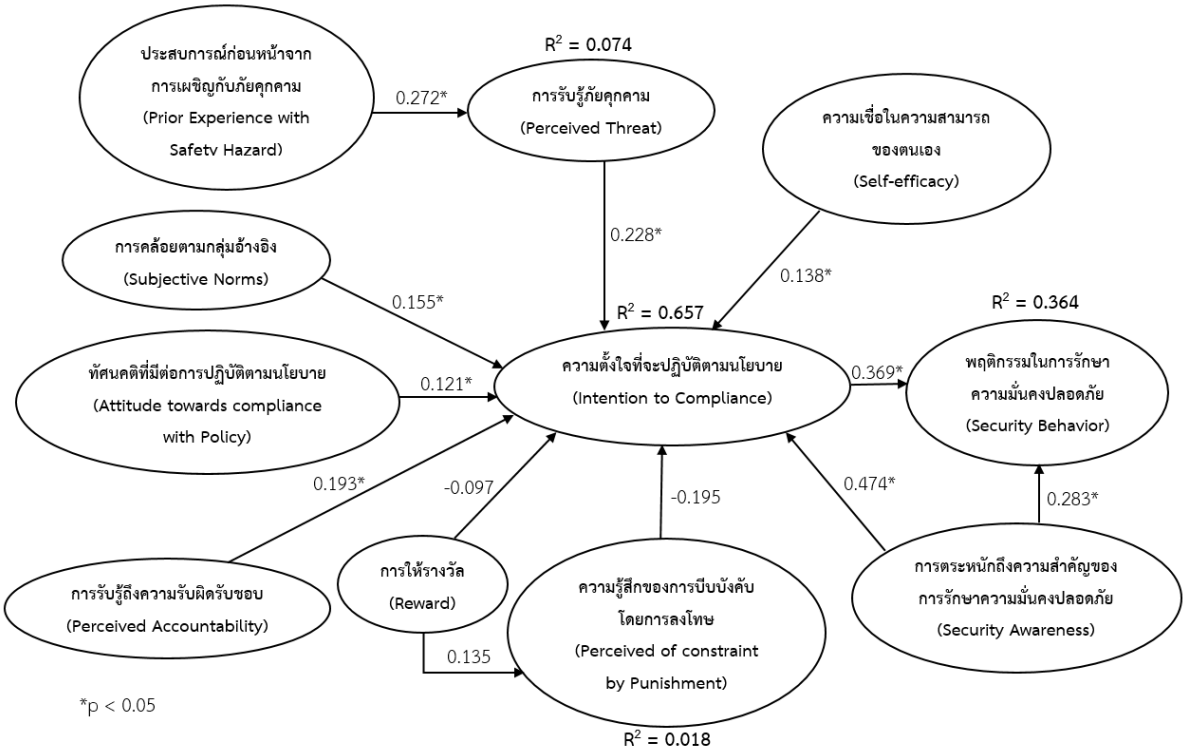
5.4.4.5 การคล้อยตามกลุ่มอ้างอิง ส่งอิทธิพลทางอ้อมผ่านความตั้งใจที่จะปฏิบัติตามนโยบายไปยังพฤติกรรมในการรักษาความมั่นคงปลอดภัย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.057 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

5.4.4.6 ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย ส่งอิทธิพลทางอ้อมผ่านความตั้งใจที่จะปฏิบัติตามนโยบายไปยังพฤติกรรมในการรักษาความมั่นคงปลอดภัย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.045 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

5.4.4.7 การรับรู้ถึงความรับผิดรับชอบ ส่งอิทธิพลทางอ้อมผ่านความตั้งใจที่จะปฏิบัติตามนโยบายไปยังพฤติกรรมในการรักษาความมั่นคงปลอดภัย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.071 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

5.4.4.8 การให้รางวัล ส่งอิทธิพลทางอ้อมผ่านความตั้งใจที่จะปฏิบัติตามนโยบายไปยังพฤติกรรมในการรักษาความมั่นคงปลอดภัย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ -0.036 โดยค่าสัมประสิทธิ์อิทธิพลมีเครื่องหมายลบ

5.4.4.9 ความรู้สึกของการบีบบังคับโดยการลงโทษ ส่งอิทธิพลทางอ้อมผ่านความตั้งใจที่จะปฏิบัติตามนโยบายไปยังพฤติกรรมในการรักษาความมั่นคงปลอดภัย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ -0.072 โดยค่าสัมประสิทธิ์อิทธิพลมีเครื่องหมายลบ



