พฤติกรรมการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวภายใน Public Cloud

นิธิป ชวนตันติกมล*

Digital Media Asia Pacific (Toyota Group)

***Correspondence:** z_generation@hotmail.com doi: xxxxx

บทคัดย่อ

งานวิจัยนี้นำเสนอผลการศึกษาเกี่ยวกับพฤติกรรมการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวภายใน Public Cloud ซึ่งส่งผลต่อปัจจัยการรับรู้ถึงจุดอ่อน การรับรู้ความรุนแรงของภัยคุกคาม การรับรู้ถึงภัยคุกคามต่อข้อมูลส่วนตัว การรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัว การรับรู้ค่าใช้จ่ายจากการใช้เครื่องมือป้องกันภัยคุกคาม การรับรู้ความสามารถของตนเองในการรับมือภัยคุกคาม การรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว แรงจูงใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว ความตระหนักในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว และพฤติกรรมการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว โดยเก็บข้อมูลจากกลุ่มตัวอย่างผู้มีประสบการณ์ในการใช้งาน Public Cloud จำนวน 290 คน ผ่านการแจกแบบสอบถามออนไลน์ ผู้วิจัยได้ตรวจสอบความเที่ยงของเครื่องมือ (Reliability Analysis) ตรวจสอบแบบสอบถามโดยการวิเคราะห์องค์ประกอบ (Factor Analysis) และทดสอบสมมติฐานตามแบบจำลองโดยใช้การวิเคราะห์การถดถอยเชิงพหุคูณ (Multiple Regression Analysis) ระยะเวลาดำเนินงาน เดือนกุมภาพันธ์ – เมษายน 2558 มีผลการวิจัยดังนี้

ปัจจัยที่ส่งผลโดยตรงต่อการรับรู้ถึงภัยคุกคาม (Perceived Threat) ประกอบด้วย ปัจจัยการรับรู้ถึงจุดอ่อน (Perceived Susceptibility) ปัจจัยการรับรู้ความรุนแรง (Perceived Severity) ปัจจัยที่ส่งผลโดยตรงต่อการรับรู้ความสามารถในการหลีกเลี่ยง (Pereived Avoidability) ประกอบด้วย ปัจจัยการรับรู้ประสิทธิผล (Perceived Effectiveness) การรับรู้ค่าใช้จ่าย (Perceived Costs) และปัจจัยการรับรู้ประสิทธิภาพของตนเอง (Self-Efficacy) ปัจจัยที่ส่งผลโดยตรงต่อพฤติกรรมการหลีกเลี่ยง (Avoidance Behavior) ประกอบด้วย ปัจจัยแรงจูงใจในการหลีกเลี่ยง (Avoidance Motivation) และปัจจัยความตระหนักในการหลีกเลี่ยงภัยคุกคาม (Awareness)

จากผลการวิจัยพบว่า ตัวแปรแรงจูงใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวภายใน Public Cloud ส่งผลต่อพฤติกรรมการหลีกเลี่ยงภัยคุกคามมากที่สุด และเมื่อศึกษาตัวแปรที่มีอิทธิพลต่อแรงจูงใจในการหลีกเลี่ยงภัยคุกคามพบว่าตัวแปรการรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคามนั้นมีอิทธิพลมากที่สุด ข้อค้นพบนี้สามารถนำมาใช้พัฒนาการป้องกันภัยคุกคามโดยมุ่งวางกลยุทธ์ให้ผู้ใช้บริการเล็งเห็นประโยชน์ในการหลีกเลี่ยงและหาทางป้องกันภัยที่อาจมาคุกคามข้อมูลส่วนตัว

คำสำคัญ: การหลีกเลี่ยงภัยคุกคาม การรับรู้ภัยคุกคาม แรงจูงใจในการหลีกเลี่ยงภัยคุกคาม พฤติกรรมการหลีกเลี่ยงภัยคุกคาม

Threat Avoidance Behavior of Privacy on Public Cloud

Nithip Chuantantigamol*

Digital Media Asia Pacific (Toyota Group)

***Correspondence:** z_generation@hotmail.com doi: xxxxx

Abstract

The purpose of this research is to identify the effect of Perceived Susceptibility, Perceived Severity, Perceived Threat, Perceived Effectiveness, Perceived Costs, Self-Efficacy, Perceived Avoidability, Avoidance Motivation and Awareness on the Behavior of Threat Avoidance on Public Cloud. Participants in this study were 290 person who have experience in using Public Cloud. The research material is online questionnaire which was shared via online media. The researcher has gone through Reliability Analysis to test the precision of tools, Factor Analysis to test the survey, and Multiple Regression Analysis to test the hypothesis of the model between February – April 2015.

The result shows that Perceived Threat has a direct impact on Perceived Susceptibility and Perceived Severity. Pereived Avoidability has a direct impact on Perceived Effectiveness and Perceived Costs and Self-Efficacy. Avoidance Behavior has a direct impact on Avoidance Motivation and Awareness.

The finding illustrates that “Avoidance Motivation” is the most influential factor effecting to Threat Avoidance Behavior, while the strongest factor effecting Avoidance Motivation is Perceived Avoidability. This insight could be exploited to prevent from Threats by focusing on how to convince people to perceived benefits from Threat Avoidance and find the method to protect personal information.

Keywords: Threat Avoidance, Perceived Threat, Avoidance Motivation, Avoidance Behavior

1. บทนำ

ปัจจุบันเทคโนโลยีด้านข้อมูลเปรียบเสมือนดาบสองคม เมื่อเทคโนโลยีเหล่านี้ได้รับการควบคุมที่ถูกต้องและเหมาะสม จะทำให้มีศักยภาพที่จะพัฒนาคุณภาพของมนุษย์และองค์กรต่าง ๆ อย่างไรก็ตามหากมีการนำเอาเทคโนโลยีด้านข้อมูลไปใช้ประโยชน์เพื่อวัตถุประสงค์ที่เป็นอันตราย มันจะเป็นภัยคุกคามที่ร้ายแรงต่อบุคคล องค์กรและสังคม ในหลายรูปแบบของการรุกรานด้านข้อมูลสารสนเทศ ดังเช่น ไวรัสคอมพิวเตอร์ หนอนเจาะระบบ อีเมลสแปม สปายแวร์ แอดแวร์และโทรจัน ซึ่งจะมีผลกระทบคอมพิวเตอร์ส่วนบุคคลและแม้แต่โครงสร้างพื้นฐานทางสารสนเทศขององค์กร ส่งผลเสียต่อผลผลิตและสูญเสียทางการเงิน (Bagchi and Udo, 2003; Stafford and Urbaczewski, 2004)

องค์ประกอบของความแตกต่างที่ทำให้เทคโนโลยีสารสนเทศประสบความสำเร็จคือ ความสามารถที่ทำให้ทุกอย่างกลายเป็นจริง มีคุณค่าและมีส่วนช่วยในการสนับสนุนทางเศรษฐกิจแก่โครงสร้างพื้นฐานของโลกแห่งเทคโนโลยี Cloud Computing จึงได้เข้ามาตอบรับโครงสร้างพื้นฐานนี้ และยังสร้างการวิจัยในโลกเสมือนขึ้นมา มีการประมวลผลแบบกระจายหรือที่เรียกว่า “Grid Computing” ใช้ประโยชน์ในการประมวลผล รวมถึงเชื่อมต่อเครือข่าย เวบไซต์และบริการทางด้านซอฟต์แวร์ เป็นการแสดงถึงสถาปัตยกรรมที่มุ่งเน้นด้านการบริการ ลดข้อมูลทางเทคโนโลยีสำหรับผู้ใช้งานที่ปลายทาง, มีความยืดหยุ่นสูงและลดต้นทุนในการให้บริการ (Vouk, 2008)

