ปัจจัยที่ส่งผลต่อระดับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร

สุพิชญา อาชวิรดา*

สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ

***Correspondence:** supichaya_a@hotmail.com doi: 10.14456/jisb.2016.11

บทคัดย่อ

ปัจจุบันสารสนเทศเข้ามามีบทบาทต่อการดำเนินธุรกิจเป็นอย่างมาก แต่ความเสี่ยงทางธุรกิจที่พบมากเป็นอันดับต้นๆ คือการรับเอาเทคโนโลยีมาใช้โดยไม่ได้คำนึงถึงการรักษาความมั่นคงปลอดภัยในระดับที่เพียงพอควบคู่กันไปด้วย ดังนั้น การรักษาความมั่นคงปลอดภัยต่อการใช้ระบบสารสนเทศในองค์กรถือเป็นเรื่องสำคัญ องค์กรจำเป็นต้องทบทวนบทบาทและเพิ่มระดับการรักษาความมั่นคงปลอดภัย ให้มากขึ้น นอกจากนี้ ผู้บริหารระดับสูงยังจะต้องเร่งสร้าง การตระหนัก ในเรื่องการรักษาความมั่นคงปลอดภัยของข้อมูลบนระบบสารสนเทศให้เกิดแก่พนักงาน ลูกจ้างและ ผู้ถือหุ้น อื่นๆ รวมทั้งปลูกฝังจริยธรรมในการเผยแพร่ข้อมูลซึ่งถือเป็น สินทรัพย์ ที่สำคัญของบริษัทออกไปภายนอก เนื่องจากการทำให้พนักงานในองค์กรตระหนักถึงการใช้ระบบสารสนเทศในองค์กรจะมีส่วนช่วยให้องค์กรมีระดับการรักษาความมั่นคงปลอดภัยที่สูงขึ้น ผู้วิจัยจึงทำการศึกษาว่ามีปัจจัยใดบ้างที่ส่งผลต่อระดับการรักษาความมั่นคงปลอดภัยในการใช้ระบบสารสนเทศ โดยงานวิจัยนี้เป็นการวิจัยเชิงปริมาณประเภทการวิจัยเชิงสำรวจ โดยรวบรวมข้อมูลจากพนักงานในองค์กรที่มีรายชื่อจดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทยจำนวน 240 ชุดและนำข้อมูลที่ได้มาวิเคราะห์สมการถดถอยโดยใช้โปรแกรมสำเร็จรูปทางสถิติ เพื่อศึกษาปัจจัยที่มีผลต่อการตระหนักถึงความปลอดภัยต่อการใช้ระบบสารสนเทศในองค์กร ซึ่งผลของงานวิจัยนี้แสดงให้เห็นว่า การรับรู้ถึงภัยคุกคาม การฝึกอบรมและให้ความรู้ ความรู้ความเข้าใจในระบบสารสนเทศล้วนส่งผลต่อการตระหนักถึงความปลอดภัย และเมื่อพนักงานเกิดความตระหนักแล้วยังส่งผลต่อพฤติกรรมการใช้ระบบสารสนเทศในองค์กรทำให้เกิดความตระหนักในการใช้งานมากขึ้น สุดท้ายก่อให้เกิดระดับการรักษาความมั่นคงปลอดภัยที่สูงขึ้นนั่นเอง ประโยชน์ที่ได้จากการวิจัยนี้ทำให้ทราบถึงระดับการรักษาความมั่นคงปลอดภัยของสารสนเทศในองค์กร อีกทั้งจะช่วยให้ผู้ใช้ตระหนักถึงความปลอดภัยในการใช้สารสนเทศในองค์กร และสามารถนำไปเป็นแนวทางให้องค์กรกำหนดนโยบายการควบคุมดูแลการใช้ระบบสารสนเทศ

คำสำคัญ : ระดับการรักษาความมั่นคงปลอดภัย การตระหนักถึงความปลอดภัย ระบบสารสนเทศ

Factors Affecting the Security Level of Information Systems in Organization

Supichaya Archavajirada*

Computer Center, Srinakharinwirot University

***Correspondence:** supichaya_a@hotmail.com doi: 10.14456/jisb.2016.11

Abstract

Nowadays Information System plays a vital role in running businesses. However, top ranking of their risk is to adopt technology to the organization by not taking the consideration in high level of data security, simultaneously. Technically, data security for organization's information system is very important. Thus, organization would review and raise security's level. Besides, management has to promote not only realization in data security's importance to all staffs, stakeholders, and shareholders but also ethic by not to externally broadcasting organization's data, which is very important organization's asset. This practice tends to help organization to have higher data security's level. Researcher studies factors affecting to level of Information System's data security. This research is a quantitative survey study by collecting data from staffs in the organization, being public company limited total 240 copies. Then, all data is analyzed by regression equation to study factors affecting to realization in data security within the organization. The result of this research represents that risk's awareness, training, and learning in information system altogether impacting to realization in data security. If staffs start realizing in importance of data security, level of its will increase, absolutely. The benefit of research can help to understand level of information system's data security in the organization and can be guideline for organization to set up policy and monitor information system usage.

Keywords: security of information systems, security awareness, information systems