ภาพที่ 2 ผลการวิเคราะห์กรอบแนวคิดการวิจัยเพื่อการแสดงออกถึงพฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศของพนักงานในองค์กร

ตารางที่ 2 ค่าสัมประสิทธิ์อิทธิพลทางตรง ทางอ้อม และอิทธิพลโดยรวมของตัวแปรแฝงในกรอบแนวคิดการวิจัย (แสดงเป็นคะแนนมาตรฐาน)

ตัวแปรตาม	R^2	อิทธิพล	ตัวแปรอิสระ									
			ประสบการณ์ก่อนหน้าจากการเผชิญกับภัยคุกคาม	การรับรู้ภัยคุกคาม	ความเชื่อในความสามารถของตนเอง	การคล้อยตามกลุ่มอ้างอิง	ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย	การรับรู้ถึงความรับผิดชอบ	การให้รางวัล	ความรู้สึกของการบีบบังคับโดยการลงโทษ	การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย	ความตั้งใจที่จะปฏิบัติตามนโยบาย
พฤติกรรมในการรักษาความมั่นคงปลอดภัย	0.364	ทางตรง	-	-	-	-	-	-	-	-	0.283*	0.369*
		ทางอ้อม	-	0.084*	0.051*	0.057*	0.045*	0.071*	-0.036	-0.072	0.175*	-
		โดยรวม	-	0.084*	0.051*	0.057*	0.045*	0.071*	-0.036	-0.072	0.458*	0.369*
ความตั้งใจที่จะปฏิบัติตามนโยบาย	0.657	ทางตรง	-	0.228*	0.138*	0.155*	0.121*	0.193*	-0.097	-0.195	0.474*	-
		ทางอ้อม	0.062*	-	-	-	-	-	-0.026	-	-	-
		โดยรวม	0.062*	0.228*	0.138*	0.155*	0.121*	0.193*	-0.123	-0.195	0.474*	-
การรับรู้ภัยคุกคาม	0.074	ทางตรง	0.272*	-	-	-	-	-	-	-	-	-
		ทางอ้อม	-	-	-	-	-	-	-	-	-	-
		โดยรวม	0.272*	-	-	-	-	-	-	-	-	-
ความรู้สึกของการบีบบังคับโดยการลงโทษ	0.018	ทางตรง	-	-	-	-	-	-	0.135	-	-	-
		ทางอ้อม	-	-	-	-	-	-	-	-	-	-
		โดยรวม	-	-	-	-	-	-	0.135	-	-	-

* $p < 0.05$

6. สรุปผลการวิจัย

6.1 อภิปรายผลการวิจัย

ผลการวิเคราะห์ข้อมูลพบว่า ปัจจัยที่ส่งผลต่อการแสดงออกถึงพฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศของพนักงานในองค์กรมากที่สุด ประกอบด้วย ความตั้งใจที่จะปฏิบัติตามนโยบายการตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย การรับรู้ภัยคุกคาม การรับรู้ถึงความรับผิดรับชอบการคล้อยตามกลุ่มอ้างอิง ความเชื่อในความสามารถของตนเอง ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย ตามลำดับ ซึ่งแสดงให้เห็นว่า กรอบแนวคิดพฤติกรรมในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศมีความสอดคล้องกับข้อมูลเชิงประจักษ์ ดังนี้

(1) ประสบการณ์ก่อนหน้าจากการเผชิญกับภัยคุกคามส่งผลต่อการรับรู้ภัยคุกคาม กล่าวคือ หากพนักงานในองค์กรเคยมีประสบการณ์ก่อนหน้าจากการเผชิญกับภัยคุกคามมาแล้วนั้น จะช่วยให้รับรู้ถึงภัยคุกคามที่อาจจะเกิดขึ้นและหาวิธีป้องกันและรับมือกับภัยคุกคาม เพื่อไม่ให้ส่งผลกระทบร้ายแรงต่อองค์กรได้ ซึ่งเป็นไปตามผลการวิจัยของ Lee at al. (2008)

