การจัดการความเสี่ยงระบบสารสนเทศด้วยแนวทางการจัดการเชิงรุกและเชิงรับ : กรณีศึกษาองค์การขนาดกลางและขนาดย่อมในเขตกรุงเทพมหานคร

Security risk management of information systems with proactive and reactive approaches : a case study of small- and medium-sized enterprise organizations in Bangkok metropolis

กัลยา สิรินาคบำรุง

สาขาวิชาการจัดการ คณะบริหารธุรกิจ มหาวิทยาลัยรามคำแหง
Email : kallaya_ss@hotmail.com

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อ 1) เพื่อศึกษาความสัมพันธ์ระหว่างรูปแบบการจัดการความปลอดภัยเชิงรุกและเชิงรับกับความสำเร็จในการรักษาความปลอดภัยขององค์การขนาดกลางและขนาดย่อม 2) เพื่อเปรียบเทียบความสำเร็จในการรักษาความปลอดภัย กับรูปแบบการจัดการความปลอดภัยเชิงรุกและเชิงรับขององค์การขนาดกลางและขนาดย่อม และ 3) เพื่อเป็นแนวทางในการจัดการความปลอดภัยขององค์การขนาดกลางและขนาดย่อม กลุ่มตัวอย่างเป็นองค์การขนาดกลางและขนาดย่อมในเขตกรุงเทพมหานคร จำนวน 221 ราย โดยใช้แบบสอบถามในการเก็บข้อมูล สถิติที่ใช้ในการวิเคราะห์ข้อมูล ได้แก่ ความถี่ ค่าร้อยละ ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน การทดสอบค่า One-Way ANOVA ค่า Chi-square และ ค่า Cramer's V ผลการวิจัยพบว่า 1) ขนาดองค์การที่แตกต่างกันมีรูปแบบการจัดการความปลอดภัยเชิงรุกและเชิงรับแตกต่างกัน อย่างมีนัยสำคัญทางสถิติ .05 2) งบประมาณด้านความปลอดภัยที่แตกต่างกันมีรูปแบบการจัดการความปลอดภัยเชิงรุกและเชิงรับแตกต่างกัน อย่างมีนัยสำคัญทางสถิติ .05 3) ความรู้ด้านความปลอดภัยของพนักงานในแผนกเทคโนโลยีสารสนเทศ (IT) ที่แตกต่างกัน มีรูปแบบการจัดการความปลอดภัยเชิงรุกและเชิงรับแตกต่างกัน อย่างมีนัยสำคัญทางสถิติ .05 4) ความรู้ด้านความปลอดภัยของผู้บริหาร/เจ้าของกิจการที่แตกต่างกัน มีรูปแบบการจัดการความปลอดภัยเชิงรุกและเชิงรับแตกต่างกัน อย่างมีนัยสำคัญทางสถิติ .05 5) รูปแบบการจัดการความปลอดภัยเชิงรุกมีผลต่อการเพิ่มขึ้นของความสำเร็จในการรักษาความปลอดภัยมากกว่าเชิงรับในระดับปานกลางทั้งรายรวมและรายด้าน ได้แก่ ความลับ ความคงสภาพ และความพร้อมใช้งาน อย่างมีนัยสำคัญทางสถิติ .05 6) รูปแบบการจัดการความปลอดภัยเชิงรุก มีความสำเร็จในการรักษาความปลอดภัยมากกว่าเชิงรับ อย่างมีนัยสำคัญทางสถิติ .05

คำสำคัญ : ความปลอดภัยระบบสารสนเทศ / เชิงรุกและเชิงรับ / องค์การขนาดกลางและขนาดย่อม / SME

Abstract

The objectives of this study were 1) to study the relationship between proactive and reactive security management approaches and the success of information system security in the small- and, medium-sized enterprise organizations; 2) to compare the success of Information systems security to the proactive and reactive security management approaches of the small- and, medium-sized enterprise organizations; and (3) to provide a guidance in the security management approaches for the small- and, medium-sized enterprise organizations. The research sample consisted of 221 small- and medium-sized enterprise organizations in Bangkok metropolis. The survey questionnaire

was used to collect data and then the data is analyzed using descriptive statistics including frequency, percentage, mean and standard deviation. One-Way ANOVA, Chi-square and Cramer's V were also used to test these research hypotheses. The findings are as follows:1) Organizations with the differences in the total of employees exhibited a difference in their choice for either a proactive or a reactive security management approach at the statistically significant level of .05. 2) Organizations with the differences in the information security budget exhibited a difference their choice for either a proactive or a reactive security management approaches at the statistically significant level of .05. 3) IT employees with different levels in the security knowledge exhibited their choice for either a proactive or a reactive security management approaches at the statistically significant level of .05. 4) Executives/owners with different levels in the security knowledge exhibited their choice for either a proactive or a reactive security management approaches at the statistically significant level of .05. 5) The proactive approach of the security managements had a greater effect on increasing security success than the reactive approach had with a moderation level in both all perspective and each aspect of confidentiality, integrity and availability, at the statistically significant level of .05. 6) The proactive approach of the security managements had a better success in security than the reactive approach at the statistically significant level of .05.

Keywords : Information security / proactive and reactive / small to medium enterprises / SME