1. บทนำ

เทคโนโลยีสารสนเทศและการสื่อสาร ได้มีอิทธิพลและขยายความสำคัญต่อรูปแบบการดำเนินชีวิตเป็นอย่างมาก โดยเฉพาะด้านเทคโนโลยีสารสนเทศที่มีคุณประโยชน์หลากหลายประการ และเป็นปัจจัยหลักในการพัฒนาประเทศในทุกด้าน ก่อให้เกิดสังคมไร้พรมแดนที่ผู้คนทั่วโลกสามารถสื่อสารได้อย่างสะดวกรวดเร็ว และเป็นสื่อที่ช่วยสนับสนุนให้เกิดการพัฒนาทั้งด้านเศรษฐกิจ สังคมและอุตสาหกรรม การพัฒนาคุณภาพชีวิต การเผยแพร่ข่าวสาร และการประชาสัมพันธ์ การส่งเสริมการท่องเที่ยว ตลอดจนการติดต่อสื่อสารโทรคมนาคม อย่างไรก็ตาม แม้ว่าเทคโนโลยีสารสนเทศจะให้คุณประโยชน์มากมายมหาศาลแก่ผู้ใช้งาน แต่ในขณะเดียวกันเทคโนโลยีสารสนเทศก็สามารถก่อให้เกิดผลกระทบทางลบแก่ผู้ใช้งานได้เช่นกัน เทคโนโลยีเหล่านี้ สามารถเป็นสะพานหรือเป็นช่องทางในการก่ออาชญากรรมในรูปแบบใหม่ เช่น การจารกรรมข้อมูล การสร้างข่าวสารอันเป็นเท็จ การหลอกลวงต่างๆ เป็นต้น สิ่งเหล่านี้ส่งผลเสียต่อผู้ใช้งานได้ หากผู้ใช้งานขาดความรู้ในการป้องกันตนเองอย่างเหมาะสม จึงอาจเป็นเหตุนำมาซึ่งความเสื่อมเสียต่อตัวเอง ข้อมูล และทรัพย์สิน เช่น การถูกหลอกลวงโดยมิจฉาชีพออนไลน์ การขโมยข้อมูลส่วนตัว การขโมยอีเมล์ หรือการหลอกลวงให้ทำการโอนย้ายข้อมูลและทรัพย์สิน เป็นต้น ซึ่งภัยจากเทคโนโลยีสารสนเทศเหล่านี้มีแนวโน้มที่จะเกิดมากขึ้น และมีวิธีการที่หลากหลายอีกด้วย ซึ่งผู้ใช้งานทั่วไปมีความเสี่ยงต่อภัยคุกคามจากการใช้เทคโนโลยีสารสนเทศที่อาจเกิดขึ้น เช่น ไวรัสคอมพิวเตอร์ บัญชีผู้ใช้ถูกแฮก การถูกบุกรุกคอมพิวเตอร์จากระยะไกล เป็นต้น โดยผู้ใช้งานอาจรับทราบถึงภัยคุกคามเหล่านี้ แต่อาจยังไม่ทราบถึงวิธีปฏิบัติหรือป้องกันและแก้ไขเมื่อเกิดภัยจากการใช้เทคโนโลยีสารสนเทศ เช่น เมื่อคอมพิวเตอร์ติดไวรัสควรทำอย่างไร หากเครื่องคอมพิวเตอร์ถูกแฮกควรทำอย่างไร (กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, 2557) ดังนั้นงานวิจัยนี้จึงมีวัตถุประสงค์เพื่อ ศึกษาปัจจัยที่ส่งผลต่อระดับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร ได้แก่ พฤติกรรมการใช้ และการตระหนักถึงความปลอดภัย ซึ่งการที่จะทำให้พนักงานเกิดการตระหนักได้นั้น ควรทำให้พนักงานเกิดความรู้ความเข้าใจในการใช้ระบบสารสนเทศอย่างปลอดภัย โดยการฝึกอบรมและให้ความรู้พร้อมทั้งทำให้พนักงานรับรู้ถึงภัยคุกคาม

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ผู้วิจัยได้นำแนวคิดทฤษฎี และงานวิจัยที่เกี่ยวข้องมาเป็นแนวทางในการศึกษาวิจัย ดังต่อไปนี้ (1) แนวคิดพฤติกรรมตามแผน (Theory of planned behavior หรือ TPB) นำเสนอโดย Ajzen เป็นแนวคิดทางจิตวิทยาสังคม (Social psychology) พัฒนามาจากแนวคิด TRA โดย Ajzen ได้เพิ่มปัจจัยการรับรู้ถึงการควบคุมพฤติกรรมของตนเองในการแสดงพฤติกรรมใดๆ (Perceived behavioral control) (สิงหะ ฉวีสุข, 2555) (2) แบบจำลองการสร้างความตระหนักเป็นแบบจำลอง ที่พัฒนาจากการศึกษาปัจจัยที่ส่งผลต่อการตระหนักถึงความเป็นส่วนตัวที่พัฒนาต่อยอดมาจากทฤษฎีพฤติกรรมตามแผนเช่นกัน ซึ่งแสดงให้เห็นว่าหากบุคคลเกิดการรับรู้จะส่งผลต่อความตระหนักและการตั้งใจ จากนั้นจะทำให้เกิดระดับการเปิดเผยข้อมูล (ภัททิยา นภาชัยเทพ, 2555) (3) แบบจำลองในการรักษาความมั่นคงปลอดภัยที่แสดงให้เห็นว่าการฝึกอบรมเป็นส่วนสำคัญในการทำให้พนักงานเกิดความตระหนักและยังส่งผลต่อระดับการรักษาความมั่นคงปลอดภัยที่เพิ่มขึ้นด้วย (Hale, 2012) อนึ่ง งานวิจัยนี้ได้ทำการศึกษาจากงานวิจัยในอดีต โดยมีทั้งหมด 6 ปัจจัย ดังต่อไปนี้

การรับรู้ถึงภัยคุกคาม (perceived threats) หมายถึง การทราบถึงความรุนแรงหรือผลกระทบของอันตรายที่จะเกิดขึ้น ซึ่งแสดงให้เห็นถึงความกลัวต่อความรุนแรง (Gore and Bracken, 2005) ซึ่งการรับรู้ถึงภัยคุกคามจะส่งผลต่อตวามรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ (Bulgurcu et al., 2010)

ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ (Insight into the security of information systems) หมายถึง การที่บุคคลมีความทรงจำในเรื่องราว ข้อเท็จจริง รายละเอียดต่างๆ และความสามารถในการนำความรู้ที่เก็บรวบรวมมาใช้ดัดแปลง อธิบาย เปรียบเทียบในเรื่องนั้นๆ ได้อย่างมีเหตุผลในเรื่องของระบบการรักษาความ

มั่นคงปลอดภัยด้านระบบสารสนเทศภายในองค์กร จึงทำให้สามารถก่อให้เกิดเป็นพฤติกรรมในการใช้สารสนเทศอย่างมีความตระหนักถึงความปลอดภัย (จักรกริช ใจดี, 2542) ซึ่งความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศจะส่งผลต่อการตระหนักถึงความปลอดภัย (Son and Jeong, 2013)

การฝึกอบรมและให้ความรู้ (Training and education) หมายถึง รูปแบบของการเรียนรู้ ความรู้ ทักษะ ค่านิยม ความเชื่อ และพฤติกรรมของกลุ่มคนที่ได้รับการถ่ายโอนจากบุคคลหนึ่งไปยังบุคคลอื่น ผ่านการเล่าเรื่อง การสนทนา การเรียนการสอน ด้านการรักษาความมั่นคงปลอดภัย เพื่อพัฒนาความรู้และให้พนักงานทราบถึงวิธีการรักษาความมั่นคงปลอดภัยต่อการใช้ระบบสารสนเทศในองค์กร (Gadzama et al., 2014) ซึ่งการฝึกอบรมและให้ความรู้จะส่งผลต่อความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ (Maqousi et al., 2014)

