แนวทางในการเสริมสร้างความตระหนักถึงการปฏิบัติตามระเบียบการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรในการใช้อุปกรณ์สมาร์ทโฟนส่วนบุคคล

สลิสา เอียดสุย*
ธนาคารกสิกรไทย จำกัด (มหาชน)
ศากุน บุญอิต
สาขาวิชาบริหารการปฏิบัติการ คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์

***Correspondence:** pickzpickz@gmail.com
doi: 10.14456/jisb.2016.12

บทคัดย่อ

ในปัจจุบันหลายองค์กรได้มีแนวความคิดที่อนุญาตให้พนักงานสามารถนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนบุคคลมาใช้ในการทำงานขององค์กรมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง ในขณะเดียวกันหลายองค์กรต่างตระหนักดีว่าพนักงานเป็นจุดอ่อนที่สำคัญที่ทำให้เกิดการรั่วไหลของสารสนเทศหรือแม้กระทั่งขาดความตระหนักในความเสี่ยงที่เกี่ยวข้องกับการใช้สื่อสังคมออนไลน์ผ่านอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนบุคคล อาจทำให้บุคลากรตกเป็นเหยื่อของการขโมยสารสนเทศ ซึ่งความเสี่ยงเหล่านี้สามารถทำให้เกิดความเสียหายอย่างมีนัยสำคัญต่อชื่อเสียง ความน่าเชื่อถือขององค์กรหรือแม้กระทั่งข้อได้เปรียบทางการแข่งขัน องค์กรจะต้องมุ่งเน้นการรักษาความปลอดภัยข้อมูลโดยสร้างนโยบายการรักษาความปลอดภัยข้อมูลเพื่อเป็นแนวทางสำหรับพนักงานในการปฏิบัติงาน ดังนั้นองค์กรจึงจำเป็นจะต้องทำความเข้าใจถึงปัจจัยที่กระตุ้นให้พนักงานปฏิบัติตามกฎระเบียบการรักษาความปลอดภัยข้อมูลขององค์กร เพื่อสนับสนุนการตระหนักถึงการรักษาความปลอดภัยข้อมูลขององค์กรให้สอดคล้องกับแนวทางการประกอบธุรกิจขององค์กร

การวิจัยนี้ใช้การสำรวจโดยใช้แบบสอบถามเป็นเครื่องมือในการรวบรวมข้อมูล ซึ่งจากกลุ่มตัวอย่างจำนวน 447 ราย จากประชากรไทยที่ทำงานทั้งในองค์กรทั้งภาครัฐและภาคเอกชนและสามารถนำอุปกรณ์สมาร์ทโฟนส่วนบุคคลไปใช้ในที่ทำงานได้ พบว่าทัศนคติที่มีต่อการปฏิบัติตามนโยบายของพนักงาน ความเชื่อเกี่ยวกับกลุ่มอ้างอิงของพนักงาน การรับรู้ความสามารถในการควบคุมพฤติกรรมของพนักงาน ความตระหนักต่อการรักษาความปลอดภัยข้อมูลของพนักงานมีความสัมพันธ์เชิงบวกต่อการปฏิบัติตามระเบียบการรักษาความปลอดภัยข้อมูลขององค์กรในการใช้อุปกรณ์สมาร์ทโฟนส่วนบุคคล

ผลจากการวิจัยนี้ นอกจากจะทำให้ทราบว่าความตระหนักต่อการรักษาความปลอดภัยข้อมูลของพนักงานนำมาซึ่งการปฏิบัติตามระเบียบการรักษาความปลอดภัยข้อมูลขององค์กรในการใช้อุปกรณ์สมาร์ทโฟนส่วนบุคคลแล้ว ยังทำให้เห็นว่าทัศนคติมีบทบาทในการทำหน้าที่เป็นสื่อตัวกลางเพียงบางส่วน (Partial mediator) ในการอธิบายความสัมพันธ์ระหว่างความตระหนักถึงความปลอดภัยข้อมูลและความตั้งใจต่อการปฏิบัติตามระเบียบการรักษาความปลอดภัยข้อมูลขององค์กร

คำสำคัญ: การปฏิบัติตามระเบียบ การรักษาความปลอดภัย อุปกรณ์สมาร์ทโฟน

Information Security Policy Compliance: an Empirical Study of Information Security Awareness on Smartphone Devices

Salisa Adsuy*

Kasikornbank Public Company Limited

Sakun Boon-It

Operations Management Program, Thammasat Business School, Thammasat University

***Correspondence:** pickzpickz@gmail.com

doi: 10.14456/jisb.2016.12

Abstract

An increasingly trend of many organizations nowadays is allowing employees to bring personal mobile devices into organizational workspaces, meanwhile those organizations have realized that, the employees are also a weakest link of information security. The employees often lack the information security awareness, especially when surfing social medias thru their smartphones. Consequencely, the organizational information, including sensitive data or even employee's profiles, can be disclosure by unintention. The cost can be effect to a privacy of individuals, the reliability and reputation of organizations, and eventually lossing of competitive opportunity. Therefore, the organizations would realize factors to encourage their employees to comply with the information security policy rigorously.

This work studies the factors by questionaires in order to collect employee's opinion, and then process the collected data by SPSS program. The poll is collected from 447 Thai participants, who work for various organizations including both government and private sectors. According to the results, we found the factors - attitude towards behaviour, social influence, self-efficacy, and information security awareness - have positive significants to the intention to comply with organizational information security policy, when employees surf social medias thru personal smartphones in organizational workspaces.

By the results, despite the information security awareness positively related to intention to comply with the information security policy, we found that, the employee's attitude is a partial mediator for explaining the relation between the information security awareness and the intention to comply with information security policy.