1. บทนำ

องค์การขนาดกลางและขนาดย่อมส่วนใหญ่ขาดการบริหารจัดการด้านความมั่นคงปลอดภัยระบบสารสนเทศที่มีประสิทธิภาพ เนื่องจากมีความเชื่อผิด ๆ ว่าการสำรองข้อมูลเพียงอย่างเดียว จะสามารถป้องกันความเสี่ยงส่วนใหญ่ได้ และเพียงพอที่จะตอบสนองเมื่อเกิดปัญหาขึ้น [1] ผู้นำองค์การยังขาดความตื่นตัวในเรื่องความเสี่ยงที่เพิ่มสูงขึ้น ไม่มีการกำหนดกลยุทธ์และจัดสรรงบประมาณที่เหมาะสม ขาดการให้ความรู้แก่พนักงานอย่างทั่วถึง ไม่มีการร่วมมือประสานงานภายใน [2, 3] องค์การจะให้ความสำคัญเมื่อเกิดข้อผิดพลาดขึ้นในระบบสารสนเทศแล้ว โดยมองว่าการบริหารจัดการในเรื่องความมั่นคงปลอดภัยนั้น เป็นการลงทุนเพื่อแก้ปัญหาที่เกิดขึ้น การป้องกันความเสี่ยงต่าง ๆ ที่ยังไม่เกิดขึ้นนั้น ทำให้องค์การมีค่าใช้จ่ายที่สูงและไม่คุ้มค่า [4] ทั้งที่ความเป็นจริงนั้นเมื่อระบบสารสนเทศขององค์การถูกโจมตี ความเสียหายจากการโจมตี โอกาสทางธุรกิจและผลประโยชน์ที่สูญเสียไป มีมูลค่ามากกว่าจำนวนเงินที่ถูกใช้ไปในการลงทุนด้านการรักษาความมั่นคงปลอดภัยเพื่อป้องกันไม่ให้เกิดเหตุการณ์ที่เป็นอันตรายต่าง ๆ ขึ้น [3, 5]

การบริหารจัดการด้านความมั่นคงปลอดภัยระบบสารสนเทศขึ้นอยู่กับ ขนาดองค์การ งบประมาณด้านความมั่นคงปลอดภัย ความรู้ด้านความมั่นคงปลอดภัยของพนักงานในแผนกเทคโนโลยีสารสนเทศ (IT) ความรู้ด้านความมั่นคงปลอดภัยของผู้บริหาร/เจ้าของกิจการ [2, 3, 6, 7] รวมถึงการเรียนรู้ภายในขององค์การ ในด้านการจัดสรรทรัพยากรเพื่อการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ เมื่อเทียบกับมูลค่าความเสียหายจากปัญหาที่เกิดขึ้นต่อระบบสารสนเทศ ในด้านผลกระทบที่เกิดขึ้นจากการลงทุนก่อนหรือหลังการเกิดปัญหาขึ้น [4] จากเหตุผลดังกล่าว ผู้วิจัยจึงศึกษาความสัมพันธ์ระหว่าง รูปแบบของการจัดการความมั่นคงปลอดภัยเชิงรุกและเชิงรับกับความสำเร็จในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศขององค์การขนาดกลางและขนาดย่อมซึ่งดำเนินธุรกิจในเขตกรุงเทพมหานคร เพื่อให้ทราบว่าองค์การขนาดกลางและขนาดย่อมในประเทศไทยมีรูปแบบของการจัดการแบบใด และมีความสำเร็จในการรักษาความมั่นคงปลอดภัยเพียงใด โดยการจัดการความเสี่ยงระบบสารสนเทศ คือ การดำเนินการต่าง ๆ เพื่อลดโอกาสที่จะเกิดความเสียหายแก่ระบบสารสนเทศ ซึ่งคลอบคลุมถึง สารสนเทศ กระบวนการและบริการ ซอฟต์แวร์ ฮาร์ดแวร์ บุคลากร โดยมุ่งเน้นตามมาตรฐาน ISO/IEC 27001 [8] เช่น การกำหนดสิทธิ์การเข้าถึงสินทรัพย์ สารสนเทศ และเครือข่ายสารสนเทศขององค์การ บทบาทและความ

รับผิดชอบของบุคลากร รวมถึงการจัดการกับเหตุการณ์ที่เกิดขึ้นเพื่อความต่อเนื่องในการดำเนินธุรกิจ ซึ่งผลการวิจัยจะเป็นข้อมูลเบื้องต้น สำหรับการพิจารณากำหนดนโยบายด้านความมั่นคงปลอดภัยขององค์การต่าง ๆ ต่อไป

2. วัตถุประสงค์ของการวิจัย

2.1 เพื่อศึกษาความสัมพันธ์ระหว่างรูปแบบการจัดการความมั่นคงปลอดภัยเชิงรุกและเชิงรับ กับความสำเร็จในการรักษาความปลอดภัยขององค์การขนาดกลางและขนาดย่อม

2.2 เพื่อเปรียบเทียบความสำเร็จในการรักษาความปลอดภัยกับรูปแบบการจัดการความมั่นคงปลอดภัยเชิงรุกและเชิงรับ ขององค์การขนาดกลางและขนาดย่อม

2.3 เพื่อเป็นแนวทางในการจัดการความมั่นคงปลอดภัยขององค์การขนาดกลางและขนาดย่อม

3. วิธีดำเนินการวิจัย

3.1 ประชากรและกลุ่มตัวอย่าง

ประชากรคือ องค์การขนาดกลางและขนาดย่อม ซึ่งดำเนินธุรกิจในเขตกรุงเทพมหานคร โดยองค์การขนาดกลางมีจำนวนพนักงาน ตั้งแต่ 20-99 คน และองค์การขนาดย่อมมีจำนวนพนักงานน้อยกว่า 20 คน กำหนดกลุ่มตัวอย่างโดยใช้สูตรการคำนวณของคอแครน (Cochran) ในกรณีที่ไม่ทราบจำนวนที่แน่นอน ใช้วิธีการสุ่มตัวอย่างแบบแบ่งชั้นภูมิ โดยแบ่งประชากรออกตามขนาดขององค์การ กำหนดสัดส่วนของผู้ตอบแบบสอบถาม โดยองค์การขนาดกลางประมาณ 50% และขนาดย่อมประมาณ 50% ของจำนวนแบบสอบถามทั้งหมด จากนั้นจึงใช้วิธีการสุ่มตัวอย่างแบบง่ายจากสมาชิกแต่ละกลุ่มจนครบตามจำนวนที่ต้องการ

3.2 เครื่องมือที่ใช้ในการวิจัย

ตอนที่ 1 แบบสอบถามเกี่ยวกับข้อมูลทั่วไปเกี่ยวกับองค์การ ได้แก่ ขนาดองค์การ งบประมาณด้านความมั่นคงปลอดภัย ความรู้ด้านความมั่นคงปลอดภัยของพนักงานในแผนกเทคโนโลยีสารสนเทศ ความรู้ด้านความมั่นคงปลอดภัยของผู้บริหาร/เจ้าของกิจการ [2, 3, 6, 7] จำนวน 4 ข้อ โดยมีลักษณะแบบสอบถามปลายปิด ซึ่งมีลักษณะเป็นแบบหลายตัวเลือก