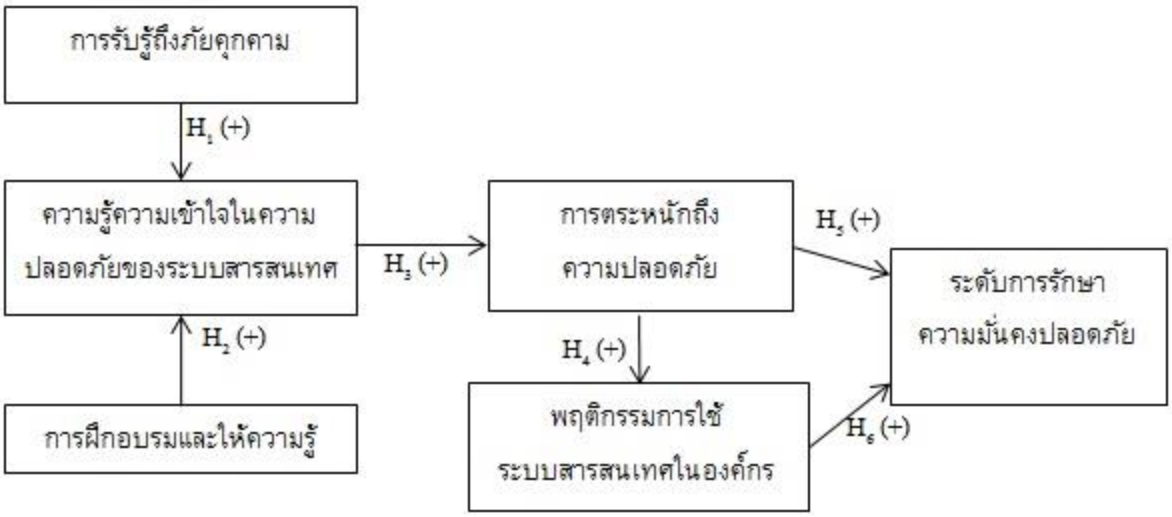
การตระหนักถึงความปลอดภัย (Awareness) หมายถึง ความสามารถในการรับรู้ หรือ รู้สึก หรือ มีสติ ต่อเหตุการณ์ ความรู้สึก หรือรูปแบบการสัมผัส การตระหนักถึงความปลอดภัยเกิดจากทัศนคติที่มีต่อสิ่งเร้าอันได้แก่ บุคคล สถานการณ์ กลุ่มสังคม และสิ่งต่าง ๆ ที่โน้มเอียง หรือตอบสนองในทางบวก หรือทางลบ เป็นสิ่งที่เกิดจากการเรียนรู้และประสบการณ์ (Solic et al., 2012) ซึ่งการตระหนักถึงความปลอดภัยจะส่งผลต่อพฤติกรรมการใช้ระบบสารสนเทศในองค์กร (Liang and Xue, 2009)

พฤติกรรมการใช้ระบบสารสนเทศในองค์กร (Bhavior) หมายถึง ความตั้งใจของพนักงานที่จะปฏิบัติตามมาตรการการรักษาความมั่นคงปลอดภัย จากทัศนคติ กฎเกณฑ์ ความเชื่อและการรับรู้ถึงมาตรการที่ควรปฏิบัติตาม ซึ่งพฤติกรรมดังกล่าวส่งผลกระทบต่อความปลอดภัยของการใช้ระบบสารสนเทศในองค์กร (Rocha et al., 2014) ซึ่งพฤติกรรมการใช้ระบบสารสนเทศในองค์กรจะส่งผลต่อระดับการรักษาความมั่นคงปลอดภัย (Bulgurcu et al., 2010)

ระดับการรักษาความมั่นคงปลอดภัย (Level of security) หมายถึง มาตรฐานที่องค์กรใช้ป้องกันภัยคุกคามที่เกิดขึ้นจากการนำระบบสารสนเทศมาใช้ในองค์กรและสามารถนำมาตรฐานนั้นมาตรวจสอบองค์กรของตนเองเพื่อดูว่าองค์กรของตนเองนั้นมีระดับการรักษาความมั่นคงปลอดภัยมากน้อยเพียงใด (Crossler et al., 2013) ซึ่งการที่องค์กรจะมีระดับการรักษาความมั่นคงปลอดภัยที่สูงขึ้นได้นั้น ขึ้นอยู่กับพฤติกรรมการใช้ระบบสารสนเทศในองค์กร และการตระหนักถึงความปลอดภัย ของพนักงาน

3. กรอบแนวคิดการวิจัยและสมมติฐานการวิจัย

จากทฤษฎี แนวคิดที่เกี่ยวข้อง และการทบทวนวรรณกรรมต่างๆที่ได้ทำการศึกษามาแล้วนั้น ซึ่งกล่าวโดยสรุปได้ว่า การรับรู้ ส่งผลให้เกิดความตระหนัก และแสดงออกเป็นพฤติกรรม จนสามารถกำหนดเป็นระดับต่างๆได้ โดยงานวิจัยนี้ได้เพิ่มปัจจัยด้าน การฝึกอบรมและการให้ความรู้ และความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศเข้าไปในงานวิจัย ทำให้สามารถกำหนดปัจจัยที่มีผลต่อการตระหนักถึงความปลอดภัยต่อการใช้ระบบสารสนเทศในองค์กร ได้ดังภาพที่ 1



ภาพที่ 1 กรอบแนวคิดระดับการรักษาความมั่นคงปลอดภัยต่อระบบสารสนเทศในองค์กร

การรับรู้ความรุนแรงของภัยคุกคามและการรับรู้ถึงสิ่งที่กระทบกระเทือนใจได้ง่ายซึ่งสิ่งกระทบกระเทือนใจได้ง่ายบางครั้งเรียกว่าการรับรู้ช่องโหว่ ที่เป็นตัวกระตุ้นให้เกิดการกระทำในการตอบสนองความกลัว เป็นการรับรู้ความน่าจะเป็นและการมีประสบการณ์กับอันตราย อย่างไรก็ตามการรับรู้ความรุนแรงเป็นระดับที่คนจะเชื่อว่าจะได้รับอันตรายถ้าหากบุคคลนั้นเคยมีประสบการณ์เกี่ยวกับอันตรายเหล่านั้น ดังนั้นเมื่อรับรู้ถึงความรุนแรง บุคคลจะเกิดความกลัวนั่นคือความกลัวไม่ได้ทำหน้าที่โดยตรงในความตั้งใจ แต่เพิ่มระดับความรุนแรงของการรับรู้ ซึ่งเมื่อบุคคลรับรู้ถึงความกลัวแล้วจะส่งผลให้บุคคลนั้นหาความรู้เพิ่มเติมเพื่อให้ตนเองเกิดความรู้ความเข้าใจถึงความปลอดภัย (Bulgurcu et al., 2010) ซึ่งสามารถตั้งสมมติฐานได้ดังนี้

H1 : การรับรู้ถึงถัยคุกคามส่งผลทางบวกต่อความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ

ปัญหาหลักของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่กำลังเติบโต คือความอ่อนแอที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยเนื่องจากผู้ใช้ที่มีความรู้ไม่เพียงพอ เกี่ยวกับการรักษาความมั่นคงปลอดภัย (Son and Jeong, 2013) ดังนั้นเมื่อมีการฝึกอบรมและให้ความรู้ เพื่อให้ผู้ใช้ เกิดความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ เพราะผลของการฝึกอบรมทำให้ผู้ใช้มีความรู้ความเข้าใจในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร ซึ่งสามารถตั้งสมมติฐานได้ดังนี้