(2) การรับรู้ภัยคุกคาม ความเชื่อในความสามารถของตนเอง การคล้อยตามกลุ่มอ้างอิง ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย การรับรู้ถึงความรับผิดรับชอบ และการตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยส่งผลต่อความตั้งใจที่จะปฏิบัติตามนโยบาย กล่าวคือ หากองค์กรต้องการให้พนักงานในองค์กรมีความตั้งใจที่จะปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศแล้ว องค์กรต้องส่งเสริมปัจจัยดังกล่าวข้างต้น เพื่อกระตุ้นและเป็นแรงจูงใจให้พนักงานในองค์กรเกิดความตั้งใจที่จะปฏิบัติตามนโยบาย ซึ่งเป็นไปตามผลการวิจัยของ Ifinedo (2012) และ Vance et al. (2015)

(3) ความตั้งใจที่จะปฏิบัติตามนโยบายและการตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยส่งผลต่อพฤติกรรมในการรักษาความมั่นคงปลอดภัย กล่าวคือ หากพนักงานรับรู้และตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นและภัยคุกคามที่เป็นอันตรายจากการใช้เทคโนโลยีสารสนเทศในองค์กร ย่อมส่งผลให้มีแนวโน้มที่จะมีความตั้งใจในการปฏิบัติตามนโยบาย โดยเมื่อพนักงานเกิดความตั้งใจที่จะแสดงออกถึงพฤติกรรมแล้วก็จะแสดงออกพฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศออกมา ซึ่งเป็นไปตามผลการวิจัยของ Bulgurcu et al. (2010) และ Shropshire et al. (2015)

นอกจากนี้ผลการวิเคราะห์ข้อมูลครั้งนี้ พบว่า ความสัมพันธ์ระหว่างปัจจัยการให้รางวัลและความรู้สึกของการบีบบังคับโดยการลงโทษที่ส่งผลต่อความตั้งใจในการปฏิบัติตามนโยบาย และความสัมพันธ์ระหว่างปัจจัยการให้รางวัลที่ส่งผลต่อความรู้สึกของการบีบบังคับโดยการลงโทษ ไม่มีความสอดคล้องกับข้อมูลเชิงประจักษ์ กล่าวคือ ปัจจัยการให้รางวัล ปัจจัยความรู้สึกของการบีบบังคับโดยการลงโทษ และปัจจัยความตั้งใจที่จะปฏิบัติตามนโยบาย มีความสัมพันธ์ในทิศทางตรงกันข้ามกับสมมติฐานการวิจัยที่ตั้งไว้ สาเหตุอาจมาจาก การให้รางวัลอาจเกิดผลกระทบในเชิงลบได้ เมื่อการให้รางวัลถูกตีความว่าเป็นเครื่องมือในการควบคุมพฤติกรรม เช่นเดียวกับความรู้สึกของการบีบบังคับโดยการลงโทษ ที่อาจมีสาเหตุมาจากการลงโทษอย่างรุนแรงอาจทำให้พนักงานรู้สึกต่อต้าน และไม่อยากที่จะปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ ตามผลการวิจัยของ Herath and Rao (2009) จึงส่งผลให้ข้อมูลที่ได้ไม่สนับสนุนสมมติฐานดังกล่าว

6.2 ข้อเสนอแนะในเชิงปฏิบัติ

ผู้ที่เกี่ยวข้องหรือผู้ที่ต้องการสร้างบรรยากาศให้เกิดการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศสามารถนำผลการวิจัยไปใช้เพื่อควบคุมให้พนักงานแสดงออกถึงพฤติกรรมในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศอย่างเหมาะสม ดังนี้

(1) องค์กรต้องจัดให้มีการฝึกอบรมและให้ความรู้เกี่ยวกับภัยคุกคาม วิธีรับมือหรือป้องกันภัยคุกคามที่อาจจะเกิดขึ้นกับระบบสารสนเทศขององค์กร และต้องมีการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศที่ชัดเจน เพื่อสร้างประสบการณ์ การรับรู้ ทัศนคติที่ดีต่อการปฏิบัติตามนโยบายและทำให้พนักงานรู้สึกว่าตนสามารถที่จะรับมือกับภัยคุกคามที่อาจเกิดขึ้นกับระบบสารสนเทศขององค์กรในกรณีต่าง ๆ