ตอนที่ 2 แบบสอบถามเกี่ยวกับระดับการปฏิบัติในการจัดการรักษาความมั่นคงปลอดภัยระบบสารสนเทศภายในองค์การ โดยสร้างคำถามขึ้นภายใต้กรอบมาตรฐานความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001 [8] โดยพิจารณาแต่ละคำถามให้สอดคล้องกับแนวทางการจัดการความมั่นคงปลอดภัยเชิงรุกและเชิงรับ [9, 10] โดยแบ่งคำถามเป็น 2 ส่วน คือ คำถามเชิงรุกและคำถามเชิงรับ ส่วนละ 12 ข้อ รวม 24 ข้อ

การจัดกลุ่มรูปแบบการจัดการความมั่นคงปลอดภัยใช้สูตรการคำนวณหาค่าพิสัยในการแปลความหมาย คือ 12-23 คะแนน คือ มีการปฏิบัติน้อย 24-36 คะแนน คือ มีการปฏิบัติมาก โดยสามารถจัดกลุ่มได้ 4 แบบ คือ

	ปฏิบัติเชิงรุก	ปฏิบัติเชิงรับ
แบบที่ 1	ปฏิบัติมาก	ปฏิบัติมาก
แบบที่ 2	ปฏิบัติมาก	ปฏิบัติน้อย
แบบที่ 3	ปฏิบัติน้อย	ปฏิบัติมาก
แบบที่ 4	ปฏิบัติน้อย	ปฏิบัติน้อย

ตอนที่ 3 แบบสอบถามเกี่ยวกับระดับความสำเร็จในการรักษาความมั่นคงปลอดภัย เป็นคำถามเกี่ยวกับปัญหาด้านความมั่นคงปลอดภัยของระบบสารสนเทศที่องค์การประสบ เมื่อเปรียบเทียบกับปีที่ผ่านมา โดยสร้างคำถามจากรายงานภัยคุกคามความปลอดภัยทางอินเทอร์เน็ตที่พบมากในปี 2558 [11] โดยแบ่งปัญหาออกเป็น 3 ด้าน คือ ด้านความลับ ความคงสภาพ และความพร้อมใช้งาน [9] ด้านละ 5 ข้อ รวมเป็น 15 ข้อ การแปลความหมายและให้คะแนน ดังนี้

ค่าเฉลี่ย	หมายถึง
1.00 - 1.66	มีปัญหามากกว่าปีที่ผ่านมา
1.67 - 2.32	มีปัญหาไม่แตกต่างจากปีที่ผ่านมา
2.33 - 3.00	มีปัญหาน้อยกว่าปีที่ผ่านมา

ใช้แบบสอบถามในการรวบรวมข้อมูลจากบุคลากรในองค์การที่มีส่วนรับผิดชอบดูแลระบบสารสนเทศ เช่น พนักงาน IT , เจ้าหน้าที่เน็ตเวิร์ค , ผู้ดูแลระบบ หรือผู้มีส่วนเกี่ยวข้องกับการกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ อาทิการกำหนดสิทธิ์การเข้าถึงสินทรัพย์ ข้อมูลและเครือข่ายสารสนเทศขององค์การ บทบาทและความรับผิดชอบของบุคลากร รวมถึงการจัดการกับเหตุการณ์ที่เกิดขึ้นเพื่อความต่อเนื่องในการดำเนินธุรกิจ เช่น ผู้บริหาร/เจ้าของกิจการที่มีความรู้ด้าน IT , หัวหน้าฝ่าย IT เป็นต้น โดยทำการ

ทดสอบความเชื่อมั่นของแบบสอบถามจำนวน 30 ชุด เก็บข้อมูลเดือนธันวาคม 2558 ได้ค่า Cronbach's Alpha คือ 0.963

3.3 การเก็บรวบรวมข้อมูล

ดำเนินการเก็บข้อมูล ในช่วงเดือนมกราคม - มีนาคม 2559 โดยแจกแบบสอบถามให้แก่กลุ่มตัวอย่างทางจดหมายอิเล็กทรอนิกส์ (e-mail) จำนวน 600 ฉบับ โดยสุ่มเลือกกลุ่มตัวอย่างจากเว็บไซต์ที่มีการขึ้นทะเบียน และให้การสนับสนุนธุรกิจขนาดกลางและขนาดย่อม ได้แก่ เว็บไซต์ศูนย์บริการสารสนเทศทางเทคโนโลยี เว็บไซต์ไทยตำบลดอทคอม และเว็บไซต์สำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม ผู้วิจัยได้โทรศัพท์ขอความร่วมมือจากกลุ่มตัวอย่างในการตอบแบบสอบถามอย่างน้อยจำนวน 3 ครั้ง โดยเว้นระยะห่างประมาณ 1 สัปดาห์ ซึ่งพบปัญหาที่จากการเก็บข้อมูลคือ ผู้วิจัยไม่สามารถติดต่อบุคคลซึ่งเป็นกลุ่มตัวอย่างได้โดยตรง ทำได้เพียงส่งเรื่องผ่านฝ่ายประชาสัมพันธ์หรือหน่วยงานอื่น ๆ ขององค์การเพื่อส่งเรื่องต่อไปยังผู้เกี่ยวข้อง กลุ่มตัวอย่างปฏิเสธที่จะให้ข้อมูล องค์การไม่มีแผนก/ฝ่าย IT หรือบุคคลที่สามารถให้ข้อมูลได้ เป็นต้น ทำให้ได้รับข้อมูลจากการตอบแบบสอบถามจำนวน 221 ฉบับ