H2 : การฝึกอบรมและให้ความรู้ส่งผลทางบวกต่อความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ

หากผู้ใช้เข้าใจถึงการใช้งานสารสนเทศในองค์กร ว่าการใช้งานอย่างไรก่อให้เกิดเป็นอันตรายได้นั้น ผู้ใช้จะตระหนักถึงอันตราย และเกิดการพัฒนาการรับรู้ของตนเอง (Liang and Xue, 2009) หากมีการให้ความรู้เกี่ยวกับรักษาความปลอดภัยที่มีจุดมุ่งหมายเพื่อให้ความรู้กับผู้ใช้ถึงภัยคุกคามทุกด้านที่อาจเกิดขึ้นและกล่าวถึงวิธีการเพื่อป้องกันการคุกคาม จะสามารถกำจัดหรือลดจำนวนของภัยคุกคามที่อาจเกิดขึ้นได้แล้วยังสามารถรักษาผู้ใช้และทรัพย์สินขององค์กรไว้ได้ (Maqousi et al., 2014) ซึ่งสามารถตั้งสมมติฐานได้ดังนี้

H3 : ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศส่งผลทางบวกต่อการตระหนักถึงความปลอดภัย

เมื่อตระหนักได้ว่ากำลังเผชิญอยู่กับภัยคุกคาม บุคคลจะมีส่วนร่วมในการแสดงออกทางพฤติกรรมเพื่อหลีกเลี่ยงภัยคุกคาม นั่นคือ เกิดเป็นพฤติกรรมเพื่อลดการเกิดภัยคุกคามจนกว่าภัยคุกคามที่เกิดขึ้นจะหายไป (Liang and Xue, 2009) โดยผู้ใช้ที่ไม่มีการตระหนักถึงความปลอดภัยของการใช้ระบบสารสนเทศในองค์กรจะกระทำพฤติกรรมที่อาจก่อให้เกิดภัยคุกคามต่อระบบสารสนเทศในองค์กร (Bulgurcu et al., 2010) ซึ่งสามารถตั้งสมมติฐานได้ดังนี้

H4 : การตระหนักถึงความปลอดภัยส่งผลทางบวกต่อพฤติกรรมการใช้ระบบสารสนเทศในองค์กร

เมื่อทุกคนในองค์กรตระหนักถึงความปลอดภัยของระบบสารสนเทศ โดยผู้ใช้ตระหนักถึงสิทธิของแต่ละบุคคลที่ได้รับอนุญาตให้ใช้ระบบ จะส่งผลดีให้แก่องค์กร ทำให้ผู้ใช้มีพฤติกรรมการใช้ระบบสารสนเทศอย่างถูกต้อง จึงทำให้องค์กรมีระดับการรักษาความปลอดภัยที่สูงขึ้น แต่หากผู้ใช้ไม่ตระหนักถึงความผิดพลาดที่อาจเกิดขึ้นได้นั้น จะเป็นอันตรายต่อความปลอดภัยของข้อมูล (Bulgurcu et al., 2010) ซึ่งสามารถตั้งสมมติฐานได้ดังนี้

H5 : การตระหนักถึงความปลอดภัยส่งผลทางบวกต่อระดับการรักษาความมั่นคงปลอดภัย

แม้องค์กรจะมีการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยเพื่อรักษาระดับการรักษาความมั่นคงปลอดภัยในองค์กรนั้น แต่ยังมีพนักงานที่ไม่ปฏิบัติตามนโยบายดังกล่าวหรือไม่ตระหนักถึงความปลอดภัย ดังนั้นองค์กรควรมีนโยบายการรักษาความมั่นคงปลอดภัยเพื่อให้แน่ใจว่าระดับการป้องกันและการรักษาความลับของข้อมูลที่สมบูรณ์ ทำให้ข้อมูลองค์กรไม่มีการทำลาย จนเกิดช่องโหว่ในการรักษาความมั่นคงปลอดภัย และความเสี่ยง รวมถึงการจัดการการรักษาความมั่นคงปลอดภัยของข้อมูล ให้ถูกต้องซึ่งการจัดการปัญหาที่เกี่ยวข้องกับข้อมูล จำเป็นต้องมีนโยบายการรักษาความมั่นคงปลอดภัยของข้อมูลในองค์กร เพื่อควบคุมพฤติกรรมการใช้ระบบสารสนเทศในองค์กร (Gadzama et al., 2014) ซึ่งสามารถตั้งสมมติฐานได้ดังนี้

H6 : พฤติกรรมการใช้ระบบสารสนเทศในองค์กรส่งผลทางบวกต่อระดับการรักษาความมั่นคงปลอดภัย

4. วิธีการวิจัย

งานวิจัยนี้จัดเก็บข้อมูลจากกลุ่มตัวอย่างที่เป็นพนักงานในองค์กรที่มีรายชื่อจดทะเบียนในตลาดหลักทรัพย์จำนวน 240 คน ผ่านทางการเก็บแบบสอบถามออนไลน์ อนึ่งก่อนการจัดเก็บข้อมูลจากกลุ่มตัวอย่าง งานวิจัยนี้ได้นำแบบสอบถามที่พัฒนามาจากงานวิจัยในอดีต (ประกอบด้วย Bulgurcu et al., 2010; Crossler et al., 2013; Kruger et al., 2011; Puhakainen and Siponen, 2010; Rocha et al., 2014) ไปทดสอบกับกลุ่มตัวอย่างจำนวน 240 คน ผลการทดสอบพบว่าข้อมูลไม่มีปัญหาด้านข้อมูลสุดโต่ง และพบว่ามีตัวแปรบางตัวที่ไม่ได้มีการกระจายแบบปกติ แต่ต่างจากเกณฑ์มาตรฐานไม่มากนัก ต่อจากนั้นจึงนำแบบสอบถามที่ปรับแก้ไปจัดเก็บข้อมูลจากกลุ่มตัวอย่างจริง

5. ผลการวิจัย

5.1 การทดสอบข้อตกลงเบื้องต้นทางสถิติ

ข้อมูลที่จัดเก็บจากกลุ่มตัวอย่างถูกนำไปทดสอบข้อมูลขาดหาย (Missing data) และข้อมูลสุดโต่ง (Outliers) นอกจากนี้ยังทดสอบว่าข้อมูล มีการกระจายแบบปกติ (Normal) มีความสัมพันธ์เชิงเส้นตรง (Linearity) มีภาวะร่วมเส้นตรงพหุ (Multicollinearity) และมีภาวะร่วมเส้นตรง (Singularity) หรือไม่ ผลการทดสอบพบว่า ข้อมูลไม่มีปัญหาด้านข้อมูลขาดหาย ข้อมูลสุดโต่ง และข้อมูลมีการกระจายเป็นแบบปกติ มีความสัมพันธ์เชิงเส้นตรง และไม่มีปัญหาภาวะร่วมเส้นตรงพหุและภาวะร่วมเส้นตรง