(2) องค์กรต้องให้บุคคลที่มีความสำคัญกับพนักงานกระทำให้ดูเป็นแบบอย่าง เพื่อทำให้พนักงานคล้อยตามพฤติกรรมของบุคคลรอบข้าง ได้แก่ เพื่อนร่วมงาน ผู้บังคับบัญชา และผู้ใต้บังคับบัญชา ซึ่งเป็นสิ่งสำคัญที่องค์กรควรนำไปใช้ เมื่อมีการปลูกฝังหรือมีการปฏิบัติตามอย่างทั่วถึงทั้งองค์กร จะทำให้พนักงานรู้สึกถึงความรับผิดชอบในหน้าที่ที่ตนเองควรทำและคล้อยตามการกระทำที่บุคคลรอบข้างแสดงออกมา

(3) องค์กรต้องมีการแจ้งหรือประกาศให้พนักงานรับทราบว่า การกระทำทุกอย่างของพนักงานที่เกี่ยวข้องกับระบบสารสนเทศขององค์กรถือเป็นความรับผิดชอบของพนักงานด้วย ซึ่งอาจมีผลทำให้ระบบสารสนเทศขององค์กรเกิดโอกาสเสี่ยงจากภัยคุกคาม ซึ่งจะทำให้พนักงานมีความระมัดระวังในการใช้งานระบบสารสนเทศเพราะกลัวผลกระทบที่จะเกิดขึ้น

(4) องค์กรต้องสร้างการตระหนักถึงการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศในองค์กร โดยอาจต้องมีการสร้างความเข้าใจ เหตุผลและประโยชน์ที่จะได้รับในการปฏิบัติตามนโยบาย ซึ่งต้องมีการย้ำเตือนพนักงานอยู่เสมอ โดยอาจใช้การเผยแพร่ความรู้ผ่านช่องทางต่าง ๆ ขององค์กร เช่น การติดป้ายประกาศ การแจ้งข้อมูลข่าวสารผ่านอีเมลหรือแจ้งเตือนผ่านคอมพิวเตอร์ เพื่อให้พนักงานเคยชินและหันมาปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยอย่างเป็นประจำ

6.3 ข้อเสนอแนะสำหรับงานวิจัยต่อเนื่อง

เพื่อประโยชน์ในด้านการสร้างองค์ความรู้ใหม่ ทางผู้วิจัยจึงขอเสนอแนะการทำวิจัยครั้งต่อไป ดังต่อไปนี้

(1) การวิจัยครั้งนี้ พบว่า ผู้ตอบแบบสอบถามส่วนใหญ่อยู่ในช่วงอายุ 26-30 ปี ซึ่งความคิดและแรงจูงใจที่ส่งผลต่อการแสดงออกถึงพฤติกรรมในการปฏิบัติตามนโยบายรักษาความมั่นคงปลอดภัยอาจแตกต่างจากองค์กรที่มีพนักงานอาวุโสเป็นจำนวนมาก จึงขอเสนอแนะงานวิจัยต่อเนื่องว่าควรศึกษาเกี่ยวกับปัจจัยที่เสริมสร้างให้พนักงานแสดงออกถึงพฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศในแต่ละกลุ่มช่วงอายุ

(2) การวิจัยครั้งนี้ พบว่า ปัจจัยการให้รางวัลและปัจจัยความรู้สึกของการบีบบังคับโดยการลงโทษที่มีผลต่อความตั้งใจที่จะปฏิบัติตาม ไม่สนับสนุนสมมติฐานการวิจัยในครั้งนี้ เนื่องจากบริบทของกลุ่มตัวอย่างอาจตอบแบบปฏิเสธความเป็นจริงเพื่อหลีกเลี่ยงความเสี่ยงที่อาจเกิดขึ้นกับตนเอง และจากการศึกษางานวิจัยในอดีต ปรากฏว่าให้ข้อสรุปที่แตกต่างกันมีทั้งสนับสนุนและไม่สนับสนุนความสัมพันธ์ดังกล่าว ดังนั้นงานวิจัยต่อเนื่องจึงควรศึกษาปัจจัยการให้รางวัลและปัจจัยความรู้สึกของการบีบบังคับโดยการลงโทษโดยเปรียบเทียบกันระหว่างองค์กรข้ามชาติที่มีพนักงานส่วนใหญ่เป็นชาวต่างชาติและองค์กรที่ส่วนใหญ่เป็นพนักงานคนไทย เพื่อศึกษาว่าวัฒนธรรมของชาติและองค์กรมีส่วนในการกำหนดปัจจัยทั้ง 2 ปัจจัยดังกล่าวหรือไม่