3.4 การวิเคราะห์ข้อมูล

ส่วนที่ 1 เป็นการวิเคราะห์ข้อมูลทั่วไปขององค์การโดยวิเคราะห์สถิติเชิงพรรณนา ส่วนที่ 2 วิเคราะห์สถิติเชิงอนุมาน โดยใช้สถิติ One-way ANOVA, Chi-square และสถิติ Cramer's V ในการทดสอบสมมติฐาน

4. สรุปผลการวิจัย

4.1 ข้อมูลทั่วไป

พบว่า กลุ่มตัวอย่างเป็นองค์การขนาดกลาง (ร้อยละ 52) และองค์การขนาดย่อม (ร้อยละ 48) ส่วนใหญ่มีงบประมาณด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศอยู่ในช่วง 1% - 4% (ร้อยละ 51.10) ผู้บริหาร/เจ้าของกิจการมีความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยระบบสารสนเทศในระดับน้อย (ร้อยละ 71.90) พนักงานในฝ่ายสารสนเทศมีความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยระบบสารสนเทศในระดับน้อย (ร้อยละ 47.50) และมีรูปแบบการจัดการความมั่นคงปลอดภัยแบบปฏิบัติน้อยทั้งเชิงรุก/รับ (ร้อยละ 66.50)

4.2 ข้อมูลด้านความสำเร็จในการรักษาความมั่นคงปลอดภัย

ความสำเร็จในการรักษาความมั่นคงปลอดภัยมีค่าเฉลี่ยรวมอยู่ในระดับที่ไม่แตกต่างจากปี 2558 (ปีที่ผ่านมา) ($\overline{X}$ =2.09) เมื่อแยกพิจารณารายด้านพบด้านที่มีค่าเฉลี่ยอยู่ในระดับที่ไม่แตกต่างจากปี 2558 (ปีที่ผ่านมา) คือ ด้านความลับ ($\overline{X}$ =2.21) รองลงมาคือ ด้านความคงสภาพ ($\overline{X}$ =2.12) และสุดท้ายคือ ด้านความพร้อมใช้งาน ($\overline{X}$ =1.94) เรียงตามลำดับ

4.3 ข้อมูลเพื่อทดสอบสมมติฐาน

สมมติฐานที่ 1 ใช้สถิติ Chi-square two-variable cases และ Cramer's ในการทดสอบสมมติฐาน พบว่า ขนาดองค์การที่แตกต่างกันมีรูปแบบการจัดการความมั่นคงปลอดภัยเชิงรุกและเชิงรับที่แตกต่างกัน ที่ระดับนัยสำคัญทางสถิติ .05 (Sig. = 0.000) มีขนาดแตกต่างกันในระดับสูง (Cramer's V = 0.564)

สมมติฐานที่ 2 ใช้สถิติ Chi-square two-variable cases และ Cramer's ในการทดสอบสมมติฐาน พบว่า งบประมาณด้านความมั่นคงปลอดภัยที่แตกต่างกัน มีรูปแบบการจัดการความมั่นคงปลอดภัยเชิงรุกและเชิงรับแตกต่างกัน ที่ระดับนัยสำคัญทางสถิติ .05 (Sig. = 0.000) มีขนาดความแตกต่างกันในระดับปานกลาง (Cramer's V = 0.410)

สมมติฐานที่ 3 ใช้สถิติ Chi-square two-variable cases และ Cramer's ในการทดสอบสมมติฐาน พบว่า ความรู้ด้านความมั่นคงปลอดภัยของพนักงานในแผนกเทคโนโลยีสารสนเทศ (IT) ที่แตกต่างกัน มีรูปแบบการจัดการความมั่นคงปลอดภัยเชิงรุกและเชิงรับแตกต่างกัน ที่ระดับนัยสำคัญทางสถิติ .05 (Sig. = 0.000) มีขนาดความแตกต่างกันในระดับปานกลาง (Cramer's V = 0.503)

สมมติฐานที่ 4 ใช้สถิติ Chi-square two-variable cases และ Cramer's ในการทดสอบสมมติฐาน พบว่า ความรู้ด้านความมั่นคงปลอดภัยของผู้บริหาร/เจ้าของกิจการที่แตกต่างกัน มีรูปแบบการจัดการความมั่นคงปลอดภัยเชิงรุกและเชิงรับแตกต่างกัน ที่ระดับนัยสำคัญทางสถิติ .05 (Sig. = 0.000) มีขนาดความแตกต่างกันในระดับปานกลาง (Cramer's V = 0. 527)

สมมติฐานที่ 5 ใช้สถิติ Chi-square และสถิติ Cramer's V ในการทดสอบสมมติฐาน พบว่า รูปแบบการจัดการความมั่นคงปลอดภัยเชิงรุกมีผลต่อการเพิ่มขึ้น

ของความสำเร็จในการรักษาความปลอดภัยมากกว่าเชิงรับรวมทุกด้าน ที่ระดับนัยสำคัญทางสถิติ .05 (Sig. = 0.000) มีขนาดความสัมพันธ์กันในระดับปานกลาง (Cramer's V = 0.377)

สมมติฐานที่ 6 ใช้สถิติ One-Way ANOVA ในการทดสอบสมมติฐาน พบว่า รูปแบบการจัดการความมั่นคงปลอดภัยเชิงรุก มีความสำเร็จในการรักษาความปลอดภัยมากกว่ารูปแบบการจัดการความมั่นคงปลอดภัยเชิงรับ ที่ระดับนัยสำคัญทางสถิติ .05 และทดสอบหาค่าเฉลี่ยเป็นรายคู่ เพื่อหาว่าคู่ใดบ้างที่แตกต่างกันโดยวิธี Scheffé พบว่า รูปแบบการจัดการความมั่นคงปลอดภัยแบบปฏิบัติมากทั้งเชิงรุก/รับ มีความสำเร็จในการรักษาความปลอดภัยรวมทุกด้านมากกว่ารูปแบบการจัดการความมั่นคงปลอดภัยแบบปฏิบัติน้อยทั้งเชิงรุก/รับ รูปแบบการจัดการความมั่นคงปลอดภัยแบบปฏิบัติเชิงรุกมากกว่าเชิงรับมีความสำเร็จในการรักษาความปลอดภัยมากกว่ารูปแบบการจัดการความมั่นคงปลอดภัยแบบปฏิบัติเชิงรับมากกว่าเชิงรุกและมากกว่าแบบปฏิบัติน้อยทั้งเชิงรุก/รับ