นอกจากนี้งานวิจัยได้ทดสอบความเชื่อถือของแบบสอบถาม โดยใช้การวิเคราะห์ค่าสัมประสิทธิ์อัลฟาของครอนบาช พบว่าทุกตัวแปรมีค่ามากกว่า 0.7 จึงถือว่ามีความเชื่อถือได้สำหรับงานวิจัยแบบ Basic research (กัลยา วานิชย์บัญชา, 2552) นอกจากนี้ยังได้ทดสอบความตรงของแบบสอบถาม ด้วยการวิเคราะห์องค์ประกอบ (Factor analysis) โดยใช้เกณฑ์ที่ข้อคำถามที่จับกลุ่มกันเป็นแต่ละตัวแปรต้องมีค่า Factor loading ไม่น้อยกว่า 0.5 ผลการวิเคราะห์องค์ประกอบได้จำนวนตัวแปรทั้งหมด 23 องค์ประกอบ (ตารางที่ 1 แสดงปัจจัยที่ได้จากการวิเคราะห์องค์ประกอบของงานวิจัยนี้) อนึ่งผลการวิเคราะห์ข้อมูลทั่วไปเกี่ยวกับผู้ตอบแบบสอบถามของกลุ่มตัวอย่าง พบว่าลักษณะประชากรส่วนใหญ่ เป็นเพศหญิง (64%) ช่วงอายุ 41-50 ปี (28%) ทำงานในกลุ่มอุสาหกรรมด้านการบริการ (34%) มีอายุการทำงานในองค์กรมากกว่า 10 ปีขึ้นไป (50%) ระดับการศึกษาอยู่ในระดับปริญญาตรี (54%) มีรายได้มากกว่า 55,000 บาท (51%) และเป็นพนักงานในระดับปฏิบัติการ (39%) ซึ่งกลุ่มตัวอย่างทั้งหมด 240 คน ปฏิบัติงานอยู่ในองค์กรที่มีรายชื่อจดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย

ตารางที่ 1 Factor analysis ของตัวแปรในงานวิจัย

ปัจจัย	น้ำหนักตัวประกอบ (Factor Loading)
ปัจจัย 1: การรับรู้ถึงภัยคุกคาม (Variance = 15.539, α = 0.746) ท่านรู้สึกไม่สบายใจเมื่อมีบุคคลอื่นมาขอใช้เครื่องคอมพิวเตอร์ของท่าน	0.715
ท่านมีความกังวลหากมีบุคคลอื่นมาใช้เครื่องคอมพิวเตอร์ของท่านโดยไม่ได้รับอนุญาต	0.826
ท่านรู้สึกกังวลว่าหากไม่มีการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ระบบสารสนเทศนั้นอาจเกิดอันตรายได้	0.696
ท่านรู้ว่าหากใช้ระบบสารสนเทศโดยไม่คำนึงถึงความปลอดภัย อาจก่อให้เกิดอันตรายต่อระบบสารสนเทศได้ เช่น โดนคุกคามจากไวรัส เป็นต้น	0.636
ปัจจัย 2: ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ (Variance = 13.249, α = 0.796) ท่านสามารถระบุได้ว่าโปรแกรมใดที่อาจเป็น spyware หรือ adware ที่รบกวนการทำงานของท่าน	0.819
ท่านมีความเข้าใจถึงวิธีการรักษาความมั่นคงปลอดภัย Information Security ในองค์กร	0.816
ท่านทราบถึงวิธีการป้องกัน ไม่ให้เครื่องคอมพิวเตอร์ของท่าน ถูกคุกคามจากโปรแกรมที่อาจเป็นไวรัสต่างๆ	0.826

ตารางที่ 1 Factor analysis ของตัวแปรในงานวิจัย (ต่อ)

ปัจจัย	น้ำหนักตัวประกอบ (Factor Loading)
ปัจจัย 3: การฝึกอบรมและให้ความรู้ (Variance = 12.442, α = 0.826) ท่านคิดว่าหากมีการให้ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร จะช่วยให้ “ท่าน” เข้าใจวิธีการรักษาความมั่นคงปลอดภัยต่อระบบสารสนเทศมากขึ้น	0.818
ท่านคิดว่าหากมีการให้ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร จะช่วยให้ “พนักงานในองค์กร” เข้าใจวิธีการรักษาความมั่นคงปลอดภัยต่อระบบสารสนเทศมากขึ้น	0.838
หากท่านได้รับการฝึกอบรมจะทำให้ท่านตระหนักถึงความปลอดภัยของข้อมูลในเครื่องคอมพิวเตอร์	0.748
สาเหตุที่พนักงานในองค์กรไม่คำนึงถึงความปลอดภัยต่อการใช้ระบบสารสนเทศในองค์กร ส่วนหนึ่งมาจากพนักงานไม่ได้รับการฝึกอบรมหรือให้ความรู้ที่เพียงพอ	0.647
ปัจจัย 4: การตระหนักถึงความปลอดภัย (Variance = 12.277, α = 0.613) ท่านมักจะมีการสำรองข้อมูลที่สำคัญ ไว้หลายๆ แห่งเสมอ เพื่อป้องกันการสูญหาย	0.729
เมื่อท่านได้รับ E-mail ที่กล่าวว่าส่งจากองค์กรที่น่าเชื่อถือ ให้ไปที่ link ตามที่แนบมากับ mail เพื่อยืนยันข้อมูลส่วนบุคคลของท่าน ท่านจะไม่ไปที่ link ดังกล่าวโดยทันที	0.824
หากท่านกำหนดรหัสผ่านในเครื่องคอมพิวเตอร์ส่วนบุคคลของท่าน ท่านจะคิดว่ารหัสผ่านดังกล่าวควรมีระดับความปลอดภัยมากน้อยแค่ไหน	0.568
ปัจจัย 5: พฤติกรรมการใช้ระบบสารสนเทศในองค์กร (Variance = 9.935, α = 0.613) ท่านให้ความสำคัญกับการจัดเก็บข้อมูลที่เป็นความลับขององค์กร	0.64
ท่านปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยในองค์กร	0.743
เมื่อปรากฏ pop up หรือหน้าต่างแจ้งเตือน ปรากฏขึ้นมาระหว่างการใช้เครื่องคอมพิวเตอร์ ท่านจะอ่านข้อความเหล่านั้นให้เข้าใจก่อนทำการ click ตัวเลือกใดๆ ก่อนเสมอ	0.692
หากท่านติดตั้งโปรแกรมสแกนไวรัสไว้ที่เครื่องคอมพิวเตอร์ส่วนบุคคลของท่าน ท่านจะทำการสแกนไวรัสเครื่องคอมพิวเตอร์ส่วนบุคคลทุกครั้งที่ท่านใช้งานเครื่องคอมพิวเตอร์	0.703

ตารางที่ 1 Factor analysis ของตัวแปรในงานวิจัย (ต่อ)