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

งานวิจัยนี้มีการนำทฤษฎีอ้างอิงมาใช้คือ Technology Threat Avoidance Model (TTAT) เป็น ทฤษฎีแยกแยะผู้ใช้บริการว่ามีความเข้าใจในเทคโนโลยี ซึ่งส่งผลต่อพฤติกรรมการหลีกเลี่ยงความเสี่ยงจากภัยคุกคามโดยจะแบ่งเป็นกรอบการประเมินภัยคุกคาม (Threat Appraisal) ประกอบด้วย การรับรู้ถึงความอ่อนไหวง่าย (Perceived Susceptibility) การรับรู้ถึงความรุนแรง (Perceived Severity) การรับรู้ถึงภัยคุกคาม (Perceived Threat) กรอบการประเมินการรับมือความเสี่ยง(Coping Appraisal) ประกอบด้วย การรับรู้ประสิทธิผล (Perceived Effectiveness) การรับรู้ราคา (Perceived Costs) ประสิทธิภาพของตนเอง (Self-Efficacy) การรับรู้ความสามารถในการหลีกเลี่ยง (Perceived Avoidability) และกรอบการรับมือ (Coping) ประกอบด้วย แรงจูงใจในการหลีกเลี่ยง(Avoidance Motivation) พฤติกรรมการหลีกเลี่ยง (Avoidance Behavior) การรับมือทางอารมณ์(Emotion-focused) ความเสี่ยงและอิทธิพลทางสังคม (Coping Risk Tolerance and Social Influence) นอกจากนี้งานวิจัยนี้ได้ทำการศึกษาจากงานวิจัยในอดีต โดยมีทั้งหมด 10 ปัจจัยดังต่อไปนี้ :

การรับรู้ถึงจุดอ่อน (Perceived Susceptibility) คือ การที่บุคคลรับรู้ถึงจุดอ่อนแอบนระบบของ Public Cloud ที่อาจถูกโจมตีหรือถูกบุกรุกโดยภัยต่างๆได้โดยง่าย (Liang and Xue, 2009) ซึ่งมาจากความอ่อนแอของระบบที่ไม่อาจป้องกันจากภัยคุกคาม

การรับรู้ความรุนแรงของภัยคุกคาม (Perceived Severity) คือ การที่บุคคลรับรู้ถึงผลกระทบจากภัยคุกคามว่าจะส่งผลด้านลบ มีสาเหตุมาจากความรุนแรงของภัยคุกคาม ซึ่งมีโอกาสส่งผลกระทบต่อระบบสารสนเทศ (Liang and Xue, 2009)

การรับรู้ถึงภัยคุกคามต่อข้อมูลส่วนตัว (Perceived Threat) คือ การรับรู้ถึงอันตรายจากภัยที่อาจมาคุกคามข้อมูลส่วนตัวภายใน Public Cloud และเกิดผลกระทบต่อคุณสมบัติของข้อมูลด้านใดด้านหนึ่งหรือมากกว่าหนึ่งด้าน (รุจิรา ธรรมสมบัติ, 2555) ภัยคุกคามยังสามารถเปลี่ยนจากภัยคุกคามธรรมดา ไปสู่ภัยคุกคามที่อาจสร้างความเสียหายให้แก่สารสนเทศขององค์กรได้

การรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัว (Perceived Effectiveness) คือ การรับรู้ถึงความสามารถในการรักษาข้อมูลส่วนตัวของเครื่องมือป้องกันภัยคุกคาม ว่ามีความปลอดภัยเพียงใด ต่อภัยจากภายนอกหรือภายในที่อาจมาคุกคามข้อมูล (Weinstein, 1993)

การรับรู้ค่าใช้จ่ายของเครื่องมือป้องกันภัยคุกคามข้อมูลส่วนตัว (Perceived Costs) คือ ระดับการรับรู้ถึงค่าใช้จ่ายที่ต้องใช้ รวมถึงประโยชน์ที่จะได้รับ หากใช้เครื่องมือในการป้องกันภัยคุกคามข้อมูลส่วนตัวจาก Public Cloud (Ng et al., 2009; Woon et al., 2005; Workman et al., 2008)

การรับรู้ประสิทธิภาพของตนเองในการรับมือภัยคุกคาม (Self Efficacy) คือ ระดับของการรับรู้ถึงความสามารถของบุคคลในการใช้เครื่องมือป้องกันเพื่อหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว (Liang and Xue, 2009) และเป็นการที่บุคคลตัดสินความสามารถของตนเองในการที่จะจัดการ โดยดำเนินการแสดงพฤติกรรมให้บรรลุเป้าหมายที่กำหนดไว้

การรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคาม (Perceived Avoiability) คือ การที่บุคคลรับรู้ว่าเครื่องมือป้องกันภัยคุกคามช่วยในการปกป้องข้อมูลและหลีกเลี่ยงจากภัยที่เข้ามาคุกคามข้อมูลส่วนตัวได้มากน้อยเพียงใด (Liang and Xue, 2009)

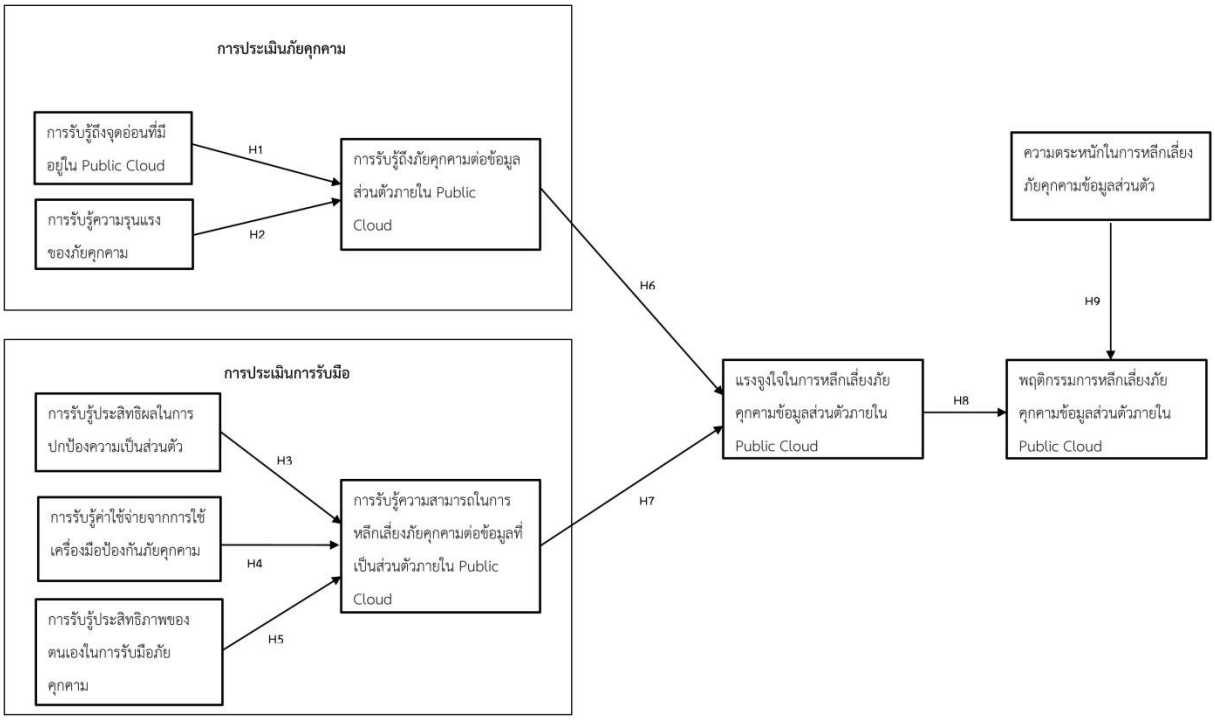
แรงจูงในในการหลีกเลี่ยง (Avoidance Motivation) คือ การที่บุคคลเกิดแรงกระตุ้นจากภัยที่มีความรู้สึกว่าอาจมาคุกคามข้อมูลส่วนตัง จึงหาทางที่จะหลีกเลี่ยงจากภัยเหล่านั้น (ธีรศักดิ์ แสงดิษฐ์, 2553)