5. การอภิปรายผล

5.1 ข้อมูลทั่วไป

ผู้บริหาร/เจ้าของกิจการ และ พนักงานในฝ่ายสารสนเทศขององค์การขนาดกลางและขนาดย่อมในเขตกรุงเทพมหานคร ส่วนใหญ่มีความรู้ด้านความมั่นคงปลอดภัยระบบสารสนเทศอยู่ในระดับน้อย จากทั้งหมด 3 ระดับคือ น้อย ปานกลาง มาก แสดงให้เห็นว่าบุคลากรที่มีส่วนเกี่ยวข้องกับการกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศขององค์การ ยังขาดความรู้ความเข้าใจในเรื่องดังกล่าว ซึ่งสอดคล้องกับการตัดสินใจในการจัดสรรงบประมาณด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศขององค์การที่อยู่ในระดับน้อยที่สุด ที่ระดับ 1% - 4% จากทั้งหมด 4 ระดับ โดยระดับสูงสุดคือ มากกว่า 10% ซึ่งแสดงให้เห็นว่าองค์การไม่ค่อยให้ความสำคัญหรือให้ความสำคัญน้อยในเรื่องการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

ในด้านรูปแบบการจัดการความมั่นคงปลอดภัย พบว่าองค์การส่วนใหญ่มีการจัดการความปลอดภัยแบบปฏิบัติน้อยทั้งเชิงรุก/รับ ซึ่งแสดงให้เห็นว่า องค์การขาดความตระหนักถึงภัยคุกคาม ปัญหา และมูลค่าความเสียหายที่จะเกิดขึ้นหากระบบสารสนเทศถูกโจมตีจากผู้ประสงค์ร้ายที่บุกรุกระบบโดยตรง หรือใช้โปรแกรมไม่พึงประสงค์ต่าง ๆ เพื่อเข้าถึงและนำข้อมูลที่ได้ไปใช้ ทำลาย หรือสร้างผลประโยชน์ทางการเงิน ซึ่งส่งผลให้ระบบสารสนเทศในองค์การถูกละเลย ขาดการดูแลและไม่ได้รับการจัดการด้านการรักษาความมั่นคงปลอดภัยที่ดีพอ ทำให้เกิดปัญหาและถูกโจมตีได้ง่าย ซึ่งสอดคล้องกับระดับความรู้ของผู้บริหาร/เจ้าของกิจการ ระดับความรู้ของพนักงานในฝ่ายสารสนเทศ และระดับงบประมาณที่อยู่ในระดับน้อย จึงส่งผลให้มีการปฏิบัติในการจัดการความมั่นคงปลอดภัยทั้งเชิงรุกและเชิงรับน้อยทั้งสองแบบ

5.2 ข้อมูลด้านความสำเร็จในการรักษาความมั่นคงปลอดภัย

โดยรวมและรายด้าน ได้แก่ ความลับ ความคงสภาพ และความพร้อมใช้งาน อยู่ในระดับไม่แตกต่างจากปี 2558 (ปีที่ผ่านมา) จากทั้งหมด 3 ระดับคือ น้อยกว่าปีที่ผ่านมา ไม่แตกต่างจากปีที่ผ่านมา มากกว่าปีที่ผ่านมา ยกเว้นปัญหาในด้านความพร้อมใช้งาน ในเรื่องปัญหาโปรแกรมไม่พึงประสงค์ เช่น virus, worms, spyware, spam ซึ่งพบมากกว่าปี 2558 และปัญหาในด้านความลับ ในเรื่องปัญหาการหลอกลวงเพื่อให้ได้ข้อมูลจากบุคลากรในองค์การ ปัญหาการขโมยข้อมูลลูกค้าขององค์การหรือบุคลากรขององค์การ และปัญหาการขโมยอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์มือถือ ซึ่งพบน้อยกว่าปี 2558 แสดงให้เห็นว่า องค์การส่วนใหญ่มักตรวจพบเพียงปัญหาที่แสดงผลชัดเจนต่อการใช้งานระบบสารสนเทศ และอาจมีการละเลยหรือยังตรวจไม่พบปัญหาที่ไม่แสดงผลชัดเจนในด้านอื่น ๆ

5.3 ข้อมูลเพื่อทดสอบสมมติฐาน

สมมติฐานที่ 1 ขนาดองค์การที่แตกต่างกันมีรูปแบบการจัดการความมั่นคงปลอดภัยเชิงรุกและเชิงรับที่แตกต่างกัน พบว่า องค์การขนาดย่อมมีการจัดการความมั่นคงปลอดภัยแบบปฏิบัติน้อยทั้งเชิงรุก/รับมากกว่าแบบอื่น ๆ มาก ในขณะที่องค์การขนาดกลางมีการจัดการความมั่นคงปลอดภัยในหลายรูปแบบ คือ แบบปฏิบัติเชิงรุกมากกว่าเชิงรับ แบบปฏิบัติมากทั้งเชิงรุก/รับ และแบบปฏิบัติน้อยทั้งเชิงรุก/รับ เนื่องจากองค์การขนาดย่อมไม่มีการกำหนดนโยบายการใช้ระบบสารสนเทศที่ชัดเจน เพราะใช้ซอฟต์แวร์เพื่ออำนวยความสะดวกในการดำเนินธุรกิจเบื้องต้นเท่านั้น เช่น การใช้ microsoft office เพื่อจัดทำใบเสนอราคา ใบสั่งซื้อ ซึ่งซอฟต์แวร์เหล่านี้ขาดระบบการป้องกันสารสนเทศ และ