ปัจจัย	น้ำหนักตัวประกอบ (Factor Loading)
ปัจจัย 6: ระดับการรักษาความมั่นคง (Variance = 10.333, α = 0.727) ระบบสารสนเทศในองค์กรของท่าน มีการกำหนดสิทธิ์ในการเข้าถึงข้อมูลที่แตกต่างกัน เช่น ระดับผู้บริหาร และระดับปฏิบัติการ เป็นต้น	.520
องค์กรของท่านมีการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นลายลักษณ์อักษร	.765
องค์กรของท่านมีการประกาศหรือแจ้งนโยบายดังกล่าวให้บุคลากรรับทราบ	.784
ผู้บริหารมีการสนับสนุนการดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภับของระบบสารสนเทศ หรือไม่ (เช่น งบประมาณ บุคลากร อุปกรณ์ เป็นต้น)	.630
องค์กรของท่านมีการดูแลด้านความมั่นคงปลอดภัย เมื่อมีการว่าจ้างหน่วยงานภายนอก (Outsource) เพื่อปรับปรุงระบบสารสนเทศขององค์กร	.598

5.2 การวิเคราะห์ผลการวิจัย

การทดสอบสมมติฐานการวิจัยในครั้งนี้ ผู้วิจัยใช้วิธีวิเคราะห์การถดถอยเชิงเส้นเดียว (Simple linear regression) และการวิเคราะห์การถดถอยพหุคูณ (Multiple regression) โดยใช้ค่า p-value ที่น้อยกว่าหรือเท่ากับ 0.05 เป็นตัวกำหนดนัยสำคัญทางสถิติ โดยแบ่งการวิเคราะห์ออกเป็น 4 ส่วน ตามกรอบแนวคิดการวิจัยดังนี้

ส่วนที่ 1 การวิเคราะห์ความสัมพันธ์ระหว่างตัวแปร การรับรู้ถึงภัยคุกคาม และ การฝึกอบรมและให้ความรู้ กับ ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ พบว่ามีความสัมพันธ์โดยตรงกับตัวแปรตาม คือ ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ โดยค่า R = 0.258 และสามารถอธิบายความผันแปรของตัวแปรตามได้ร้อยละ 6.7 (R^2 = 0.067) นอกจากนี้ผลการวิเคราะห์ความถดถอยยังแสดงให้เห็นว่าตัวแปรอิสระกำหนดตัวแปรตาม คือ ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ ที่ระดับนัยสำคัญ p = 0.000 ($F_{(1.237)}$ = 8.479) (ดังแสดงในตารางที่ 2-3) ซึ่งสอดคล้องกับงานวิจัยของ Bulgurcu et al. (2010) ที่กล่าวว่าเมื่อบุคคลรับรู้ถึงความกลัวแล้วจะส่งผลให้บุคคลนั้นหาความรู้เพิ่มเติมเพื่อให้ตนเองเกิดความรู้ความเข้าใจ และ Son and Jeong (2013) ได้กล่าวว่าการฝึกอบรมทำให้ผู้ใช้มีความรู้ความเข้าใจในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร

ตารางที่ 2 ค่าสถิติการวิเคราะห์การถดถอย (Regression model) ของความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	**5.028**	**2**	**2.514**	**8.479**	**0.000***
Residual	70.268	237	.296		
Total	75.296	239			

* p < 0.05

ตารางที่ 3 ผลการวิเคราะห์การถดถอยแบบปกติ (Coefficients) ของความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ

ตัวแปร	ค่าสัมประสิทธิ์ถดถอย (b)	ค่าสัมประสิทธิ์ถดถอยปรับมาตรฐาน (beta)	T	Sig.
ค่าคงที่	**2.320**		**7.082**	**0.000**
การรับรู้ถึงภัยคุกคาม	.131	.127	1.977	0.049
การฝึกอบรมและให้ความรู้	.253	.247	3.585	0.000

หมายเหตุ * $p < 0.05$

$R = .258$, $R^2 = .067$, $SE = .544$

ส่วนที่ 2 การวิเคราะห์ความสัมพันธ์ระหว่างตัวแปร ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ และการตระหนักถึงความปลอดภัย พบว่ามีความสัมพันธ์โดยตรงกับตัวแปรตาม คือ การตระหนักถึงความปลอดภัย โดยค่า $R = 0.237$และสามารถอธิบายความผันแปรของตัวแปรตามได้ร้อยละ 5.6 ($R^2 = 0.056$) นอกจากนี้ผลการวิเคราะห์ความถดถอยยังแสดงให้เห็นว่าตัวแปรอิสระกำหนดตัวแปรตาม คือ ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ ที่ระดับนัยสำคัญ $p = 0.000$ ($F_{(1.238)} = 14.145$) (ดังแสดงในตารางที่ 4-5) ซึ่งสอดคล้องกับงานวิจัยของ Liang and Xue (2009) ได้กล่าวว่าหากผู้ใช้มีความรู้และเข้าใจถึงการใช้งานสารสนเทศในองค์กร ว่าการใช้งานอย่างไรก่อให้เกิดเป็นอันตรายได้นั้น ผู้ใช้จะตระหนักถึงอันตราย

ตารางที่ 4 ค่าสถิติการวิเคราะห์การถดถอย (Regression model) ของ การตระหนักถึงความปลอดภัย

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	**3.407**	**1**	**3.407**	**14.145**	**0.000***
Residual	57.326	238	.241		
Total	60.733	239			

* $p < 0.05$

ตารางที่ 5 ผลการวิเคราะห์การถดถอยแบบปกติ (Coefficients) ของการตระหนักถึงความปลอดภัย

ตัวแปร	ค่าสัมประสิทธิ์ถดถอย (b)	ค่าสัมประสิทธิ์ถดถอยปรับมาตรฐาน (beta)	T	Sig.
ค่าคงที่	**3.041**		**15.224**	**0.000**
ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ	.213	.237	3.761	0.000

หมายเหตุ * $p < 0.05$

$R = .237$, $R^2 = .056$, $SE = .490$

ส่วนที่ 3 การวิเคราะห์ความสัมพันธ์ระหว่างตัวแปร การตระหนักถึงความปลอดภัย และ พฤติกรรมการใช้ระบบสารสนเทศในองค์กร พบว่ามีความสัมพันธ์โดยตรงกับตัวแปรตาม คือ พฤติกรรมการใช้ระบบสารสนเทศในองค์กร โดยค่า $R = 0.325$และสามารถอธิบายความผันแปรของตัวแปรตามได้ร้อยละ 10.6 ($R^2 = 0.106$) นอกจากนี้ผลการวิเคราะห์ความถดถอยยังแสดงให้เห็นว่าตัวแปรอิสระกำหนดตัวแปรตาม คือ พฤติกรรมการใช้ระบบสารสนเทศในองค์กร ที่ระดับนัยสำคัญ $p = 0.000$ ($F_{(1.238)} = 28.080$) (ดังแสดงในตารางที่ 6-7) ซึ่งสอดคล้องกับงานวิจัยของ Liang and Xue (2009) ได้กล่าวว่า เมื่อบุคคลตระหนักได้ว่ากำลังเผชิญอยู่กับภัยคุกคาม บุคคลจะมีส่วนร่วมในการหลีกเลี่ยงภัยคุกคาม นั่นคือ เกิดเป็นพฤติกรรมเพื่อลดการเกิดภัยคุกคามจนกว่าภัยคุกคามที่เกิดขึ้นจะหายไป