ความตระหนัก (Awareness) คือ การรับรู้แบบฉุกคิดขึ้นมากะทันหัน ว่าภัยคุกคามที่พบนั้นอาจจะส่งผลกระทบต่อข้อมูลส่วนตัว ทั้งนี้ความตระหนักจะเกิดขึ้นได้นั้น ต้องอาศัยองค์ประกอบจาก สิ่งแวดล้อมรอบตัว การกระทำในอดีต และสิ่งที่ส่งผลกับอารมณ์และความรู้สึกเป็นต้น (เอกลักษณ์ ธนเจริญพิศาล, 2554)

พฤติกรรมการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวภายใน Public Cloud (Avoidance Behavior) คือ การที่บุคคลแสดงอาการที่อาจเป็นการหลีกเลี่ยงออกมาจากสถานการณ์ที่เป็นความเสี่ยงต่อข้อมูลส่วนตัวของผู้ใช้งานบน Public Cloud (Liang and Xue, 2009)

3. กรอบแนวคิดการวิจัยและสมมติฐานการวิจัย

จากการทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้องดังที่กล่าวมาข้างต้น ผู้วิจัยจึงได้พัฒนากรอบการวิจัย ดังแสดงในภาพที่ 1



ภาพที่ 1 แสดงกรอบแนวคิดเกี่ยวกับพฤติกรรมการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว

ผลการวิจัยของ Liang and Xue (2010) พบว่า การที่บุคคลทราบว่าจุดอ่อนของระบบ Public Cloud ที่เกิดขึ้นนั้นส่งผลทำให้ถูกโจมตีโดยภัยที่เข้ามาคุกคามได้โดยง่าย จึงทำให้เกิดการรับรู้ถึงภัยคุกคามต่อข้อมูลส่วนตัว นำไปสู่ข้อสมมติฐานดังนี้

H1: การรับรู้ถึงจุดอ่อนส่งผลเชิงบวกต่อการรับรู้ความเสี่ยงของภัยคุกคามข้อมูลส่วนตัวบน Public Cloud

ผลการวิจัยของ Liang and Xue (2009) พบว่า การที่บุคคลรับรู้ถึงผลกระทบจากภัยคุกคามว่าจะส่งผลต่อข้อมูลส่วนตัว โดยมีสาเหตุมาจากความรุนแรงของภัยคุกคาม และมีโอกาสจะส่งผลกระทบต่อระบบสารสนเทศด้วย เช่น เมื่อบุคคลรับรู้ว่าเขารู้สึกถึงภัยคุกคาม โดยภัยนั้นอาจจะมาโจมตีหรือขโมยข้อมูล ทำให้เกิดการรับรู้ถึงภัยที่เข้ามาคุกคามข้อมูลและหาวิธีป้องกัน นำไปสู่ข้อสมมติฐานดังนี้

H2: การรับรู้ความรุนแรงของภัยคุกคามส่งผลเชิงบวกต่อการรับรู้ความเสี่ยงของภัยคุกคามข้อมูลส่วนตัวบน Public Cloud

ผลการวิจัยของ Bandura (1982) ได้กล่าวว่า บุคคลที่มีความเชื่อมั่นในเครื่องมือป้องกันภัยคุกคาม ส่งผลให้รับรู้ถึงประสิทธิภาพในการป้องกันภัยคุกคามของเครื่องมือนั้น นำไปสู่ข้อสมมติฐานดังนี้

H3: การรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัวส่งผลเชิงบวกต่อการรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคาม

ผลการวิจัยของ Weinstein (1993) ได้ศึกษา พบว่าเป็นการที่ผู้ใช้งานรับรู้ถึงประโยชน์ที่จะได้รับจากการใช้เครื่องมือป้องกันภัยคุกคาม เมื่อเทียบกับค่าใช้จ่ายที่จะต้องเสียไป ดังนั้นเมื่อบุคคลเลือกที่จะใช้เครื่องมือเพื่อปกป้องจากภัยคุกคาม เขาจะไม่ได้คำนึงถึงแค่ความสามารถของเครื่องมือนั้น แต่ยังรวมถึงค่าใช้จ่ายที่ต้องใช้ด้วย นำไปสู่ข้อสมมติฐานดังนี้

H4: การรับรู้ค่าใช้จ่ายจากการป้องกันภัยคุกคาม จะส่งผลเชิงลบต่อการรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคามของเครื่องมือป้องกันภัยคุกคาม

ผลการวิจัยของ Bandura (1978) พบว่า ผู้ที่รับรู้ความสามารถของตนเองสูงจะส่งผลต่อความสำเร็จของบุคคล โดยที่บุคคลกล้าเผชิญต่อปัญหาต่าง ๆ แม้กระทำความล้มเหลว หรือสิ่งที่ยากและพยายามทำให้สำเร็จ โดยมีความคาดหวังเกี่ยวกับผลที่จะเกิดขึ้นสูง ดังนั้นบุคคลที่รับรู้ความสามารถของตนเองในการหลีกเลี่ยงภัยคุกคามได้สูง ทำให้มีโอกาสที่จะรับรู้ถึงภัยคุกคามและหาทางหลีกเลี่ยง นำไปสู่ข้อสมมติฐานดังนี้

H5: การรับรู้ความสามารถของตนเองในการรับมือภัยคุกคามส่งผลเชิงบวกต่อการรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคามของเครื่องมือป้องกันภัยคุกคาม

เมื่อบุคคลรับรู้ถึงภัยคุกคามด้านความปลอดภัยและความรุนแรงของภัยคุกคามซึ่งถือเป็นจุดอ่อนของระบบสารสนเทศ เขาก็จะมีแนวโน้มที่จะเกิดแรงจูงใจที่จะปฏิบัติตามนโยบายการรักษาความปลอดภัย เพื่อเลี่ยงภัยนั้น (ประภาดา ตลึงจิตร, 2553) ดังนั้นจึงสามารถตั้งสมมติฐานได้ดังนี้