Keywords: Compliance, Security, Smartphone Devices

1. บทนำ

ในปัจจุบันหลายองค์กรได้มีแนวความคิดที่อนุญาตให้พนักงานสามารถนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนบุคคล เช่น โน๊ตบุ๊ก สมาร์ทโฟน และ แท็บเล็ต มาใช้ในการทำงานขององค์กร มีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง (ประภาดา ตลึงจิตร, 2555) ดังจะเห็นได้จากงานวิจัยของ Cisco IBSG ที่ระบุว่าการเติบโตของแนวคิดการนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนบุคคลมาใช้ในการทำงาน (Bring Your Own Device หรือ BYOD) ของประเทศชั้นนำระดับโลก มีอัตราเติบโตสูงขึ้นร้อยละ 105 ระหว่างปี ค.ศ. 2013-2016 และผลสำรวจจากผู้บริหารระดับสูง CIO (Chief Information Officer) ทั่วโลกต่างระบุตรงกันว่าบุคลากรนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนบุคคลมาใช้ในที่ทำงาน ซึ่งเกี่ยวข้องกับงานทั้งสิ้น คิดเป็น ร้อยละ 28 (ธนาคารแห่งประเทศไทย, 2556) ส่วนในประเทศไทยก็มีองค์กรจำนวนไม่น้อยที่พนักงานนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนตัวมาใช้ในการทำงาน ซึ่งมีทั้งที่ผู้บริหารขององค์กรรับทราบพร้อมทั้งอนุญาตให้นำมาใช้งานอย่างเป็นทางการ และไม่รับทราบต่อการนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนตัวมาใช้ในการทำงาน (ประจิต หาวัตร, 2556; อัครา วัฒนโยธิน, 2553) ผู้บริหารขององค์กรจึงควรทำความเข้าใจถึงแนวคิดการนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนตัวมาใช้ในการทำงาน ทั้งในด้านคุณประโยชน์ และด้านความเสี่ยงต่อการรั่วไหลของข้อมูลสารสนเทศองค์กร (Allam et al., 2014) โดยข้อมูลสารสนเทศเป็นสิ่งสำคัญที่องค์กรจะนำมาใช้ในการบริหารจัดการ พัฒนากระบวนการทำงาน และสร้าง ความได้เปรียบทางการแข่งขันขององค์กร หากบุคลากรสามารถเข้าถึงข้อมูลสารสนเทศขององค์กรได้ทุกที่ทุกเวลาก็จะช่วยเพิ่มประสิทธิภาพในการทำงานให้แก่องค์กรมากยิ่งขึ้น (Allam et al., 2014) ในขณะเดียวกันหลายองค์กรต่างตระหนักดีว่าบุคลากรเป็นจุดอ่อนที่สำคัญที่ทำให้เกิดการรั่วไหลของข้อมูลสารสนเทศ (Haeussinger and Kranz, 2013; Ifinedo, 2012; Toshihiko Takemura, 2013) หรือแม้กระทั่งขาดความตระหนักในความเสี่ยงที่เกี่ยวข้องกับการใช้สื่อสังคมออนไลน์ผ่านอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนบุคคล (Fagnot and Paquette, 2012) ได้ในหลายกรณี เช่น อุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนบุคคลสูญหาย (ประภาดา ตลึงจิตร, 2555) หรือบุคลากรขาดความตระหนักในการดูแลอุปกรณ์หรือติดตั้งซอฟแวร์ที่สำคัญ (Ifinedo, 2012) อาจทำให้บุคลากรตกเป็นเหยื่อของการขโมยข้อมูลสารสนเทศหรืออาจจะเผยแพร่ข้อมูลสารสนเทศขององค์กรโดยตั้งใจหรือไม่ได้ตั้งใจ (อัครา วัฒนโยธิน, 2553) หากอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนตัวไม่มีการป้องกันไว้อย่างดีก็อาจเป็นช่องโหว่ที่ทำให้ระบบเครือข่ายหรือข้อมูลสารสนเทศขององค์กรโดนโจมตีได้ง่ายยิ่งขึ้น (Bertot et al., 2012; อัครา วัฒนโยธิน, 2553) หรือบุคลากรละเมิดกฎระเบียบและข้อบังคับขององค์กรเกี่ยวกับการรักษาความปลอดภัยข้อมูล (Information Security Policy หรือ ISP) (BRohme, 2013; Cheng et al., 2013; Lebek et al., 2013) เป็นต้น ซึ่งความเสี่ยงเหล่านี้จะสามารถทำให้เกิดความเสียหายอย่างมีนัยสำคัญต่อชื่อเสียงขององค์กร ความน่าเชื่อถือขององค์กร ความเสียหายที่เป็นตัวเงิน หรือแม้กระทั่งข้อได้เปรียบทางการแข่งขัน (Webb et al., 2014)

องค์กรจึงพยายามที่จะลดความเสี่ยงที่เกี่ยวข้องกับการรักษาความปลอดภัยข้อมูล (Lebek et al., 2013) หลายองค์กรมักจะพึ่งพาเทคโนโลยีเข้ามาช่วยบรรเทาความเสี่ยง มีการลงทุนกับ Firewall , VPN , Anti-Virus Solution และอื่นๆ อีกเป็นจำนวนเงินมหาศาล (อัครา วัฒนโยธิน, 2553) ถึงแม้ว่าการแก้ไขปัญหาเหล่านั้นจะช่วยปรับปรุงการรักษาความปลอดภัยข้อมูลขององค์กร แต่ผลลัพธ์ที่ได้ไม่เป็นไปตามที่คิดไว้ ซึ่งปัญหาส่วนใหญ่มาจากการขาดความร่วมมือของพนักงานที่อาจจะไม่เข้าใจในเรื่องของการรักษาความปลอดภัยข้อมูลที่ดี (ประภาดา ตลึงจิตร, 2555; อัครา วัฒนโยธิน, 2553) องค์กรจะต้องมุ่งเน้นการรักษาความปลอดภัยข้อมูลโดยสร้างนโยบายการรักษาความปลอดภัยข้อมูลเพื่อเป็นแนวทางสำหรับพนักงานในการปฏิบัติงาน (Al-Omari et al., 2013) อย่างไรก็ตามในขณะที่การสร้างนโยบายการรักษาความปลอดภัยข้อมูลและแนวทางสำหรับการปฏิบัติงานที่จำเป็น อาจจะยังไม่เพียงพอที่จะทำให้แน่ใจว่าพนักงานขององค์กรจะปฏิบัติตามนโยบายหรือปฏิบัติตามกฎระเบียบ (Gritzalis et al., 2014)