ตารางที่ 6 ค่าสถิติการวิเคราะห์การถดถอย (Regression model) ของ พฤติกรรมการใช้ระบบสารสนเทศในองค์กร

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	**6.371**	**1**	**6.371**	**28.080**	**0.000***
Residual	54.001	238	.227		
Total	60.373	239			

* $p < 0.05$

ตารางที่ 7 ผลการวิเคราะห์การถดถอยแบบปกติ (Coefficients) ของ พฤติกรรมการใช้ระบบสารสนเทศในองค์กร

ตัวแปร	ค่าสัมประสิทธิ์ถดถอย (b)	ค่าสัมประสิทธิ์ถดถอยปรับมาตรฐาน (beta)	T	Sig.
ค่าคงที่	**2.896**		**12.416**	**0.000**
การตระหนักถึงความปลอดภัย	.324	.325	5.299	0.000

หมายเหตุ * $p < 0.05$

$R = .325$, $R^2 = .106$, $SE = .476$

ส่วนที่ 4 การวิเคราะห์ความสัมพันธ์ระหว่างตัวแปร การตระหนักถึงความปลอดภัย และ พฤติกรรมการใช้ระบบสารสนเทศในองค์กร กับ ระดับการรักษาความมั่นคงปลอดภัย พบว่ามีความสัมพันธ์โดยตรงกับตัวแปรตาม คือ ระดับการรักษาความมั่นคงปลอดภัย โดยค่า R = 0.510 และสามารถอธิบายความผันแปรของตัวแปรตามได้ร้อยละ 26.1 (R^2 = 0.261) นอกจากนี้ผลการวิเคราะห์ความถดถอยยังแสดงให้เห็นว่าตัวแปรอิสระกำหนดตัวแปรตาม คือ ระดับการรักษาความมั่นคงปลอดภัย ที่ระดับนัยสำคัญ p = 0.000 ($F_{(1.237)}$ = 41.751) (ดังแสดงในตารางที่ 8-9) ซึ่งสอดคล้องกับงานวิจัยของ Bulgurcu et al. (2010) ได้กล่าวว่า เมื่อทุกคนในองค์กรตระหนักถึงความมั่นคงปลอดภัยของระบบสารสนเทศ จะส่งผลให้องค์กรมีระดับ การรักษาความมั่นคงปลอดภัยที่สูงขึ้น และ Gadzama et al. (2014) ได้กล่าวว่าพฤติกรรมการใช้ระบบสารสนเทศส่งผลต่อความมั่นคงปลอดภัยขององค์กร

ตารางที่ 8 ค่าสถิติการวิเคราะห์การถดถอย (Regression model) ของ ระดับการรักษาความมั่นคงปลอดภัย

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	**25.735**	**2**	**12.868**	**41.751**	**0.000***
Residual	73.044	237	.308		
Total	98.780	239			

* p < 0.05

ตารางที่ 9 ผลการวิเคราะห์การถดถอยแบบปกติ (Coefficients) ของ ระดับการรักษาความมั่นคงปลอดภัย

ตัวแปร	ค่าสัมประสิทธิ์ถดถอย (b)	ค่าสัมประสิทธิ์ถดถอยปรับมาตรฐาน (beta)	T	Sig.
ค่าคงที่	**1.050**		**3.009**	**0.000**
การตระหนักถึงความปลอดภัย	.311	.244	3.884	0.003
พฤติกรรมการใช้ระบบสารสนเทศในองค์กร	.606	.474	8.025	0.000

หมายเหตุ * p < 0.05

R = .510, R^2 =.261, SE = .555

6. สรุปผลการวิจัย

งานวิจัยนี้จัดเก็บข้อมูลจากแบบสอบถามในรูปแบบออนไลน์ และนำข้อมูลที่เก็บรวบรวมมาวิเคราะห์ผลทางสถิติ ซึ่งจากการวิจัยพบว่าหากทำให้พนักงานรับรู้ถึงอันตรายที่อาจเกิดขึ้นพร้อมทั้งมีการฝึกอบรมให้แก่พนักงานแล้วนั้นจะส่งผลต่อความเข้าใจของพนักงาน และเมื่อพนักงานเกิดความเข้าใจถึงวิธีการรักษาความมั่นคงปลอดภัยจากการใช้ระบบสารสนเทศจะทำให้พนักงานเกิดการตระหนักถึงการใช้ระบบสารสนเทศดังกล่าว และนำไปสู่พฤติกรรมการใช้งานที่คำนึงถึงความปลอดภัย สุดท้ายส่งผลให้องค์กรมีระดับการรักษาความมั่นคงปลอดภัยที่สูงขึ้นตามไปด้วย

เนื่องจากปัจจุบัน สารสนเทศเข้ามามีบทบาทสำคัญยิ่งต่อองค์กรหลายแห่ง บางองค์ใช้ระบบสารสนเทศเป็นหลักในการขับเคลื่อนธุรกิจให้มีการเจริญเติบโต และใช้ระบบสารสนเทศเก็บข้อมูลต่างๆ ขององค์กร ดังนั้นองค์กรจึงต้องเห็น

ความสำคัญในการรักษาความมั่นคงปลอดภัย ของการใช้ระบบสารสนเทศเพื่อปกป้องข้อมูลให้มีความปลอดภัยอยู่เสมอ ซึ่งสามารถสรุปประโยชน์ที่ได้รับจากงานวิจัยได้ ดังนี้

(1) ผลของงานวิจัยแสดงให้เห็นว่าระดับการรักษาความมั่นคงปลอดภัยนอกจากจะขึ้นอยู่กับ การรับรู้ถึงภัยคุกคาม และ พฤติกรรมการใช้ระบบสารสนเทศในองค์กร ตามทฤษฎีพฤติกรรมตามแผน ยังขึ้นอยู่กับปัจจัยด้าน ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ การฝึกอบรมและให้ความรู้ และ การตระหนักถึงความปลอดภัย ซึ่งเป็นปัจจัยที่ได้จากการทบทวนวรรณกรรม เพื่อเสริมเข้าไปในทฤษฎีพฤติกรรมตามแผน