(3) การวิจัยครั้งนี้ พบว่า ปัจจัยการรับรู้ภัยคุกคาม มีความผันแปรของตัวแปรตาม (R^2) ระหว่างประสบการณ์ก่อนหน้าจากการเผชิญกับภัยคุกคามที่ส่งอิทธิพลทางตรงต่อการรับรู้ภัยคุกคามมีค่าค่อนข้างน้อย ซึ่งเท่ากับร้อยละ 7.4 ($R^2 = 0.074$) จึงควรศึกษาว่ามีปัจจัยเพิ่มเติมใดบ้างที่ส่งผลต่อปัจจัยการรับรู้ภัยคุกคาม

(4) การวิจัยครั้งนี้ พบว่า ปัจจัยการตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยส่งอิทธิพลทางตรงต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ที่ค่าสัมประสิทธิ์อิทธิพล เท่ากับ 0.474 และมีความผันแปรของตัวแปรตาม (R^2) เท่ากับร้อยละ 65.7 (R^2 = 0.657) ซึ่งมีค่าค่อนข้างสูง จึงควรศึกษาว่ามีปัจจัยใดบ้างที่ส่งผลต่อการตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

บรรณานุกรม

จตุชัย แพงจันทร์. (2550). *Master in security รวบรวมเนื้อหาด้าน Security ไว้ครบทุกด้านสำหรับ Admin มืออาชีพ* (1). นนทบุรี: อินโฟเพรส.

สำนักงานราชบัณฑิตยสภา. (2532). ความหมายของประสบการณ์. ดึงข้อมูลวันที่ 10 มกราคม 2560, จาก http: / / www. royin. go. th/ ?knowledges= % E0% B8% 9B% E0% B8% A3% E0% B8% B0% E0 %B8%AA%E0%B8%9A%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%93%E0%B9%8C.

สุธีรา เดชนครินทร์ และ สุธินี ฤกษ์ขำ. (2558). *ผลกระทบของมิติทางวัฒนธรรมที่มีต่อระบบการบริหารงานที่มีประสิทธิภาพสูง: การบูรณาการทบทวนวรรณกรรม.* วิทยานิพนธ์ที่ยังไม่ได้ตีพิมพ์, คณะวิทยาการจัดการ, มหาวิทยาลัยสงขลานครินทร์.

สุพิชญา อาชวจิรดา. (2557). *ปัจจัยที่ส่งผลต่อระดับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร.* (วิทยาศาตรมหาบัณฑิต). คณะพาณิชยศาสตร์และการบัญชี, มหาวิทยาลัยธรรมศาสตร์.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211.

Al-Omari, A., Deokar, A., El-Gayar, O., Walters, J., & Aleassa, H. (2013). Information Security Policy Compliance: An Empirical Study of Ethical Ideology. *46th Hawaii International Conference on System Sciences*, Hawaii, 3018-3027.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers and Security, 26*(4), 276-289.

Bandura, A. (1980). Gauging the relationship between self-efficacy judgment and action. *Cognitive Therapy and Research*, *4,* 263-268.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems, 18*(2), 151-164.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

Cavallari, M. (2011). The organizational relationship between compliance and information security. *International Journal of the Academic Business World, 5*(2), 63-76.

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of Information Security at the Workplace: Linking Information Security Climate to Compliant Behavior. *Journal of Information Privacy and Security, 1*(3), 18-41.

Chen, Y., Ramamurthy, K. R., & Wen, K.-W. (2012). Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems, 29*(3), 157-188.

Chen, Y., & Zahedi, F. M. (2016). Indiviuals' Internet security perceptions and behaviors: Polycontextual contrasts between the United States and China. *MIS Quarterly, 40*(1), 205-222.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS Security policy in organizations: An integrated model based on social control and deterrence theory. *Computer and Security, 39*, 447-459.

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems, 20*, 643-658.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research, 20*(1), 79-98.

Dinev, T., & Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies *Journal of the Association for Information System, 8*(7), 386-408.

Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. MA: Addison-Wesley.

Greitemeyer, T., & Weiner, B. (2008). Asymmetrical effects of Reward and punishment on attributions of morality. *The Journal of Social Psychology, 148*(4), 407-420.