ดังนั้นองค์กรจึงจำเป็นจะต้องทำความเข้าใจถึงปัจจัยที่กระตุ้นให้พนักงานปฏิบัติตามกฎระเบียบการรักษาความปลอดภัยข้อมูลขององค์กร (Bulgurcu et al., 2010) เพื่อสนับสนุนการตระหนักถึงการรักษาความปลอดภัยข้อมูลขององค์กร (Information security awareness หรือ ISA) ให้สอดคล้องกับแนวทางการประกอบธุรกิจขององค์กรและอ้างอิงตามนโยบายการรักษาความปลอดภัยขององค์กร (Anderson and Agarwal, 2010; Mani et al., 2014) ถึงแม้ว่าบทบาทความสำคัญของการตระหนักถึงการรักษาความปลอดภัยข้อมูล(Information security awareness) จะได้รับการยอมรับอย่างแพร่หลายแต่ความเข้าใจต่อปัจจัยที่มีอิทธิพลต่อการตระหนักถึงการรักษาความปลอดภัยข้อมูล (Information security awareness) ยังขาดแคลน (Bulgurcu et al., 2010)

การวิจัยฉบับนี้จัดทำขึ้นเพื่อศึกษาปัจจัยเกี่ยวกับ นโยบายการรักษาความปลอดภัยข้อมูล (Information Security Policy) องค์ความรู้ (Knowledge) จะอ้างถึงสิ่งที่พนักงานรู้ ทัศนคติ (Attitude) จะมุ่งเน้นในสิ่งที่พนักงานคิด และพฤติกรรม (Behavior) จะเกี่ยวกับสิ่งที่พนักงานทำ โดยยึดทฤษฎีพฤติกรรมตามแบบแผน (Theory of Planned Behavior) เป็นพื้นฐาน และเพื่อศึกษาความสัมพันธ์ระหว่างการตระหนักถึงการรักษาความปลอดภัยข้อมูลส่วนบุคคล (Information security awareness's antecedents) และความตั้งใจที่จะปฏิบัติตามกฎระเบียบและข้อบังคับขององค์กร (Intention to Comply with the security policies) เพื่อเป็นแนวทางในการเสริมสร้างนโยบายการรักษาความปลอดภัยข้อมูลสำหรับองค์กรและให้พนักงานเกิดการตระหนักในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรและนำไปสู่ความตั้งใจที่จะปฏิบัติตาม

2. ทบทวนวรรณกรรม

จากการศึกษางานวิจัยในอดีตที่เกี่ยวข้อง เนื่องจากนโยบาย กฎระเบียบและข้อบังคับขององค์กรเป็นสิ่งที่กำหนดขึ้นมาเพื่อเป็นแนวทางสำหรับการแสดงพฤติกรรมของพนักงานขององค์กร ดังนั้นวิธีการนำนโยบายมาบังคับใช้จะมีความสำคัญอย่างมากต่อการยอมรับนโยบายนั้นในองค์กร เพื่อให้เข้าใจพฤติกรรมของมนุษย์และวิธีการสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรและนำไปสู่ความตั้งใจที่จะปฏิบัติตาม จึงได้ศึกษาทฤษฎีเชิงพฤติกรรม (Behavior Research)

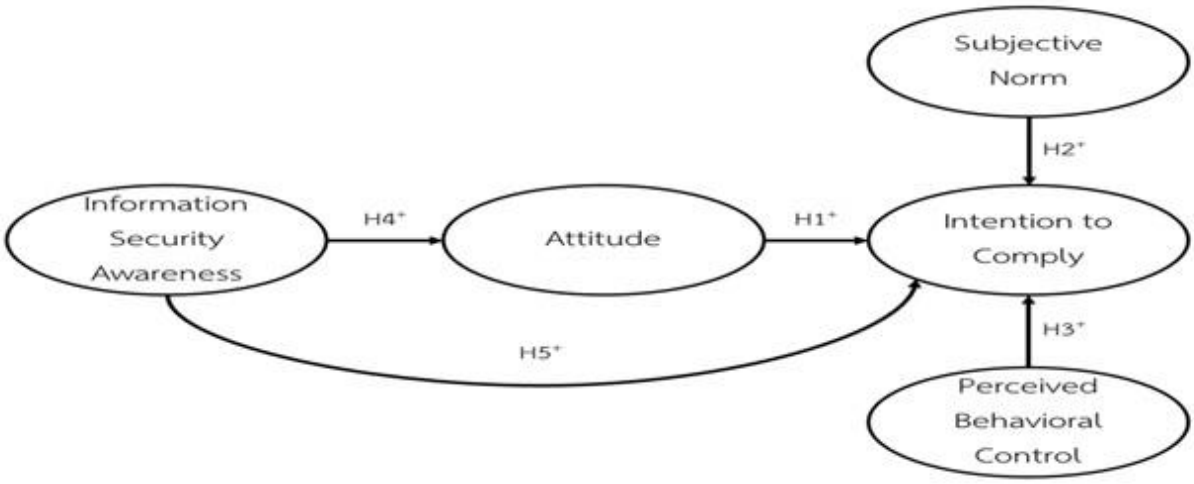
ทฤษฎีพฤติกรรมตามแผน (Theory of Planned Behavior หรือ TPB) นำเสนอโดย (Ajzen, 1991) จัดอยู่ในกลุ่มของทฤษฎีเชิงพฤติกรรม (Bulgurcu et al., 2010; Lebek et al., 2013) พัฒนามาจากทฤษฎีการกระทำตามหลักเหตุและผล (The Theory of Reasoned Action หรือ TRA) นำเสนอโดย (Ajzen and Fishbein, 1980) ซึ่งทฤษฎีดังกล่าวถูกนำมาใช้เป็นพื้นฐานสำหรับการศึกษาพฤติกรรมของมนุษย์มากที่สุด (Lebek et al., 2013; Toshihiko Takemura, 2013; สิงหะ ฉวีสุข และสุนันทา วงศ์จตุรภัทร, 2555)