H6: การรับรู้ถึงภัยคุกคามต่อข้อมูลส่วนตัวส่งผลเชิงบวกต่อแรงจูงใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว

การรับรู้ความสามารถในการหลีกเลี่ยงเป็นวิธีการที่จะตัดสินว่า เครื่องมือป้องกันจะมีประสิทธิภาพในการหลีกเลี่ยงภัยคุกคามทางสารสนเทศเพียงไร และจะสร้างความเชื่อมั่นของแต่บุคคลต่อเครื่องมือป้องกันได้อย่างไร ซึ่งบุคคลจะมีแรงจูงใจที่จะนำเครื่องมือป้องกันภัยคุกคามมาใช้ ก็ต่อเมื่อบุคคลนั้นรับรู้ว่าเครื่องมือป้องกันภัยคุกคามสามารถที่จะรับมือกับภัยนั้นได้ และเครื่องมือป้องกันที่มีประสิทธิภาพในการหลีกเลี่ยงภัยมากที่สุดจะถูกนำมาใช้เพื่อเลี่ยงภัยคุกคาม (Compeau and Higgins, 1995) ดังนั้นจึงสามารถตั้งสมมติฐานได้ดังนี้

H7: การรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคามของเครื่องมือป้องกันภัยคุกคามส่งผลเชิงบวกต่อแรงจูงใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว

เมื่อบุคคลที่มีแรงจูงใจในการหลีกเลี่ยงสูงมีแนวโน้มที่จะมีพฤติกรรมหลีกเลี่ยงภัยคุกคามโดยใช้เครื่องมือป้องกันภัยคุกคาม (Liang and Xue, 2010) เพื่อลดอัตราความเสี่ยงที่จะถูกโจมตีข้อมูล จะส่งผลต่อการเปลี่ยนแปลงพฤติกรรม เป็นแรงผลักดันให้บุคคลแสดงพฤติกรรมเพื่อประโยชน์จากเป้าหมายบางประการ

H8: แรงจูงใจในการหลีกเลี่ยงความเสี่ยงจากภัยคุกคามข้อมูลส่วนตัวส่งผลเชิงบวกต่อพฤติกรรมการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว

การที่บุคคลมีความตระหนักรู้และเข้าใจในศักยภาพที่สัมพันธ์กับความปลอดภัยของข้อมูลส่วนตัว จะทำให้เกิดพฤติกรรมที่ต้องการหลีกเลี่ยงจากความเสี่ยง ซึ่งความตระหนักรู้ถึงความปลอดภัยในข้อมูลอาจจะสร้างได้จากประสบการณ์ ดังเช่น บุคคลที่ไม่ยึดถือและปฏิบัติตามกฎของการรักษาความปลอดภัย จะมีความเสี่ยงจากการถูกโจมตีโดยไวรัส (Bulgurcu, et al., 2010) ดังนั้นจึงสามารถตั้งสมมติฐานได้ดังนี้

H9: ความตระหนักในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว ส่งผลเชิงบวกต่อพฤติกรรมการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว

4. วิธีการวิจัย

งานวิจัยนี้เป็นงานวิจัยเชิงปริมาณ (Quantitative Analysis) โดยใช้แบบสอบถาม เป็นเครื่องมือในการเก็บข้อมูล ซึ่งจะอธิบายถึงรายละเอียดการกำหนดประชากรและกลุ่มตัวอย่าง เครื่องมือที่ใช้ในงานวิจัย วิธีการเก็บรวบรวมข้อมูล และการวิเคราะห์ผลข้อมูล

อนึ่งก่อนการจัดเก็บข้อมูลจากกลุ่มตัวอย่าง งานวิจัยนี้ได้นำแบบสอบถามที่พัฒนามาจากงานวิจัยในอดีต (ประกอบด้วย Johnston and Allen, 2010; Xu et al., 2011; Lankton and Tripp, 2013; Dinev and Hart, 2004; Johnston and Warkentin, 2010; Putri and Hovav, 2014; Liang and Xue, 2010; He and Freeman, 2010; Xu and Chan, 2008; Schmidt et al., 2007) ไปทดสอบกับกลุ่มตัวอย่างจำนวน 30 คน ผลในการทดสอบพบว่าข้อมูลมีการกระจาย ซึ่งผู้วิจัยได้ทำการปรับเปลี่ยนข้อความในคำถามที่กระจายจากกลุ่มให้เหมาะสม ต่อจากนั้นจึงนำแบบสอบถามไปจัดเก็บข้อมูลจากกลุ่มตัวอย่างจริง

หลังจากทำการทดสอบความเหมาะสมเบื้องต้นของเครื่องมือแล้ว จึงเก็บข้อมูลจริงกับกลุ่มตัวอย่างจำนวน 300 คน และเนื่องจากเพื่อความสะดวกรวดเร็วในการกระจายและได้ข้อมูลตอบกลับที่มีคุณภาพ จึงใช้การส่งแบบสอบถามเวบไซต์ด้านเทคโนโลยีต่างๆ และผ่านทาง Online Media ผลที่ได้จึงได้รับแบบสอบถามตอบกลับมาทั้งหมด 290 ชุด

5. ผลการวิจัย

5.1 การทดสอบข้อตกลงเบื้องต้นทางสถิติ

ข้อมูลที่จัดเก็บจากกลุ่มตัวอย่างถูกนำไปทดสอบข้อมูลขาดหายและข้อมูลสุดโต่ง นอกจากนี้ยังทดสอบว่าข้อมูลมีการกระจายแบบปกติ มีความสัมพันธ์เชิงเส้นตรง มีภาวะร่วมเส้นตรงพหุ และมีภาวะร่วมเส้นตรงหรือไม่ ผลจากการทดสอบพบว่าข้อมูลไม่มีปัญหาด้านข้อมูลขาดหาย ข้อมูลสุดโต่ง และข้อมูลมีการกระจายเป็นแบบปกติ มีความสัมพันธ์เชิงเส้นตรงและไม่มีปัญหาภาวะร่วมเส้นตรงพหุและภาวะร่วมเส้นตรง ดังกล่าว

นอกจากนี้งานวิจัยได้ทดสอบความน่าเชื่อถือของแบบสอบถาม โดยพิจารณาจากค่าสัมประสิทธิ์ ครอนบัคแอลฟาที่สูงที่แต่ไม่น้อยกว่า 0.7 ซึ่งถือเป็นเกณฑ์ที่เหมาะสมสำหรับงานวิจัย Basic Research (Aoki and Downes, 2003) นอกจากนี้ยังได้ทดสอบความตรงของแบบสอบถามด้วยการวิเคราะห์องค์ประกอบโดยใช้เกณฑ์ข้อคำถามจับกลุ่มกันเป็นแต่ละตัวแปรต้องมีค่า น้ำหนักตัวประกอบไม่น้อยกว่า 0.5 (Hair et al., 2006, อ้างถึงใน อรวดี เนื่องฤทธ์, 2556) ผลการวิเคราะห์องค์ประกอบได้จำนวนทั้งหมด 10 องค์ประกอบ ประกอบด้วยการรับรู้ถึงจุดอ่อน การรับรู้ความรุนแรง การรับรู้ถึงภัย