ในบางองค์การมีการใช้เครื่องคอมพิวเตอร์รวมกัน โดยปราศจากการป้องกันข้อมูลและกระบวนการตรวจสอบการพิสูจน์ตัวตน ขณะที่องค์การขนาดกลางมีการกำหนดนโยบายการใช้ระบบสารสนเทศที่ชัดเจน เช่น การกำหนดสิทธิ์การใช้งานระบบคอมพิวเตอร์และการเข้าถึงข้อมูลต่าง ๆ เนื่องจากมีการใช้ระบบสารสนเทศเพื่อการดำเนินธุรกิจมากกว่าองค์การขนาดย่อม เช่น ระบบซื้อสินค้าออนไลน์ ระบบคลังสินค้า ระบบจัดซื้อ เป็นต้น จึงทำให้มีระดับการจัดการความมั่นคงปลอดภัยที่แตกต่างกัน สอดคล้องกับ Makumbi et al. [2] ที่พบว่า ระดับของการรักษาความปลอดภัยระบบสารสนเทศขึ้นอยู่กับการนำระบบสารสนเทศมาใช้ในการดำเนินกิจกรรมทางธุรกิจขององค์การ และสอดคล้องกับ Clear [12] พบว่า องค์การขนาดกลางมีการกำหนดนโยบายในการรักษาความปลอดภัย รวมถึงมีการจัดการอบรมเพื่อให้ตระหนักถึงการรักษาความปลอดภัยมากกว่าองค์การขนาดเล็ก

สมมติฐานที่ 2 งบประมาณด้านความมั่นคงปลอดภัยที่แตกต่างกัน มีรูปแบบการจัดการความมั่นคงปลอดภัยเชิงรุกและเชิงรับแตกต่างกัน พบว่า องค์การส่วนใหญ่มีระดับงบประมาณ 1% - 4% และมีรูปแบบการจัดการความมั่นคงปลอดภัยแบบปฏิบัติน้อยทั้งเชิงรุก/รับ เนื่องจากการได้รับงบประมาณที่น้อยทำให้ไม่เพียงพอต่อการดำเนินงาน จึงทำให้การจัดการความมั่นคงปลอดภัยมีการปฏิบัติในระดับน้อย ในขณะที่เมื่อองค์การมีงบประมาณที่มากขึ้นทำให้มีการจัดการความมั่นคงปลอดภัยทั้งเชิงรุกและเชิงรับมีการปฏิบัติมากขึ้นด้วย สอดคล้องกับ Amrin [13] ที่พบว่า ผู้บริหารไม่ต้องการเสียค่าใช้จ่ายจำนวนมากจากการใช้ซอฟแวร์รักษาความปลอดภัยที่เหมาะสม รวมถึงการดำเนินการต่าง ๆ เกี่ยวกับมาตรฐานและนโยบายความมั่นคงปลอดภัย สอดคล้องกับ จุมพฏ กาญจนกำธร [14] ที่พบว่า งบประมาณที่องค์การได้รับ เพื่อการบริหารความมั่นคงปลอดภัยระบบสารสนเทศยังไม่เพียงพอ และสอดคล้องกับ Ngura et al. [15] ที่พบว่า ควรมีการจัดสรรทรัพยากรให้เพียงพอเพื่อให้การรักษาความมั่นคงปลอดภัยสามารถดำเนินการได้อย่างต่อเนื่อง

สมมติฐานที่ 3 ความรู้ด้านความมั่นคงปลอดภัยของพนักงานในแผนกเทคโนโลยีสารสนเทศ (IT) ที่แตกต่างกัน มีรูปแบบการจัดการความมั่นคงปลอดภัยเชิงรุกและเชิงรับที่แตกต่างกัน พบว่า พนักงานในแผนกเทคโนโลยีสารสนเทศ (IT) ส่วนใหญ่มีระดับความรู้ในระดับน้อยและมีรูปแบบการจัดการความมั่นคงปลอดภัยแบบปฏิบัติน้อยทั้งเชิงรุก/รับ ทั้งนี้เนื่องจากพนักงานขาดความรู้ความเข้าใจ จึงทำให้ไม่ทราบถึงช่องโหว่ที่มี อันตรายและภัยคุกคามต่าง ๆ ไม่ทราบถึงคุณสมบัติของอุปกรณ์ฮาร์ดแวร์และซอฟต์แวร์ที่ใช้ในการตรวจจับและป้องกัน ไม่ทราบถึงมาตรฐานหรือแนวทางในการปฏิบัติงานที่ทำให้เกิดความปลอดภัยต่อระบบสารสนเทศสำหรับผู้ใช้งาน รวมถึงไม่สามารถนำเสนอแนวทางหรือข้อเสนอแนะแก่ผู้บริหารเพื่อจัดการช่องโหว่และภัยคุกคามต่าง ๆ ได้ จึงทำให้การจัดการความมั่นคงปลอดภัยมีการปฏิบัติในระดับน้อย ในขณะที่เมื่อพนักงานมีระดับความรู้ที่มากขึ้นทำให้มีการจัดการความมั่นคงปลอดภัยทั้งเชิงรุกและเชิงรับมีระดับการปฏิบัติที่มากขึ้นด้วย สอดคล้องกับ วราภรณ์ ธวิทย์ชัยพร [16] ที่พบว่า บุคลากรยังขาดความรู้ความเข้าใจในเรื่องของความปลอดภัยสารสนเทศ และให้สนใจเพียงความสะดวกรวดเร็ว ในการนำข้อมูลไปใช้งานเป็นหลัก จนละเลยมุมมองสำคัญในด้านอื่นๆ และสอดคล้องกับ ถนอมศรี เตมานุวัตร์ [17] ที่พบว่า บุคลากรต้องพัฒนาความรู้และความเข้าใจในมาตรฐาน ISO/IEC 27001 และมีความตระหนักด้านความปลอดภัยในระบบสารสนเทศด้วย