หลักการของทฤษฎีพฤติกรรมตามแผนเป็นการรับรู้ของแต่ละบุคคลเพื่อที่จะแสดงพฤติกรรมที่ได้รับแรงขับเคลื่อนจากความตั้งใจ (Bulgurcu et al., 2010; Lebek et al., 2013) เพื่อแสดงพฤติกรรมใดๆของบุคคลสามารถคาดการณ์ได้จากทัศนคติต่อพฤติกรรม (Attitude toward behavior) ความเชื่อเกี่ยวกับกลุ่มอ้างอิง (Subjective Norm) และการรับรู้ความสามารถในการควบคุมพฤติกรรม (Perceived Behavioral Control) (Lebek et al., 2013; ประภาดา ตลึงจิตร, 2555; สิงหะ ฉวีสุข และสุนันทา วงศ์จตุรภัทร, 2555) พบว่าความตั้งใจจะได้รับอิทธิพลจากทัศนคติที่มีต่อพฤติกรรม (Attitude toward behavior) ความเชื่อเกี่ยวกับกลุ่มอ้างอิง (Subjective Norm) และการรับรู้ความสามารถในการควบคุมพฤติกรรม (Perceived Behavioral Control) และความตั้งใจมีอิทธิพลโดยตรงกับพฤติกรรม

จากทฤษฎีพฤติกรรมตามแผน แนวทางในการเสริมสร้างความตระหนักถึงการปฏิบัติตามระเบียบการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรในการใช้อุปกรณ์สมาร์ทโฟนส่วนบุคคล จะเกิดขึ้นได้ ปัจจัยแรกคือ พนักงาน

จะต้องมีความเชื่อว่าความตระหนักถึงกฎระเบียบและข้อบังคับขององค์กรเกี่ยวกับการรักษาความปลอดภัยข้อมูล (Information Security Policy) จะก่อให้เกิดประโยชน์ต่อตนเองและองค์กร เมื่อพนักงานมีทัศนคติที่ดีต่อกฎระเบียบและข้อบังคับขององค์กรแล้ว พนักงานก็จะมีความตั้งใจที่จะปฏิบัติตามกฎระเบียบ ปัจจัยที่สองคือ พนักงานเห็นว่าเพื่อนร่วมงานได้กระทำตามกฎระเบียบและข้อบังคับขององค์กรเกี่ยวกับการรักษาความปลอดภัยข้อมูล พนักงานก็จะแนวโน้มที่จะแสดงพฤติกรรมเหล่านั้นด้วย ปัจจัยที่สามคือ พนักงานสามารถรับรู้ความสามารถในการควบคุมพฤติกรรมถึงการปฏิบัติตามกฎระเบียบและข้อบังคับขององค์กร รวมถึงผลให้เป็นไปตามที่ต้องการ พนักงานก็จะมีความตั้งใจที่จะปฏิบัติตามกฎระเบียบและข้อบังคับขององค์กร

การทบทวนแนวคิดและทฤษฎีที่เกี่ยวข้องทำให้สามารถนำมาพัฒนากรอบแนวคิดของปัจจัยทางด้านความตระหนักถึงการปฏิบัติตามระเบียบการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรในการใช้อุปกรณ์สมาร์ทโฟนส่วนบุคคล ซึ่งเป็นการบูรณาการกรอบแนวคิดมาจากงานวิจัยในอดีต ประกอบด้วย ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย ความเชื่อเกี่ยวกับกลุ่มอ้างอิง การรับรู้ความสามารถในการควบคุมพฤติกรรม ความตั้งใจที่จะปฏิบัติตาม และความตระหนักถึงความปลอดภัยข้อมูล



ภาพที่ 1 กรอบแนวคิดของงานวิจัย (Conceptual model)

3. วิธีการวิจัย

งานวิจัยชิ้นนี้เป็นงานวิจัยเชิงปริมาณ (Quantitative Research) มีจุดมุ่งหมายเพื่อพิสูจน์สมมติฐานงานวิจัยที่กำหนดขึ้น เป็นการศึกษาในลักษณะของการวิจัยเชิงสำรวจ (Survey Research) ด้วยวิธีการทบทวนวรรณกรรมที่เกี่ยวข้อง ซึ่งใช้วิธีการเก็บรวบรวมข้อมูลด้วยแบบสอบถาม (Questionnaire) แบบสอบถามจะพัฒนาเป็นแบบสอบถามอิเล็กทรอนิกส์และแบบสอบถามแบบกระดาษ เพื่อนำมาวิเคราะห์ทางสถิติ

ผู้วิจัยได้ทำออกแบบและทดสอบแบบสอบถาม ซึ่งจะใช้เป็นเครื่องมือในการเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่าง จำนวน 447 ตัวอย่าง จากประชากรไทยที่ทำงานทั้งในองค์กรทั้งภาครัฐและภาคเอกชนและสามารถนำอุปกรณ์สมาร์ทโฟนส่วนบุคคลไปใช้ในที่ทำงานได้ ในเขตกรุงเทพมหานครและปริมณฑล การสร้างและพัฒนาข้อคำถามของงานวิจัยทางผู้วิจัยเป็นการรวบรวมข้อคำถามที่เกี่ยวข้องจากงานวิจัยในอดีต ซึ่งแบบสอบถามที่ใช้ได้จากการปรับประยุกต์จากการศึกษางานวิจัยในอดีตที่เกี่ยวข้อง บทความ เพื่อนำมากำหนดขอบเขตและเนื้อหาของแบบสอบถามที่จะนำไปใช้ศึกษากับกลุ่มตัวอย่างและผู้วิจัยมีการพัฒนาข้อคำถามที่เกี่ยวข้องจากการรวบรวมงานวิจัยในอดีต โดยข้อคำถามทางด้านระเบียบการรักษาความ

มั่นคงปลอดภัยทางด้านสารสนเทศขององค์กร จากงานวิจัยของ (Anderson and Agarwal, 2010; Bulgurcu et al., 2010; Fagnot and Paquette, 2012)