(2) งานวิจัยนี้สามารถประยุกต์ใช้ในแง่ของธุรกิจต่อองค์กรอื่นๆที่มีรายชื่อจดทะเบียนในตลาดหลักทรัพย์ได้ ซึ่งผลของการวิจัยทำให้ทราบว่าหากพนักงานในองค์กรมีความตระหนักถึงความปลอดภัยแล้วจะส่งผลให้องค์กรมีระดับการรักษาความมั่นคงปลอดภัยที่เพิ่มขึ้นดังนั้นองค์กรจึงต้องเพิ่มปัจจัยต่างๆที่จะทำให้พนักงานเกิดความตระหนักมากขึ้น ได้แก่การทำให้พนักงานรับรู้ถึงภัยคุกคามและมีความรู้ความเข้าใจในการรักษาความมั่นคงปลอดภัยโดยการจัดการฝึกอบรมและให้ความรู้แก่พนักงาน หรือมีการประชาสัมพันธ์ให้พนักงานทุกคนในองค์กรทราบถึงวิธีการรักษาความมั่นคงปลอดภัยเบื้องต้น และส่วนที่สำคัญก็คือ การที่ผู้บริหารเห็นความสำคัญในการรักษาความมั่นคงปลอดภัยต่อระบบสารสนเทศในองค์กร

งานวิจัยนี้ศึกษาอิทธิพลที่มีต่อระดับการรักษาความมั่นคงปลอดภัยของการใช้ระบบสารสนเทศในองค์กร ซึ่งศึกษาเฉพาะกลุ่มพนักงานที่ทำงานในองค์กรที่มีการจดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทยเท่านั้น ดังนั้นงานวิจัยในอนาคตควรศึกษาเพิ่มเติม ในกลุ่มองค์กรอื่นๆ เช่น หน่วยงานรัฐบาล หน่วยงานรัฐวิสาหกิจ หรือ บริษัทข้ามชาติ เป็นต้น นอกจากนี้ ระเบียบวิธีวิจัยจากงานวิจัยนี้เป็นรูปแบบงานวิจัยเชิงปริมาณที่เก็บรวบรวมข้อมูลโดยการสำรวจ จากการทำแบบสอบถามและนำข้อมูลที่ได้มาวิเคราะห์ผลทางสถิติ จึงควรศึกษาในรูปแบบงานวิจัยเชิงคุณภาพเพิ่มเติม ซึ่งเป็นการวิจัยที่ไม่เน้นข้อมูลตัวเลข แต่เน้นการหารายละเอียดต่างๆ ของกลุ่มประชากรที่ทำการศึกษาจึงก่อให้เกิดความรู้ความเข้าใจอย่างลึกซึ้งในเรื่องนั้นๆ เพื่อค้นหาปัจจัยที่ส่งผลให้พนักงานเกิดความตระหนักและส่งผลให้มีระดับการรักษาความมั่นคงปลอดภัยต่อการใช้ระบบสารสนเทศในองค์กรเพิ่ม มากขึ้น

จากผลการวิจัยทำให้พบว่าปัจจัยที่ได้กล่าวมาทั้งหมด อาจจะยังไม่ใช่ปัจจัยทั้งหมดที่ส่งผลต่อระดับการรักษาความมั่นคงปลอดภัย จากค่าทางสถิติที่สามารถอธิบายความผันแปรของตัวแปรตามไม่มากนัก จึงแสดงให้เห็นว่าปัจจัยในกรอบการวิจัยนี้ยังไม่ครอบคลุมถึงปัจจัยที่ส่งผลต่อระดับการรักษาความมั่นคงปลอดภัยทั้งหมด ผู้สนใจสามารถทำการศึกษาเพิ่มเติมว่ามีปัจจัยอื่นใด ที่จะส่งผลต่อระดับการรักษาความมั่นคงปลอดภัยอีกหรือไม่

บรรณานุกรม

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (2557). วิธีปฏิบัติตนเมื่อเกิดภัยคุกคามจากการใช้เทคโนโลยีสารสนเทศ. ดึงข้อมูลวันที่ 20 มิถุนายน 2557, จาก http://www.ictkm.info/content /detail/112.html.

กัลยา วานิชย์บัญชา. (2552). สถิติสำหรับงานวิจัย (พิมพ์ครั้งที่ 4). กรุงเทพฯ: โรงพิมพ์แห่งจุฬาลงกรณ์ มหาวิทยาลัย.

จักรกริช ใจดี. (2542). *ความเข้าใจเกี่ยวกับประชาธิปไตย ของนิสิตมหาวิทยาลัยเกษตร*. กรุงเทพมหานคร: วิทยานิพนธ์ปริญญาโท, มหาวิทยาลัยเกษตรศาสตร์.

ภัททิยา นภาชัยเทพ. (2555). *การตระหนักถึงความเป็นส่วนตัวในการใช้เฟซบุ๊ก.* วิทยานิพนธ์ที่ยังไม่ได้ตีพิมพ์, มหาวิทยาลัยธรรมศาสตร์.

สิงหะ ฉวีสุข และ สุนันทา วงศ์จตุรภัทร. (2555). *ทฤษฎีการยอมรับการใช้เทคโนโลยีสารสนเทศ*. วิทยานิพนธ์ที่ ยังไม่ได้ตีพิมพ์, สถาบันพระจอมเกล้าเจ้าคุณทหารลาดกระบัง.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information Security Policy Compliance: Anempirical Study Of Rationality-Based Beliefsand Information Security Awareness. *MIS Quarterly*, 34(3), 523-548.

Crossler, E. R., Johnston, C. A., Lowry, B. P., Hu, Q., Warkentin, M., and Baskerville, R. (2013). Future directions for behavioral information security research. *ELSEVIER*, 32, 90-101.

Gadzama, W. A., Katuka, J. I., Gambo, Y., Abali, A. M., and Usman, M. J. (2014). Evaluation of employees awareness and usage of information security policy in organizations of developing countries: a study of federal inland revenue service. Journal of Theoretical and Applied Information Technology, 67(2), 443-460.

Gore, T. D., and Bracken, C. C. (2005). Testing the theoretical design of a health risk message: Reexamining the major tenets of the extended parallel process model. *Health Education and Behavior*, 32(1), 27-41.

Hale, Gr. (2012). SCADA Security is a Mindset. Retrieved April 20, 2015 from https://www.tofinosecurity.com/blog/scada-security-mindset-isssource-explains-why-belden-design-seminar.

Kruger, H., Flowerday, S., Drevin, L., and Steyn, T. (2011). An assessment of the role of cultural factors in information security awareness. *IEEE*, 978-984.

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

Maqousi, A., Balikhina, T., Meridji, K., and Al-Sarayreh, Kh. T. (2014). A reference model of security requirements for early identification and measurement of security awareness program. *Journal of Theoretical and Applied Information Technology*, 63(1), 74-84.

Puhakainen, P., and Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, 34(4), 757-778.

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

Solic, K., Tovjanin, B., and Ilakovac, V. (2012). Assessment Methodology for the Categorization of ICT System Users Security Awareness. *MIPRO*, 1560-1564.

Son, H. J., and Jeong, S. (2013). A Research on Security Awareness and Countermeasures for the Single Server. *International Journal of Security and Its Applications*, 7(6), 31-42.