Haeussinger, F. J., & Kranz, J. J. (2013). Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior *International Conference on Information Systems 2013*, 1-16.

Hanus, B., & Wu, Y. A. (2016). Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management, 33*(1), 2-16.

Hepler, J. (2015). A good thing isn't always a good thing: dispositional attitudes predict non-normative judgments. *Personality and Individual Differences, 75*(0), 59-63.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*, 106-125.

Hochwarter, W. A., Perrewe, P. L., Hall, A. T., & Ferris, G. R. (2005). Negative affectivity as a moderator of the form and magnitude of the relationship between felt accountability and job tension. *Journal of Organizational Behavior, 26*, 517-534.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences, 43*(4), 615-660.

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

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management, 51*(1), 69-79.

Jouini, M., & Rabai, L. B. A. (2016). Comparative Study of Information Security Risk Assessment Models for Cloud Computing systems. *Procedia Computer Science,* 83, 1084-1089.

Karahanna, E., Straub, D. W., & Chervany, N. L. (1999). Information Technology Adoption Across Time: A Cross-Sectional Comparison of Pre-Adoption and Post-Adoption Beliefs. *MIS Quarterly, 23*(2), 183-213.

Kaur, J., & Mustafa, N. (2013). Examining the Effects of Knowledge, Attitude and Behaviour on Information Security Awareness: A Case on SME. *3rd International Conference on Research and Innovation in Information Systems*, Malaysia, 286-290.

Lee, C., Lee, C. C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computer and Security, 59*, 60-70.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour and Information Technology, 27*(5), 445-454.

Liang, H., & Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems, 11*(7), 394-413.

Merriam-Webster Online Dictionary (2010). Meaning of Behavior. Retrieved September 2, 2016, from https://www.merriam-webster.com/dictionary/behavior.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' Behavior towards IS Security Policy Compliance. *Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS'07)*, Hawaii, 231-254.

Peace, A. G., Galletta, D. F., & Thong, J. Y. L. (2003). Software Piracy in the Workplace: A Model and Empirical Test. *Journal of Management Information Systems, 20*(1), 153-177.

PwC. (2014). 2014 Information Security Breaches Survey. Retrieved October 3, 2016, from http://www.pwc.co.uk/services/audit-assurance/insights/2014-information-security-breaches-survey.html.

PwC. (2015). Information Security Breaches Survey 2015. Retrieved October 3, 2016, from http://www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html.

Safa, N. S., Solms, R. V., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computer and Security, 56*, 20-82.

Schlenker, B. R., Britt, T. W., Pennington, J., Murphy, R., & Doherty, K. (1994). The triangle model of responsibility. *Psychological Review, 101*(4), 632-652.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computer and Security, 49*, 177-191.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2009). Are employees putting your company at risk by not following information security policies? *Communications of the ACM, 52*(12), 145-147.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management and Computer Security, 8*(1), 31-41.

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: an empirical study. *IFIP International Federation for Information Processing, 1,* 33-44.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer, 43*(2), 64-71.

Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information and Management, 48*(7), 296-302.

Stajkovic, A. D., & Luthans, F. (1988). Self-efficacy and work-related performance: A meta-analysis. *Psychological Bulletin, 124*(2), 240-261.

Stanciu, V., & Tinca, A. (2016). Students' awareness on information security between own perception and reality – an empirical study. *Accounting and Management Information Systems,* 15*(1)*, 112-130.

Straub, Jr., D. W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research, 1*(3), 255-276.

Trustwave. (2014). 2014 State of Risk Report. Retrieved October 3, 2016, from https://www.trustwave.com/Resources/Library/Documents/2014-State-of-Risk-Report/.

Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computer and Security, 59*, 138-150.

Vance, A., Lowry, P. B., & Eggett, D. (2015). A new approach to the problem of access policy violations: Increasing perceptions of accountability through the user interface. *MIS Quarterly*, 1-18.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly, 27*(3), 425-478.

Yoon, C., Hwang, J., & Kim, R. (2012). Exploring Factors That Influence Students' Behaviors in Information Security. *Journal of Information Systems Education, 23*(4), 407-415.

Zaharia, A. (2015). 10+ Critical Corporate Cyber Security Risks – A Data Driven List. Retrieved October 3, 2016, from https://heimdalsecurity.com/blog/10-critical-corporate-cyber-security-risks-a-data-driven-list/.