การวิจัยครั้งนี้ผู้วิจัยดำเนินการควบคุมของเครื่องมือที่ใช้ในการวิจัย 2 ส่วน ดังนี้ (1) การตรวจสอบความเที่ยงตรงเชิงเนื้อหา (Content Validity) ให้อาจารย์ที่ปรึกษาผู้ทรงคุณวุฒิ ซึ่งมีความชำนาญในการทำงานวิจัย พิจารณาและตรวจสอบความเที่ยงตรงของเนื้อหา แล้วทำการปรับปรุงแก้ไขตามข้อเสนอแนะ เพื่อความชัดเจนและครบถ้วนตามจุดประสงค์ของงานวิจัย (2) การทดสอบความเชื่อมั่นของชุดคำถามที่ใช้วัดตัวแปร โดยการนำแบบสอบถามที่ได้รับการปรับปรุงแก้ไขแล้วเพื่อทดสอบแบบสอบถามของงานวิจัยกับกลุ่มตัวอย่าง จำนวน 20 คน (Pre-Test) โดยใช้แบบสอบถามแบบกระดาษ เพื่อประเมินถึงความเหมาะสมและความชัดเจนของแบบสอบถามก่อนการเก็บข้อมูลจริง โดยใช้สูตรของ Cornbach เพื่อคำนวณหาค่าสัมประสิทธิ์แอลฟา (Cronbach, 1951) แล้วทำการปรับปรุงแก้ไขแบบสอบถาม หลังจากได้แบบสอบถามที่มีความเหมาะสมเรียบร้อยแล้ว ผู้วิจัยจึงนำแบบสอบถามไปใช้ในการเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่าง โดยใช้แบบสอบถามอิเล็กทรอนิกส์

4. ผลการศึกษา

ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม ผลการวิเคราะห์ในส่วนนี้เป็นการแจกแจงข้อมูลทั่วไปของผู้ตอบแบบสอบถาม จำนวนกลุ่มตัวอย่างที่ใช้ในการวิจัยครั้งนี้มีทั้งหมด 447 คน และเมื่อแยกตามข้อมูลส่วนบุคคลของกลุ่มตัวอย่าง พบว่าช่วงอายุของกลุ่มตัวอย่าง 26-30 ปี สูงถึงร้อยละ 61.74 และระดับการศึกษาของกลุ่มตัวอย่างพบว่า ปริญญาตรี ร้อยละ 70.02 ในขณะที่ทำการจำแนกตามระดับตำแหน่งงานระดับปฏิบัติการ ร้อยละ 82.77 แจกแจงตามกลุ่มสายงานที่เกี่ยวข้องพบว่ากลุ่มสายงาน Financial Services มีมากที่สุดถึงร้อยละ 58.61 สุดท้ายการจำแนกกลุ่มตัวอย่างตามลักษณะการใช้งานอุปกรณ์สมาร์ทโฟนส่วนบุคคลของกลุ่มตัวอย่าง โดยแบ่งตามระดับความรู้เกี่ยวกับคอมพิวเตอร์และเทคโนโลยี ไม่ดีเลย ร้อยละ 0.45 ค่อนข้างไม่ดี ร้อยละ 4.03 ปานกลาง ร้อยละ 46.31 ค่อนข้างดี ร้อยละ 40.27 และ ดีมาก ร้อยละ 8.95

ผลการวิเคราะห์องค์ประกอบร่วม (Factor Analysis) เป็นการนำเสนอผลของการจับกลุ่มปัจจัยที่ส่งผลถึงการปฏิบัติตามระเบียบการรักษาความมั่นคงปลอดภัย ทั้ง 5 ตัวแปร ประกอบด้วย ความตระหนักถึงความปลอดภัยข้อมูล ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย ความเชื่อเกี่ยวกับกลุ่มอ้างอิง การรับรู้ความสามารถในการควบคุมพฤติกรรม และความตั้งใจที่จะปฏิบัติตามนโยบาย ซึ่งวิธีการสกัดปัจจัยจะเลือกเฉพาะปัจจัยที่มีค่า Eigenvalue มากกว่า 1 เท่านั้น เมื่อพิจารณาค่าสถิติพบว่าค่าดัชนี KMO มีค่ามากกว่า 0.80 ทุกตัวแปรแสดงว่า ข้อมูลที่มีอยู่มีความเหมาะสมที่จะใช้ Factor Analysis ในการวิเคราะห์องค์ประกอบร่วมมาก

ความเชื่อมั่นของเครื่องมือ ได้ทำการตรวจสอบความเชื่อมั่น (Reliability) ของเครื่องมือ โดยใช้สูตรสัมประสิทธิ์แอลฟ่า (Alpha Coefficient) ของ Cronbach ซึ่งผลการวิเคราะห์ปรากฏว่าจำนวนกลุ่มตัวอย่างที่เก็บรวบรวม ให้ค่าความเชื่อมั่นของทั้ง 5 ตัวแปร อยู่ในเกณฑ์ที่ยอมรับได้ คือมากกว่า 0.7 ซึ่งแสดงให้เห็นว่ามีความเชื่อมั่นในระดับที่สูงมาก

5. สรุปผลการวิจัย

งานวิจัยนี้มีการศึกษาเอกสารงานวิจัยในอดีตที่เกี่ยวข้อง เพื่อเป็นแนวทางในการสร้างและสรุปกรอบแนวคิดในการวิจัยเพื่อทดสอบสมมติฐานที่ว่าทัศนคติของพนักงานที่มีต่อการปฏิบัติตามนโยบายรักษาความปลอดภัยข้อมูลขององค์กร ความเชื่อเกี่ยวกับกลุ่มอ้างอิงของพนักงานเกี่ยวกับการปฏิบัติตามนโยบายรักษาความปลอดภัยข้อมูลขององค์กร การรับรู้ความสามารถในการควบคุมพฤติกรรมของพนักงานเกี่ยวกับการปฏิบัติตามนโยบายรักษาความปลอดภัยข้อมูลขององค์กร และความตระหนักถึงความปลอดภัยข้อมูลของพนักงานเป็นปัจจัยที่ส่งผลเชิงบวกต่อความตั้งใจที่จะปฏิบัติตาม ข้อกำหนด