สมมติฐานที่ 4 ความรู้ด้านความมั่นคงปลอดภัยของผู้บริหาร/เจ้าของกิจการที่แตกต่างกัน มีรูปแบบการจัดการความมั่นคงปลอดภัยเชิงรุกและเชิงรับที่แตกต่างกัน พบว่า ผู้บริหาร/เจ้าของกิจการส่วนใหญ่มีระดับความรู้ในระดับน้อย และมีรูปแบบการจัดการความมั่นคงปลอดภัยแบบปฏิบัติน้อยทั้งเชิงรุก/รับ เนื่องจากผู้บริหาร/เจ้าของกิจการส่วนมากมักมีความรู้เกี่ยวกับการดำเนินธุรกิจเท่านั้น ไม่มีความรู้หรือมีความรู้เพียงเล็กน้อยในด้านเทคโนโลยีสารสนเทศ ทำให้ไม่ทราบถึงจุดอ่อนที่เป็นช่องโหว่ของระบบสารสนเทศที่นำมาใช้ อันตรายจากภัยคุกคามต่าง ๆ รวมถึงมูลค่าความเสียหายที่อาจเกิดขึ้นเมื่อถูกโจมตี ผู้บริหาร/เจ้าของกิจการจึงมักไม่เห็นความสำคัญในการรักษาความมั่นคงปลอดภัยมากเท่าที่ควร ไม่มีการกำหนดนโยบายเพื่อสนับสนุนในเรื่องดังกล่าว ทำให้การจัดการความมั่นคงปลอดภัยระบบสารสนเทศขององค์การมีการปฏิบัติในระดับน้อย ในขณะที่เมื่อผู้บริหาร/เจ้าของกิจการมีระดับความรู้ที่มากขึ้นทำให้มีการจัดการความมั่นคงปลอดภัยทั้งเชิงรุกและเชิงรับมีระดับการปฏิบัติที่มากขึ้นเช่นกัน สอดคล้องกับ Makumbi et al. [2] ที่พบว่า เจ้าของกิจการยังขาด

ความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยในเรื่องเทคโนโลยีที่ใช้ และมาตรการการควบคุมต่าง ๆ ในการรักษาความมั่นคงปลอดภัย มีการละเลยการประเมินความเสี่ยง ไม่มีการกำหนดบุคลากรผู้รับผิดชอบที่ชัดเจน และขาดการดำเนินงานอย่างต่อเนื่อง ซึ่งเป็นอุปสรรคต่อการดำเนินงานรักษาความปลอดภัยระบบสารสนเทศเป็นอย่างมาก

สมมติฐานที่ 5 รูปแบบการจัดการความมั่นคงปลอดภัยเชิงรุกมีผลต่อการเพิ่มขึ้นของความสำเร็จในการรักษาความปลอดภัยมากกว่าเชิงรับ พบว่า ความสำเร็จในการรักษาความมั่นคงปลอดภัยในด้านความลับ และด้านความพร้อมใช้งาน องค์การส่วนใหญ่นั้นมีปัญหาด้านความมั่นคงปลอดภัยอยู่ในระดับน้อยกว่าปี 2558 (ปีที่ผ่านมา) ได้แก่ องค์การที่มีรูปแบบปฏิบัติมากทั้งเชิงรุก/รับ และแบบปฏิบัติเชิงรุกมากกว่าเชิงรับ และในด้านความคงสภาพ องค์การส่วนใหญ่ที่มีปัญหาด้านความมั่นคงปลอดภัยอยู่ในระดับน้อยกว่าปี 2558 คือองค์การที่มีรูปแบบปฏิบัติเชิงรุกมากกว่าเชิงรับ ในขณะที่ความสำเร็จในภาพรวมทั้ง 3 ด้านมีเพียงองค์การที่มีรูปแบบปฏิบัติเชิงรุกมากกว่าเชิงรับเท่านั้น ที่มีปัญหาด้านความมั่นคงปลอดภัยน้อยกว่าปี 2558 อาจเนื่องมาจากการใช้งบประมาณที่มีจำกัดในการดำเนินการทั้งเชิงรุกและเชิงรับ ทำให้ไม่สามารถดำเนินการได้อย่างเต็มที่ส่งผลให้มีประสิทธิภาพลดน้อยลง ดังนั้นจึงควรมุ่งเน้นการจัดการความมั่นคงปลอดภัยแบบเชิงรุก ซึ่งเป็นการป้องกันไม่ให้เกิดปัญหามากกว่าการแก้ปัญหาที่เกิดขึ้นแบบเชิงรับ สอดคล้องกับ Kwon and Johnson [4] ที่พบว่า การลงทุนเชิงรุกในการรักษาความมั่นคงปลอดภัยทำให้องค์การปลอดภัยจากภัยคุกคาม เป็นระยะเวลายาวนานกว่าการลงทุนเชิงรับ และพบความล้มเหลวด้านความมั่นคงปลอดภัยลดลง 60 % ในขณะที่การลงทุนเชิงรับพบความล้มเหลวลดลงเพียง 30 % และสอดคล้องกับ King and Teo [18] พบว่าการบริหารจัดการเชิงรุก ทำให้มีปัญหาต่าง ๆ เกิดขึ้นน้อยกว่าการจัดการเชิงรับ

สมมติฐานที่ 6 รูปแบบการจัดการความมั่นคงปลอดภัยเชิงรุก มีความสำเร็จในการรักษาความปลอดภัยมากกว่าเชิงรับ พบว่า ในรายรวมและในรายด้าน ได้แก่ ด้านความลับ ความคงสภาพ และความพร้อมใช้งาน รูปแบบการจัดการความมั่นคงปลอดภัยแบบปฏิบัติมากทั้งเชิงรุก/รับ และแบบปฏิบัติเชิงรุกมากกว่าเชิงรับ มีความสำเร็จในการรักษาความปลอดภัยมากกว่าแบบปฏิบัติน้อยทั้งเชิงรุก/รับ นอกจากนี้ยังพบว่าในด้านความพร้อมใช้งาน แบบปฏิบัติเชิงรุกมากกว่าเชิงรับมีความสำเร็จในการรักษาความปลอดภัยมากกว่าแบบปฏิบัติเชิงรับมากกว่าเชิงรุกอีกด้วย แสดงว่าการจัดการความมั่นคงปลอดภัยเชิงรุกทำให้ปัญหาลดน้อยลงและมีความสำเร็จเพิ่มมากขึ้น สอดคล้องกับ Qian et al. [3] ที่พบว่าวิธีการจัดการความเสี่ยงเชิงรุกมีอัตรารองรับการเกิดการโจมตีได้มากกว่า ความรุนแรงและความเสียหายของปัญหาที่เกิดขึ้นน้อยกว่า มีการตรวจจับการโจมตีได้ดีกว่า และมีการป้องกันหรือตอบสนองการโจมตีได้ดีกว่าวิธีการจัดการความเสี่ยงเชิงรับ