คุกคาม การรับรู้ประสิทธิผล การรับรู้ต้นทุนจากการป้องกันภัยคุกคาม การรับรู้ความสามารถของตนเอง การรับรู้ความสามารถในการหลีกเลี่ยง แรงจูงในในการหลีกเลี่ยง ความตระหนักในการหลีกเลี่ยง และพฤติกรรมการหลีกเลี่ยง (ดังแสดงในตารางที่ 1)

ตารางที่ 1 ปัจจัยที่ได้จากการวิเคราะห์องค์ประกอบ

ปัจจัย	Factor Loading
ปัจจัย 1: การรับรู้ถึงจุดอ่อน (75.678% of variance, α = 0.838)	
ท่านคิดว่ามีความเป็นไปได้สูงที่ระบบ Public Cloud ที่ท่านใช้บริการอยู่ จะมีช่องโหว่ และอาจถูกคุกคาม	0.894
ท่านคิดว่ามีความเป็นไปได้สูงที่ระบบ Public Cloud ที่ท่านใช้บริการอยู่ จะมีสปายแวร์คุกคาม	0.864
ท่านคิดว่าระบบ Public Cloud ที่ท่านใช้บริการอยู่ อาจเก็บรักษาข้อมูลส่วนตัวของท่านได้ไม่เหมาะสม	0.851
ปัจจัย 2: การรับรู้ความรุนแรง (75.415% of variance, α = 0.891)	
ท่านคิดว่าสปายแวร์หรือไวรัสที่ติดมาจาก Public Cloud อาจลอบเก็บข้อมูลในคอมพิวเตอร์ของท่าน	0.846
ท่านคิดว่าสปายแวร์หรือไวรัสที่ติดมาจาก Public Cloud อาจทำให้คอมพิวเตอร์ของท่านทำงานได้ช้าลง	0.890
ท่านคิดว่าสปายแวร์หรือไวรัสที่ติดมาจาก Public Cloud ที่ท่านใช้บริการ อาจทำให้คอมพิวเตอร์ของท่านเสียหาย	0.918
ท่านคิดว่าสปายแวร์หรือไวรัสที่ติดมาจาก Public Cloud อาจจะควบคุมคอมพิวเตอร์ของท่านเพื่อไปขโมยข้อมูลของผู้อื่น	0.816
ปัจจัย 3: การรับรู้ถึงภัยคุกคาม (60.533% of variance, α = 0.795)	
ท่านรู้สึกไม่สบายใจหากข้อมูลส่วนตัวของท่านที่ถูกแชร์บน Public Cloud มีผู้อื่นเข้าถึงได้โดยง่าย	0.882
ท่านรู้สึกไม่สบายใจหาก Public Cloud มีเทคโนโลยีด้านความปลอดภัยที่ยังล้าหลัง จนทำให้ถูกคุกคาม	0.864

ตารางที่ 1 ปัจจัยที่ได้จากการวิเคราะห์องค์ประกอบ (ต่อ)

ปัจจัย	Factor Loading
ปัจจัย 4: การรับรู้ประสิทธิผล (66.940% of variance, α = 0.831)	
ท่านคิดว่านโยบายรักษาความเป็นส่วนตัวของ Public Cloud ที่ท่านใช้บริการ นำเครื่องมือป้องกันภัยคุกคามมาปกป้องข้อมูลได้เหมาะสม	0.818
ท่านคิดว่านโยบายรักษาความเป็นส่วนตัวของ Public Cloud ที่ท่านใช้บริการ จะช่วยกำจัดสปายแวร์ที่อาจมาคุกคามข้อมูลของท่าน	0.722
ท่านมั่นใจในนโยบายรักษาความเป็นส่วนตัวของ Public Cloud ที่ท่านใช้บริการ ว่าข้อมูลส่วนตัวจะถูกเก็บเป็นความลับจากผู้ไม่หวังดี	0.885
ท่านคิดว่านโยบายรักษาความเป็นส่วนตัวของ Public Cloud ที่ท่านใช้บริการอยู่ จะสามารถรักษาข้อมูลได้เป็นอย่างดี	0.840
ปัจจัย 5: การรับรู้ต้นทุนจากการป้องกันภัยคุกคาม (55.375% of variance, α = 0.684)	
ท่านจะเปรียบเทียบผลประโยชน์และค่าใช้จ่ายก่อนที่จะตัดสินใจใช้งานโปรแกรมแอนตีไวรัส	0.797
ท่านรับรู้ถึงประโยชน์ที่จะได้รับ และยอมรับค่าใช้จ่ายที่อาจเกิดขึ้นหากใช้โปรแกรมแอนตีไวรัสในการป้องกันภัยคุกคาม	0.856
ปัจจัย 6: การรับรู้ประสิทธิภาพของตนเอง (74.592% of variance, α = 0.886)	
ท่านคิดว่ามีความสามารถในการแก้ไขปัญหาที่มาจากภัยคุกคามใน Public Cloud ได้ด้วยตัวท่านเอง	0.902
ท่านคิดว่ามีความสามารถในการจัดการกับผู้ที่ต้องการขโมยข้อมูลส่วนตัวของท่านบน Public Cloud ได้	0.865
ท่านคิดว่าจะจัดการกับผู้ที่ต้องการขโมยข้อมูลส่วนตัวของท่านบน Public Cloud ด้วยตัวท่านเองก่อนที่จะปรึกษาผู้อื่น	0.880
ท่านคิดว่ามีความสามารถในการใช้โปรแกรมป้องกันภัยคุกคามใน Public Cloud เพื่อป้องกันสปายแวร์ที่อาจมาคุกคาม	0.849
ปัจจัย 7: การรับรู้ความสามารถในการหลีกเลี่ยง (64.723% of variance, α = 0.726)	
ท่านจะติดตามข่าวสารความเคลื่อนไหวของ Public Cloud ที่ท่านใช้บริการ ในด้านการรักษาความปลอดภัยของข้อมูลเสมอ	0.809
ท่านจะศึกษานโยบายการรักษาความเป็นส่วนตัวของผู้ให้บริการ อย่างระมัดระวัง ก่อนนำข้อมูลส่วนตัวขึ้นสู่ระบบ Public Cloud	0.875
ท่านจะศึกษาการตั้งค่าการเข้าถึงข้อมูลภายใน Public Cloud ก่อนใช้งาน และเปิดเผยข้อมูลส่วนตัวให้น้อยที่สุด	0.722

ตารางที่ 1 ปัจจัยที่ได้จากการวิเคราะห์องค์ประกอบ (ต่อ)