ของนโยบายการรักษาความปลอดภัยข้อมูลขององค์กรในการใช้อุปกรณ์สมาร์ทโฟนส่วนบุคคล รวมถึงความตระหนักถึงความปลอดภัยข้อมูลของพนักงานเป็นปัจจัยที่ส่งผลเชิงบวกต่อทัศนคติที่มีต่อการปฏิบัติตามข้อกำหนดของนโยบายการรักษาความปลอดภัยข้อมูลขององค์กรในการใช้อุปกรณ์สมาร์ทโฟนส่วนบุคคล

การวิจัยนี้มีกลุ่มตัวอย่างเป็นพนักงานขององค์กรทั้งภาครัฐและภาคเอกชนในประเทศไทย โดยสามารถนำอุปกรณ์สมาร์ทโฟนส่วนบุคคลไปใช้ในที่ทำงานได้ จำนวน 447 ราย ซึ่งการเลือกกลุ่มตัวอย่างนั้นใช้วิธีการสุ่มแบบเฉพาะเจาะจง และใช้แบบสอบถามเป็นเครื่องมือในการรวบรวมข้อมูล

สถิติที่ใช้ในการวิเคราะห์ข้อมูลสำหรับการวิจัยในครั้งนี้ ได้แก่ สถิติบรรยายเพื่อวิเคราะห์การแจกแจงความถี่ของข้อมูลส่วนตัวของผู้ตอบแบบสอบถาม การวิเคราะห์องค์ประกอบร่วม (Factor analysis) เพื่อจับกลุ่มปัจจัย และการวิเคราะห์ Regression เพื่อหาความสัมพันธ์ระหว่างกลุ่มปัจจัยทัศนคติของพนักงานที่มีต่อการปฏิบัติตามนโยบายรักษาความปลอดภัยข้อมูลขององค์กร ความเชื่อเกี่ยวกับกลุ่มอ้างอิงของพนักงาน การรับรู้ความสามารถในการควบคุมพฤติกรรมของพนักงานและความตระหนักถึงความปลอดภัยข้อมูลของพนักงานกับความตั้งใจที่จะปฏิบัติตามข้อกำหนดของนโยบายการรักษาความปลอดภัยข้อมูลขององค์กร สรุปผลการทดสอบสมมติฐานแสดงในตารางที่ 1

ตารางที่ 1 สรุปผลการทดสอบสมมติฐาน

สมมติฐาน	**ความสัมพันธ์**			**ผลทดสอบการสนับสนุนสมมติฐานที่ระดับนัยสำคัญ(P<0.01)**
H1	ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย	→	ความตั้งใจที่จะปฏิบัติตามนโยบาย	สนับสนุน
H2	ความเชื่อเกี่ยวกับกลุ่มอ้างอิง	→	ความตั้งใจที่จะปฏิบัติตามนโยบาย	สนับสนุน
H3	การรับรู้ความสามารถในการควบคุมพฤติกรรม	→	ความตั้งใจที่จะปฏิบัติตามนโยบาย	สนับสนุน
H4	ความตระหนักถึงความปลอดภัยข้อมูล	→	ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย	สนับสนุน
H5	ความตระหนักถึงความปลอดภัยข้อมูล	→	ความตั้งใจที่จะปฏิบัติตามนโยบาย	สนับสนุน

5.1 ประโยชน์ที่จะได้รับ

เชิงทฤษฎี งานวิจัยฉบับนี้สามารถทำให้ทราบถึงองค์ความรู้ที่สำคัญ ซึ่งเกี่ยวข้องกับปัญหาเชิงพฤติกรรมของพนักงานต่อการปฏิบัติตามระเบียบการรักษาความปลอดภัยข้อมูลขององค์กรและปัจจัยของการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กร จากการทบทวนวรรณกรรมที่เกี่ยวข้องและตรวจสอบบทบาทของปัจจัยอิทธิพลจากทัศนคติที่มีต่อพฤติกรรม (Attitude toward behavior) ในการทำหน้าที่เป็นสื่อตัวกลางที่สำคัญ (มีการใช้กันอย่างกว้างขวางจากหลายทฤษฎี เช่น TAM) (Bulgurcu et al., 2010; Kaur and Mustafa, 2013) จากผลการวิจัยครั้งนี้ได้ทำการตรวจสอบในบริบทของทัศนคติของพนักงานที่มีต่อความตั้งใจในการปฏิบัติตามนโยบายองค์กร งานวิจัยฉบับนี้ได้ชี้แนวทางให้เห็นว่าทัศนคติมีบทบาทในการทำหน้าที่เป็นสื่อตัวกลางเพียงบางส่วน (Partial mediator) ในการอธิบายความสัมพันธ์ระหว่างความตระหนัก

ถึงความปลอดภัยข้อมูล (Information Security Awareness) และความตั้งใจต่อการปฏิบัติตามระเบียบการรักษาความปลอดภัยข้อมูลขององค์กร (Intention to Comply) นอกจากนี้งานวิจัยยังสามารถแสดงให้เห็นว่าปัจจัยความตระหนักต่อการรักษาความปลอดภัยข้อมูลของพนักงานมีอิทธิพลทางตรงต่อปัจจัยการปฏิบัติตามระเบียบการรักษาความปลอดภัยข้อมูลขององค์กรในการใช้อุปกรณ์สมาร์ทโฟนส่วนบุคคล ดังนั้นวิจัยฉบับนี้ได้ชี้แนวทางให้เห็นว่าความตระหนักถึงความปลอดภัยข้อมูล (Information Security Awareness) มีอิทธิพลทั้งทางตรงต่อการปฏิบัติตามระเบียบการรักษาความปลอดภัยข้อมูลขององค์กรได้และทางอ้อมโดยผ่านปัจจัยทัศนคติที่มีต่อการปฏิบัติตามนโยบายของพนักงานกับพฤติกรรมของพนักงานต่อการปฏิบัติตามระเบียบการรักษาความปลอดภัยข้อมูลขององค์กรได้