6. ข้อเสนอแนะ

6.1 ข้อเสนอแนะเพื่อนำไปใช้

6.1.1 องค์การควรมีความตื่นตัวและพัฒนาตนเองอยู่เสมอ โดยการอบรมพนักงานในฝ่ายสารสนเทศ และผู้บริหาร/เจ้าของกิจการอย่างสม่ำเสมอ เพื่อเพิ่มความรู้ความเข้าใจในการรักษาความมั่นคงปลอดภัยจากภัยคุกคามใหม่ ๆ รวมถึงควรจัดหาฮาร์ดแวร์และซอฟต์แวร์ที่มีประสิทธิภาพ ในการตรวจจับและป้องกันภัยคุกคามมาใช้งานเพิ่มมากขึ้น เพื่อให้ระบบสารสนเทศสามารถทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ

6.1.2 องค์การควรกำหนดนโยบายด้านความมั่นคงปลอดภัยระบบสารสนเทศ โดยใช้แนวทางเชิงรุก ควบคู่กับมาตรฐาน ISO/IEC 27001 เพื่อให้เกิดประสิทธิภาพในการรักษาความมั่นคงปลอดภัยสูงสุด

6.2 ข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป

6.2.1 ควรมีการศึกษาปัจจัยในด้านอื่น ๆ ที่มีผลต่อรูปแบบการจัดการด้านความมั่นคงปลอดภัยขององค์การ เช่น ประเภทธุรกิจ ระยะเวลาดำเนินกิจการ รายได้องค์การ ระบบสารสนเทศที่ใช้งาน อุปกรณ์ฮาร์ดแวร์หรือซอฟร์แวร์ที่ใช้ในการรักษาความปลอดภัย เป็นต้น เพื่อให้คลอบคลุมและชัดเจนมากยิ่งขึ้น

6.2.2 ควรมีการสัมภาษณ์ในการเก็บรวบรวมข้อมูล ซึ่งอาจทำให้ได้รับข้อมูลที่แท้จริงและหลากหลายมากขึ้น

7. เอกสารอ้างอิง

[1] Xian Ng, Z., Ahmad, A., Maynard, S. B., “Information security management: factors that influence security investments in

SMES", Retrieved May 11, 2016, from http://ro.ecu.edu.au/ism/157.

[2] Makumbi, L., Miriti, E. K., Kahonge, A. M., "An analysis of information technology (IT) security practices : A case study of Kenyan small and medium enterprises (SMEs) in the financial sector", International Journal of Computer Applications, 18(57), 2012: 33-36.

[3] Qian, Y., Fang, Y., Gonzalez, J. J., "Manage information security risks during new technology adoption", Computers and Security, 31(8), 2012: 859-869.

[4] Kwon, J., Johnson, M. E., "Proactive vs reactive security investments in the health sector", MIS Quarterly, 2(38), 2014: 451-471.

[5] Kaspersky Lab ZAO, "Global corporate IT security risks: 2013", Retrieved July 30, 2014, from http://media.kaspersky.com.

[6] Chang, S. E., Ho, C. B., "Organizational factors to the effectiveness of implementing information security management", Industrial management & data systems, 3(106), 2006: 345-361.

[7] Al-Awadi, M., Renaud, K., "Success factors in information security implementation in organizations", Retrieved August 5, 2014, from http://theses.gla.ac.uk/.

[8] ปริญญ์ เสรีพงศ์, "ISO 27001 introduction to information security management system", สถาบันเพิ่มผลผลิตแห่งชาติ, 2551.

[9] Microsoft, "Security strategies", Retrieved August 31, 2014, from http://technet.microsoft.com/en-us/library/cc723506.aspx

[10] Stroie, E. R., Rusu, A. C., "Security risk management - approaches and methodology", Informatica Economica, 15(1), 2011: 228-240.

[11] Symantec Corporation, "Internet security threat report 2016 volume 21", Retrieved May 11, 2016, from www.symantec.com.

[12] Clear, F., "SMEs, electronically-mediated working and data security : cause for concern?", Int. Journal of Business Science and Applied Management, 2(2), 2007: 1-20.

[13] Amrin, N., "The Impact of Cyber Security on SMEs", Unpublished master's thesis, University of Twente, Enschede, Netherlands, 2014.

[14] จุมพฏ กาญจนกำธร, "การพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา", ดุษฎีนิพนธ์ปรัชญาดุษฎีบัณฑิต, มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา, 2555.

[15] Ngura, S., Kimwele, M., Rotich, G., "Determinants of Information Security Small and Medium Enterprises in Kenya", European Journal of Business Management, 2(1), 2015: 124-143.

[16] วราภรณ์ ธวิทย์ชัยพร, "แนวทางการนำ Information Security Management มาใช้ในการจัดระเบียบการบริหารจัดการด้านความปลอดภัยสารสนเทศ กรณีศึกษาบริษัทให้คำปรึกษาด้านสารสนเทศแห่งหนึ่ง", สารนิพนธ์วิทยาศาสตรมหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์, 2549.

[17] ถนอมศรี เตมานุวัตร์, "การปรับปรุงกระบวนการให้บริการงานสารสนเทศ โดยการประยุกต์ใช้มาตรฐานบริหารความปลอดภัยของข้อมูลสารสนเทศ ISO/IEC 27001", วิทยานิพนธ์วิทยาศาสตรมหาบัณฑิต, มหาวิทยาลัยราชภัฏสวนสุนันทา, 2554.

[18] King, W. R., Teo, T. S. H., "Assessing the impact of proactive versus reactive modes of strategic information systems planning", Omega The International Journal of Management Science, 6(28), 2000: 667-679.