ปัจจัย	Factor Loading
ปัจจัย 8: แรงจูงในในการหลีกเลี่ยง (73.399% of variance, α = 0.814)	
ท่านเข้าใจถึงภัยคุกคามข้อมูลส่วนตัวที่มีมากขึ้น จึงตั้งใจที่จะใช้โปรแกรมป้องกันสปายแวร์ในการป้องกันภัยคุกคาม	0.805
ท่านเข้าใจถึงภัยคุกคามข้อมูลส่วนตัวที่มีมากขึ้น จึงต้องการให้มีการปรับปรุงโปรแกรมป้องกันสปายแวร์อยู่เสมอ	0.909
ท่านเข้าใจถึงภัยคุกคามข้อมูลส่วนตัวที่มีมากขึ้น จึงต้องการใช้บริการ Public Cloud ที่มีโปรแกรมป้องกันสปายแวร์มาตรฐานสูง	0.853
ปัจจัย 9: ความตระหนักในการหลีกเลี่ยง (79.210% of variance, α = 0.869)	
ท่านเข้าใจถึงการปฏิบัติตามระเบียบการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศภายใน Public Cloud	0.897
ท่านเข้าใจถึงอุปสรรคในการปฏิบัติตามระเบียบการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศภายใน Public Cloud	0. 925
ท่านเข้าใจถึงปัจจัยในการเสริมสร้างความปลอดภัยภายใน Public Cloud เพื่อป้องกันภัยจากผู้ที่อาจมาคุกคามข้อมูล	0.847
ปัจจัย 10: พฤติกรรมการหลีกเลี่ยงภัยคุกคาม (62.976% of variance, α = 0.833)	
ถ้าหากท่านใช้งานโปรแกรมแอนตีไวรัส จะใช้เพื่อป้องกันสปายแวร์ที่อาจมาจาก Public Cloud	0.885
ท่านจะปรับปรุงข้อมูลในโปรแกรมแอนตีไวรัส เพื่อป้องกันการถูกขโมยข้อมูลในการ Login เข้าสู่ระบบ Public Cloud	0.891

อนึ่งผลของการวิเคราะห์ข้อมูลทั่วไปเกี่ยวกับผู้ตอบแบบสอบถามของของกลุ่มตัวอย่างพบว่ากลุ่มตัวอย่างส่วนใหญ่ที่ตอบแบบสอบถามเป็นกลุ่มช่วงอายุ 26-30 ปี และส่วนใหญ่มีอาชีพพนักงานบริษัท/ลูกจ้างเอกชน ถึงร้อยละ 45.9 ซึ่งเป็นกลุ่มที่สนใจในเรื่อง Public Cloud มากที่สุด

5.2 การวิเคราะห์ผลการวิจัย

การทดสอบสมมติฐานการวิจัยในครั้งนี้ ผู้วิจัยใช้วิธีวิเคราะห์การถดถอยเชิงเส้นเดียว และการวิเคราะห์ถดถอยพหุคูณ โดยใช้ค่า p-value ที่น้อยกว่าหรือเท่ากับ 0.05 เป็นตัวกำหนดนัยสำคัญทางสถิติโดยแบ่งการวิเคราะห์ออกเป็น 4 ส่วน ดังนี้

ส่วนที่ 1 ผลการวิเคราะห์สมการถดถอยพหุคูณแสดงให้เห็นว่าการรับรู้ความรุนแรงของภัยคุกคาม และการรับรู้ถึงจุดอ่อนกำหนดการรับรู้ถึงภัยคุกคาม ที่ระดับนัยสำคัญ $F(2, 287) = 53.787$ ($p = 0.000$) ซึ่งสามารถอธิบายความผันแปรของตัวแปรตามได้ร้อยละ 27.3% ($R^2 = 0.273$) เมื่อวิเคราะห์ในรายละเอียดของตัวแปรอิสระพบว่าการรับรู้ความรุนแรงของภัยคุกคาม และการรับรู้ถึงจุดอ่อน เป็นตัวกำหนดการรับรู้ถึงภัยคุกคามที่ระดับนัยสำคัญที่ $p = 0.005$ และ 0.007 (ดังแสดงในตารางที่ 2-3) ซึ่งสอดคล้องกับงานวิจัยของ Liang and Xue (2009) ที่กล่าวว่าการที่บุคคลรับรู้ถึงช่องโหว่หรือจุดอ่อนแอที่เกิดขึ้น ทำให้บุคคลรับรู้ถึงภัยที่จะมาคุกคามข้อมูลส่วนตัวของตนเองและ การที่บุคคลรับรู้ถึงผลลัพธ์ด้านลบจากภัยคุกคามจะมีสาเหตุมาจากระดับของภัยคุกคามทางสารสนเทศที่มีความรุนแรงต่อข้อมูลส่วนตัว

ตารางที่ 2 ผลการวิเคราะห์การถดถอย (Regression) ของการรับรู้ความรุนแรงของภัยคุกคาม และการรับรู้ถึงจุดอ่อนที่มีอยู่ใน Public Cloud ต่อการรับรู้ถึงภัยคุกคาม

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	54.205	2	27.102	53.787	.000**
Residual	144.615	287	0.504		
Total	198.820	289			

** p<0.05

ตารางที่ 3 ผลการวิเคราะห์การถดถอยแบบปกติ (Coefficients) ของการรับรู้ความรุนแรงของภัยคุกคาม และการรับรู้ถึงจุดอ่อนที่มีอยู่ใน Public Cloud ต่อการรับรู้ถึงภัยคุกคาม

Model	Unstandardized Coefficients	Standardized Coefficients	t	Sig.
	B	Beta		
การรับรู้ถึงจุดอ่อนที่มีอยู่ใน Public Cloud (Weak)	0.155	0.172	2.821	0.005**
การรับรู้ความรุนแรงของภัยคุกคาม (Per_serv)	0.305	0.405	6.630	0.000**

** p<0.05

$R = 0.522$, $R^2 = 0.273$, SE = 0.70985

ส่วนที่ 2 ผลการวิเคราะห์สมการถดถอยพหุคูณแสดงให้เห็นว่าการรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัว การรับรู้ค่าใช้จ่ายจากการใช้เครื่องมือป้องกันภัยคุกคามและการรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัวกำหนดการรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคาม ที่ระดับนัยสำคัญ $F(3, 286) = 39.563$ ($p = 0.000$) ซึ่งสามารถอธิบายความผันแปรของตัวแปรตามได้ร้อยละ 29.3 % ($R^2 = 0.293$) เมื่อวิเคราะห์ในรายละเอียดของตัวแปรอิสระพบว่าการรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัว การรับรู้ค่าใช้จ่ายจากการใช้เครื่องมือป้องกันภัยคุกคามและการรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัว เป็นตัวกำหนดการรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคามที่ระดับนัยสำคัญที่ $p = 0.000$ (ดังแสดงในตารางที่ 4-5) ซึ่งสอดคล้องกับงานวิจัยของ Bandura (1982) ที่กล่าวว่า การที่บุคคลรับรู้ความสามารถในการหลีกเลี่ยงนั้นจะเป็นผลมาจากการที่บุคคลรู้ถึงประสิทธิภาพในการหลีกเลี่ยงภัยคุกคามของเครื่องมือที่ใช้ในการปกป้องข้อมูลทางสารสนเทศ Weinstein (1993) ที่กล่าวว่า การที่บุคคลจะเลือกใช้เครื่องมือป้องกันภัยคุกคามชนิดใดนั้น เขาจะไม่ได้ตัดสินเลือกจากแค่ความสามารถในการหลีกเลี่ยงเท่านั้น แต่ยังรวมถึงค่าใช้จ่ายที่ต้องใช้และ Ng et al. (2009); Woon et al. (2005) และ Workman et al. (2008) ที่กล่าวว่า บุคคลจะแสดงความสามารถหลีกเลี่ยงภัยคุกคาม เมื่อระดับของประสิทธิภาพการหลีกเลี่ยงของตนเองเพิ่มขึ้น

ตารางที่ 4 ผลการวิเคราะห์การถดถอย (Regression) ของการรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัว การรับรู้ค่าใช้จ่ายจากการใช้เครื่องมือป้องกันภัยคุกคาม และการรับรู้ความสามารถของตนเองในการรับมือภัยคุกคามต่อการรับรู้ความสามารถในการหลีกเลี่ยง