เชิงปฏิบัติ งานวิจัยฉบับนี้สามารถนำไปกำหนดแนวทางเพื่อส่งเสริมความตระหนักของพนักงานต่อการปฏิบัติตามระเบียบการรักษาความปลอดภัยทางด้านสารสนเทศขององค์กรในการใช้อุปกรณ์สมาร์ทโฟนส่วนบุคคล องค์กรต่างๆ สามารถใช้มาตรการตอบโต้ทั้ง 3 รูปแบบเพื่อที่จะสามารถลดการกระทำผิดของพนักงานต่อการปฏิบัติตามระเบียบการรักษาความปลอดภัยทางด้านสารสนเทศขององค์กร ซึ่งมาตรการตอบโต้ ทั้งสามรูปแบบได้แก่ ความตระหนักต่อนโยบายความปลอดภัยของผู้ใช้งาน การศึกษาและฝึกอบรมเกี่ยวกับทางด้านความมั่นคงปลอดภัย และการตรวจสอบคอมพิวเตอร์และอุปกรณ์สมาร์ทโฟนส่วนบุคคล โดยองค์กรสามารถนำไปประยุกต์ใช้ในทางปฏิบัติได้ ดังนี้ ผู้บริหารขององค์กร หรือผู้บริหารสารสนเทศระดับสูงควรให้ความสำคัญในการบริหารจัดการ โดยผู้บริหารจะต้องแสดงถึงการให้ความสำคัญต่อการกำหนดการลงมือปฏิบัติการ ดำเนินการ เฝ้าระวัง การทบทวน การบำรุงรักษาและการปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย ผู้บริหารควรมอบหมายให้หน่วยงานภายในองค์กรที่เกี่ยวข้อง เช่น ฝ่ายสารสนเทศ ฝ่ายทรัพยากรบุคคลในการบริหารจัดการทรัพยากรที่จำเป็น เช่น การอบรม การประชาสัมพันธ์เผยแพร่ข้อมูลข่าวสาร การสร้างความรู้ความเข้าใจเกี่ยวกับการควบคุมภายในและนโยบายความมั่นคงปลอดภัยข้อมูลองค์กร การสร้างความตระหนักถึงความปลอดภัยข้อมูลและการเพิ่มขีดความสามารถเพื่อให้พนักงานทั้งหมดที่ได้รับมอบหมายหน้าที่สามารถปฏิบัติงานได้ตามที่กำหนดไว้ในนโยบายความมั่นคงปลอดภัย เพื่อสร้างความมั่นใจว่าพนักงานทุกคนในองค์กรมีความตระหนักในบทบาทของพวกเขาและความรับผิดชอบที่มีต่อการรักษาความปลอดภัยข้อมูลขององค์กร นอกจากนี้ผู้บริหารควรให้ความสำคัญในการลงทุนด้านความมั่นคงปลอดภัยข้อมูลองค์กรซึ่งต้องพัฒนาความความรู้ด้านความปลอดภัยทางเทคโนโลยีอย่างต่อเนื่องและเปิดโอกาสให้พนักงานได้เข้าอบรม ศึกษาดูงานเพื่อเพิ่มพูนความรู้ตามความเหมาะสม ดังนั้นงานวิจัยชิ้นนี้สามารถกระตุ้นให้องค์กรเห็นความสำคัญของการเสริมสร้างความตระหนักถึงการปฏิบัติตามระเบียบการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรในการใช้อุปกรณ์สมาร์ทโฟนส่วนบุคคลของพนักงาน เพื่อเป็นแนวทางในการเสริมสร้างนโยบายการรักษาความปลอดภัยข้อมูลสำหรับองค์กรและให้พนักงานเกิดการตระหนักในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรและนำไปสู่ความตั้งใจที่จะปฏิบัติตาม

5.2 ข้อจำกัดในงานวิจัย

แม้ว่างานวิจัยฉบับนี้จะมีการค้นพบที่เป็นประโยชน์และน่าสนใจ แต่ก็ยังมีข้อจำกัดบางประการ ได้แก่ งานวิจัยในครั้งนี้เลือกกลุ่มตัวอย่างทั้งหมดจากองค์กรทั้งภาครัฐและภาคเอกชนโดยสามารถนำอุปกรณ์สมาร์ทโฟนส่วนบุคคลไปใช้ในที่ทำงาน วิธีการเลือกกลุ่มประชากรที่ใช้เป็นกลุ่มตัวอย่างแบบเจาะจง (Purposive Sampling) ถึงแม้ว่ากลุ่มตัวอย่างจำนวน 447 รายจะสามารถเป็นตัวแทนของประชากรทั้งหมด แต่วิธีการเลือกกลุ่มตัวอย่างแบบเจาะจงเป็นการเลือกกลุ่มตัวอย่างโดยใช้ดุลพินิจและการตัดสินใจของผู้วิจัยหลักในการพิจารณาเลือกกลุ่มตัวอย่างว่ามีลักษณะสอดคล้องหรือเป็นตัวแทนที่จะศึกษาได้หรือเป็นไปตามวัตถุประสงค์ของการงานวิจัยหรือไม่ ซึ่งการตัดสินใจของผู้วิจัยอาจจะส่งผลต่อความน่าเชื่อถือของผลที่ได้จากการวิจัย จาการคัดเลือกกลุ่มตัวอย่างผู้วิจัยได้คัดเลือกเฉพาะกลุ่มตัวอย่างที่ทำงานเป็นพนักงานประจำ

(Permanent Employee) เท่านั้น อาจจะทำให้เกิดอคติหรือขาดข้อมูลในการตอบแบบสอบถามในส่วนของพนักงานชั่วคราว (Temporary Employee)

5.3 ข้อเสนอแนะ

สืบเนื่องจากข้อจำกัดที่ได้กล่าวข้างต้น เพื่อให้งานวิจัยในอนาคต มีความสมบูรณ์และน่าสนใจยิ่งขึ้น จึงใคร่ขอเสนอข้อเสนอแนะสำหรับการทำงานวิจัยครั้งต่อไป ใน 2 ประเด็น ดังนี้ ประเด็นที่แรก งานวิจัยในครั้งนี้มุ่งศึกษาปัจจัยที่จะนำไปสู่การปฏิบัติตามระเบียบการรักษาความปลอดภัยข้อมูลขององค์กร โดยเลือกปัจจัยจากกลุ่มของทฤษฎีเชิงพฤติกรรม (Behavioral Theories) เป็นหลัก งานวิจัยครั้งต่อไปควรมีการศึกษาปัจจัยทางด้านแรงจูงใจเพื่อศึกษาปัจจัยใดบ้างที่ช่วยเสริมสร้างแรงจูงใจในการปฏิบัติตามระเบียบการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กร เช่น การให้รางวัลหากพนักงานปฏิบัติตามระเบียบการรักษาความปลอดภัยข้อมูลขององค์กร หรือ การลงโทษหากพนักงานไม่ตามระเบียบการรักษาความปลอดภัยข้อมูลขององค์กร ประเด็นที่สอง เนื่องจากงานวิจัยชิ้นนี้ได้ระบุขอบเขตการวิจัยเฉพาะพนักงานประจำเนื่องจากพนักงานประจำได้ผ่านกระบวนการอบรมหรือได้รับความรู้ถึงกฎระเบียบการรักษาความปลอดภัยข้อมูลขององค์กรเป็นอย่างดี และมีสิทธิ์หรือสามารถเข้าถึงข้อมูลขององค์กรได้ แต่อย่างไรก็ตามบางองค์กรให้สิทธิ์พนักงานชั่วคราวสามารถเข้าถึงข้อมูลขององค์กรได้เช่นกันและหลายองค์กรไม่ได้ให้ความสำคัญหรือเน้นย้ำต่อการปฏิบัติตามระเบียบการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรสำหรับพนักงานชั่วคราว เนื่องจากมองว่าพนักงานเหล่านั้นใช้เวลาทำงานตามสัญญาจ้าง ซึ่งจากจุดนี้อาจจะทำให้เกิดช่องโหว่หรือเกิดความเสี่ยงที่จะทำให้ข้อมูลขององค์กรรั่วไหล ดังนั้นสำหรับงานวิจัยในอนาคต อาจจะทำการศึกษาเกี่ยวกับปัจจัยที่เสริมสร้างความตระหนักให้พนักงานชั่วคราวในการปฏิบัติตามระเบียบการรักษาความปลอดภัยข้อมูลขององค์กรทั้งในขณะที่ปฏิบัติงานในองค์กรและหมดสัญญาจ้าง

บรรณานุกรม

ธนาคารแห่งประเทศไทย. (2556). BYOD@BOT เปิดโลกการทำงานยุคใหม่แบบไร้ขีดจำกัด.

ประจิต หาวัตร. (2556). กลยุทธ์การจัดการความเสี่ยงจากการใช้ BYOD. บทความวิชาการ, 25, 91-95.

ประภาดา ตลึงจิตร. (2555). แนวทางในการเสริมสร้างความตระหนักถึงการปฏิบัติตามระเบียบการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ไทย: case study research of Thai cooperative. [กรุงเทพฯ]: คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์.

สิงหะ ฉวีสุข และสุนันทา วงศ์จตุรภัทร. (2555). ทฤษฎีการยอมรับการใช้เทคโนโลยีสารสนเทศ. KMITL Information Technology, jan-jun.2012.

อัครา วัฒนโยธิน. (2553). ความตระหนักของพนักงานต่อการป้องกันรักษาทรัพย์สินทางด้านสารสนเทศ: กรณีศึกษา : การไฟฟ้าส่วนภูมิภาค สำนักงานกลาง. [กรุงเทพฯ]: วิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์.

Ajzen, I. (1991). The theory of planned behavior. Organizational behavior and human decision processes, 50(2), 179-211.

Ajzen, I., and Fishbein, M. (1980). Understanding attitudes and predicting social. Behaviour. Englewood Cliffs, NJ: Prentice-Hall.

Al-Omari, A., Deokar, A., El-Gayar, O., Walters, J., and Aleassa, H. (2013). Information Security Policy Compliance: An Empirical Study of Ethical Ideology. Paper presented at the System Sciences (HICSS), 2013 46th Hawaii International Conference on.

Allam, S., Flowerday, S. V., and Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. Computers & Security, 42(0), 56-65.

Anderson, C. L., and Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. MIS quarterly, 34(3), 613-643.

Bertot, J. C., Jaeger, P. T., and Hansen, D. (2012). The impact of polices on government social media usage: Issues, challenges, and recommendations. Government Information Quarterly, 29(1), 30-40.

BRohme, R. (2013). The Economics of Information Security and Privacy. Book. doi: 10.1007/978-3-642-39498-0.

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.

Cheng, L., Li, Y., Li, W., Holm, E., and Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. Computers & Security, 39, Part B(0), 447-459.

Fagnot, I., and Paquette, S. (2012). Organizational Information Security: The Impact of Employee Attitudes and Social Media Use.

Gritzalis, D., Kandias, M., Stavrou, V., and Mitrou, L. (2014). History of Information: The case of Privacy and Security in Social Media. Paper presented at the Proc. of the History of Information Conference.

Haeussinger, F., and Kranz, J. (2013). Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior.

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

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., and Hohler, B. (2013). Employees' Information Security Awareness and Behavior: A Literature Review. Paper presented at the System Sciences (HICSS), 2013 46th Hawaii International Conference on.

Mani, D., Mubarak, S., and Choo, K.-K. R. (2014). Understanding the Information Security Awareness Process in Real Estate Organizations Using the Seci Model. Paper presented at the 20th Americas Conference on Information Systems (AMCIS 2014).

Toshihiko Takemura, A. K. (2013). An Empirical Study on Information Security Behaviors and Awareness. Book, 95-114.

Webb, J., Ahmad, A., Maynard, S. B., and Shanks, G. (2014). A situation awareness model for information security risk management. Computers & Security, 44(0), 1-15.