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	63.131	3	21.044	39.563	0.000**
Residual	152.126	286	0.532		
Total	215.257	289			

** p<0.05

ตารางที่ 5 ผลการวิเคราะห์การถดถอยแบบปกติ (Coefficients) ของการรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัว การรับรู้ค่าใช้จ่ายจากการใช้เครื่องมือป้องกันภัยคุกคาม และการรับรู้ความสามารถของตนเองในการรับมือภัยคุกคามต่อการรับรู้ความสามารถในการหลีกเลี่ยง

Model	Unstandardized Coefficients	Standardized Coefficients	t	Sig.
	B	Beta		
การรับรู้ค่าใช้จ่ายจากการใช้เครื่องมือป้องกันภัยคุกคาม (Per_cos)	0.292	0.274	5.325	0.000**
การรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัว (Per_eff)	0.254	0.202	3.978	0.000**
การรับรู้ความสามารถของตนเองในการรับมือภัยคุกคาม (Self)	0.258	0.313	6.022	0.000**

** P < 0.05

R = 0.542, R^2 = 0.293, SE = 0.72932

ส่วนที่ 3 ผลการวิเคราะห์สมการถดถอยพหุคูณแสดงให้เห็นว่าการรับรู้ถึงภัยคุกคามต่อข้อมูลส่วนตัวและการรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคามกำหนดแรงจูงใจในการหลีกเลี่ยงภัยคุกคาม ที่ระดับนัยสำคัญ F(2, 287) = 80.052 (p = 0.000) ซึ่งสามารถอธิบายความผันแปรของตัวแปรตามได้ร้อยละ 35.8 % (R^2 = 0.358) เมื่อวิเคราะห์ในรายละเอียดของตัวแปรอิสระพบว่าการรับรู้ถึงภัยคุกคามต่อข้อมูลส่วนตัวและการรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคาม เป็นตัวกำหนดแรงจูงใจในการหลีกเลี่ยงภัยคุกคามที่ระดับนัยสำคัญที่ p = 0.000 ทุกปัจจัย (ดังแสดงในตารางที่ 6-7) ซึ่งสอดคล้องกับงานวิจัยของ (Freud, 1915; James, 1890) ที่ศึกษาในกฎแห่งความชอบว่า บุคคลมีแนวโน้มที่จะหลีกเลี่ยงภัย

ที่อาจมาคุกคามตนเอง หากภัยนั้นทำให้ตนเองเกิดความเสียหายและ Liang and Xue (2010) ที่ศึกษาพบว่า บุคคลจะมีความตั้งใจที่จะนำเครื่องมือป้องกันภัยคุกคามมาใช้ ก็ต่อเมื่อบุคคลนั้นรับรู้ว่าเครื่องมือป้องกันภัยคุกคามสามารถที่จะรับมือกับภัยนั้นได้

ตารางที่ 6 ผลการวิเคราะห์การถดถอย (Regression) ของการรับรู้ถึงภัยคุกคามต่อข้อมูลส่วนตัวภายใน Public Cloud และการรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคาม ต่อแรงจูงใจในการหลีกเลี่ยง

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	74.899	2	37.450	80.052	0.000**
Residual	134.264	287	0.468		
Total	209.163	289			

** p<0.05

ตารางที่ 7 ผลการวิเคราะห์การถดถอยแบบปกติ (Coefficients) ของการรับรู้ถึงภัยคุกคามต่อข้อมูลส่วนตัวภายใน Public Cloud และการรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคาม ต่อแรงจูงใจในการหลีกเลี่ยง

Model	Unstandardized Coefficients	Standardized Coefficients	t	Sig.
	B	Beta		
การรับรู้ถึงภัยคุกคามต่อข้อมูลส่วนตัวภายใน Public Cloud (Per_thr)	0.263	0.257	5.361	0.000**
การรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคามต่อข้อมูลที่เป็นส่วนตัว (Avoi)	0.496	0.503	10.507	0.000**

** P < 0.05

R = 0.598, R2 = 0.358, SE = 0.68397

ส่วนที่ 4 ผลการวิเคราะห์สมการถดถอยพหุคูณแสดงให้เห็นว่าแรงจูงใจในการหลีกเลี่ยงภัยคุกคามและความตระหนักในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวกำหนดพฤติกรรมการหลีกเลี่ยงภัยคุกคาม ที่ระดับนัยสำคัญ F(2, 287) = 71.458 (p = 0.000) ซึ่งสามารถอธิบายความผันแปรของตัวแปรตามได้ร้อยละ 33.2 % (R^2 = 0.332) เมื่อวิเคราะห์ในรายละเอียดของตัวแปรอิสระพบว่าแรงจูงใจในการหลีกเลี่ยงภัยคุกคามและความตระหนักในการหลีกเลี่ยงภัยคุกคาม เป็นตัวกำหนดพฤติกรรมการหลีกเลี่ยงภัยคุกคาม ที่ระดับนัยสำคัญที่ p = 0.034 และ 0.000 (ดังแสดงในตารางที่ 8-9) ซึ่งสอดคล้องกับงานวิจัยของ ของ Liang and Xue (2010) ที่กล่าวว่า บุคคลที่มีแรงจูงใจในการหลีกเลี่ยงสูงจะมีแนวโน้มที่จะมีพฤติกรรม

หลีกเลี่ยงภัยคุกคามโดยใช้เครื่องมือป้องกันภัยคุกคาม เพื่อลดความเสี่ยงที่จะเกิดขึ้นและ ประภาดา ตลึงจิตร (2553) ที่กล่าวว่าพฤติกรรมทางการหลีกเลี่ยงภัยคุกคามยังถือว่าเป็นการแสดงให้เห็นว่าบุคคลนั้นมีความตระหนักถึงความปลอดภัย

ตารางที่ 8 ผลการวิเคราะห์การถดถอย (Regression) ของแรงจูงใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว และความตระหนักในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว ต่อพฤติกรรมการหลีกเลี่ยง

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	80.408	2	40.204	71.458	0.000**
Residual	161.472	287	0.563		
Total	241.879	289			

** p<0.05

ตารางที่ 9 ผลการวิเคราะห์การถดถอยแบบปกติ (Coefficients) ของแรงจูงใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว และความตระหนักในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว ต่อพฤติกรรมการหลีกเลี่ยง

Model	Unstandardized Coefficients	Standardized Coefficients	t	Sig.
	B	Beta		
ความตระหนักในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว (Awar)	0.122	0.114	2.127	0.034
แรงจูงใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว (Motiv)	0.558	0.519	9.718	0.000

** P < 0.05

R = 0.577, R2 = 0.332, SE = 0.75008

6. สรุปผลการวิจัย

ผลการวิจัยพบว่า ตัวแปรที่มีอิทธิพลต่อการรับรู้ถึงภัยคุกคามต่อข้อมูลส่วนตัวภายใน Public Cloud มากที่สุด คือ ตัวแปรการรับรู้ความรุนแรงของภัยคุกคาม รองลงมาคือ ตัวแปรการรับรู้ถึงจุดอ่อนที่มีอยู่ใน Public Cloud ส่วนตัวแปรที่มีอิทธิพลต่อการรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคามต่อข้อมูลที่เป็นส่วนตัวภายใน Public Cloud พบว่า ตัวแปรการรับรู้ค่าใช้จ่ายจากการใช้เครื่องมือป้องกันภัยคุกคามเป็นตัวแปรอิสระที่มีความสัมพันธ์เชิงบวกมากที่สุด รองลงมา คือ ตัวแปรการรับรู้ความสามารถของตนเองในการรับมือภัยคุกคาม และการรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัวเป็นตัวแปรอิสระที่มีความสัมพันธ์น้อยที่สุด ส่วนตัวแปรที่มีอิทธิพลต่อแรงจูงใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวภายใน Public Cloud มากที่สุด คือ ตัวแปรการรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคามต่อข้อมูลที่เป็นส่วนตัวภายใน Public Cloud ส่งผลเชิงบวกและมีอิทธิพลมากกว่าตัวแปรการรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคามต่อข้อมูลที่เป็นส่วนตัวภายใน Public Cloud ส่วนส่วนตัวแปรที่มีอิทธิพลต่อพฤติกรรมการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวภายใน Public Cloud

มากที่สุด คือ ตัวแปรแรงจูงใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวภายใน Public Cloud ในขณะที่ตัวแปรความตระหนักในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวนั้นเป็นตัวแปรที่รองลงมา

โดยกลุ่มตัวอย่างของงานวิจัยนี้ ได้แก่ กลุ่มตัวอย่างที่ที่ใช้ในการวิจัยนี้ คือ ผู้ใช้บริการ Public Cloud อันได้แก่ Google Drive, Dropbox เนื่องจากไม่ทราบจำนวนประชากรทั้งหมดว่ามีจำนวนเท่าไหร่ ในการวิจัยครั้งนี้ จึงใช้วิธีการกำหนดขนาดตัวอย่างจากการประมาณค่าเฉลี่ยประชากร และสร้างแบบสอบถามออนไลน์ในการเก็บข้อมูลเพื่ออำนวยความสะดวกแก่ผู้ตอบแบบสอบถาม โดยการวาง URL ของแบบสอบถามไว้บนเครือข่ายสังคม (Facebook) สารสนเทศของผู้วิจัยกระจายไปยังกลุ่มตัวอย่าง, เวบไซต์ด้านเทคโนโลยี ซึ่งมีผู้ตอบแบบสอบทั้งสิ้นจำนวน 302 ชุด และได้ตัดข้อมูลที่ไม่ใช่กลุ่มตัวอย่างที่แท้จริงออก เหลือแบบสอบถามทั้งสิ้น 290 ชุด จึงนำข้อมูลดังกล่าวมาวิเคราะห์ทางสถิติ

กลุ่มประชากรที่ตอบแบบสอบถามส่วนใหญ่อยู่ในช่วงอายุ 26-30 ปี และส่วนใหญ่ผู้ตอบแบบสอบถามเป็นพนักงานบริษัท/ลูกจ้างเอกชน หากเป็นช่วงอายุอื่นหรือประกอบอาชีพอื่น อาจได้ผลลัพธ์ที่แตกต่างกัน เนื่องจากผู้ใช้งานมีกระจายกลุ่มมากขึ้น แนวทางในการใช้งานก็จะต่างกันไปด้วย

งานวิจัยนี้ผู้วิจัยได้ศึกษาเฉพาะผู้ที่เคยใช้งานหรือใช้งาน Public Cloud อยู่เท่านั้น ไม่รวมถึง Cloud ประเภทอื่นๆ ซึ่งวิจัยต่อเนื่องอาจจะศึกษาปัจจัยอื่นๆที่อาจส่งผลกระทบต่อพฤติกรรมการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวมากกว่านี้ เนื่องจากในผลการวิจัยค่าสถิติของตัวแปรส่วนใหญ่จะอยู่ในช่วง 0.2 ซึ่งถือว่ายังไม่สูงมากนัก อาจมีตัวแปรอื่นๆที่ส่งผลกระทบได้อีก

บรรณานุกรม

กิ่งแก้ว ศรีสาลีกุลรัตน์. (2551). ประสิทธิผล (Effectiveness). ดึงข้อมูลวันที่ 21 มีนาคม 2558, จาก https://www.gotoknow.org/posts/213948.

กองบัญชาการการศึกษา สำนักงานตำรวจแห่งชาติ. (2548). จิตวิทยาเบื้องต้น. ดึงข้อมูลวันที่ 18 เมษายน 2558, จาก http://www.edupol.org/edu_P/systemedu/cschool/data/9.pdf.

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล. (2558). ความหมายของการบริหารความเสี่ยง. ดึงข้อมูลวันที่ 20 มีนาคม 2558, จากhttp://www.eg.mahidol.ac.th/qa/index.php?option=com_content&view=article&id=82&Itemid=113.

ธีรศักดิ์ แสงดิษฐ์ (2553) แรงจูงใจของชุมชนกับการระดมทรัพยากรเพื่อการศึกษาของโรงเรียนสังกัดสำนักงานเขตพื้นที่การศึกษาราชบุรีเขต 1, วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยศิลปากร, คณะศึกษาศาสตร์.

ประภาดา ตลึงจิตร (2555) แนวทางในการเสริมสร้างความตระหนักถึงการปฏิบัติตามระเบียบการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ไทย : Case study research of Thai Cooperative, วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์, คณะพาณิชยศาสตร์และการบัญชี.

วิมลรัศมิ์ พันธุ์จิรภาค (2554) ผลของโปรแกรมออกกำลังกายเพื่อส่งเสริมสุขภาพของผู้สูงอายุหญิง จังหวัดสมุทรปราการ, วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยบูรพา, คณะสาธารณสุขศาสตร์.

Al-Haderi, S.M. (2013). The Effect of Self-Efficacy in the Acceptance of Information Technology in the Public Sector. *International Journal of Business and Social Science*, 4(9), 188-198.

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

Choi, C. F., and Jiang, Z. (2013). Responses to Social Predicament on Online Social Networks. Proceedings of the Nineteenth Americas Conference on Information Systems.

Dinev, T., and Hart, P. (2004). Internet Privacy, Social Awareness, And Internet Technical Literacy. An Exploratory Investigation BLED 2004 Proceedings, Paper 24.

Hardin, A., Looney, C., and Fuller, M. (2006). Computer based learning systems and the development of computer selfefficacy: Are all sources of efficacy created equal? AMCIS 2006 Proceedings, Paper 273.

He, J., and Freeman, L. A. (2010). Understanding the Formation of General Computer Self-Efficacy. *Communications of the Association for Information Systems*, 26, Article 12.

Hwang, K., Kulkarni, S., and Hu, Y. (2009). Cloud Security with Virtualized Defense and Reputation-based Trust Management. 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 717-722.

Johnston, A. C., and Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, 34(3), 549-566.

Lankton, N., and Tripp, J. (2013). A Quantitative and Qualitative Study of Facebook Privacy using the Antecedent-Privacy Concern-Outcome Macro. Proceedings of the Nineteenth Americas Conference on Information Systems.

Leberknight, C. S., Widmeyer, G. R., and Recce, M. L. (2008). Decision Support for Perceived Threat in the Context of Intrustion Detection Systems. AMCIS 2008 Proceedings, Paper 317.

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

Liang, H., and 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.