ตัวแบบการรักษาความมั่นคงปลอดภัยสารสนเทศของกองบัญชาการกองทัพไทย

Royal Thai Armed Force Information Security Models

ธันวัฒน์ นามอ่อนตา[1]
วศิณ ชูประยูร[2]

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อศึกษา 1) ระดับอิทธิพลของพฤติกรรมปัจจุบันเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศของข้าราชการกองทัพไทยต่อปัญหาและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ 2) ระดับอิทธิพลของสภาพปัญหาด้านการรักษาความมั่นคงปลอดภัยสารสนเทศต่อแนวปฏิบัติดังกล่าว และ3) พัฒนาแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยที่เหมาะสมกับบริบทของกองบัญชาการกองทัพไทยใช้แบบสอบถามเป็นเครื่องมือในการเก็บรวบรวมข้อมูลจากข้าราชการของกองบัญชาการกองทัพไทยจำนวน 400 คน สถิติที่ใช้ในการทดสอบสมมติฐานคือการวิเคราะห์ถดถอยพหุคูณ ได้ผลการทดสอบเป็นสมการอิทธิพล (ตัวแบบ) จำนวน 3 ตัวแบบที่ขนาดอิทธิพล (R^2) เท่ากับ .744, .443 และ .445 ผลการวิจัยชี้ว่าแนวปฏิบัติที่เหมาะสมด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของกองบัญชาการกองทัพไทยควรประกอบด้วย 4 ด้านสำคัญ ดังนี้ 1) กำหนดตัวบุคคลอย่างชัดเจนเป็นลายลักษณ์อักษรในการเข้าถึงข้อมูลชั้นความลับของหน่วยงาน อาทิ ข้อมูลเกี่ยวกับบุคคล เอกสาร และสถานที่ 2) เข้มงวดในการใช้ระบบการพิสูจน์บุคคลก่อนเข้าใช้ระบบสารสนเทศของผู้ใช้ 3) จัดแหล่งเก็บข้อมูลสำรองขององค์กรอย่างเป็นรูปธรรมและกำหนดให้มีหน่วยงานรับผิดชอบโดยเฉพาะ และ 4) ใช้ผลิตภัณฑ์ซอฟต์แวร์ที่ถูกต้องตามลิขสิทธิ์เท่านั้น

คำสำคัญ: ISO/IEC 27001 พฤติกรรมความมั่นคงปลอดภัยสารสนเทศ แนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศกองบัญชาการกองทัพไทย

---

[1]นักศึกษาปริญญาโท, หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาการจัดการเทคโนโลยีสารสนเทศ วิทยาลัยเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยรังสิต, E-mail: sfosamod@gmail.com

[2]ผู้ช่วยศาสตราจารย์, หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาการจัดการเทคโนโลยีสารสนเทศ วิทยาลัยเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยรังสิต, E-mail: vasin@rsu.ac.th

ABSTRACT

This research aimed to study 1) influence levels of current information security behavior of the Thai Armed Force officers toward information security practices, 2) influence levels of the information security problems toward the practices, and 3) to develop appropriate information security practices based on the Thai Armed Forces contexts. Questionnaires were used as a tool gathering data from 400 Royal Thai Armed Force officers (the respondents). The multiple regression analysistechnique was applied to test hypotheses. The test resulted that there were three influence equations (models) at $R^2$0.744, 0.443, and 0.445.The findings also pointed out that the practices should be composed of four key dimensions: 1) clearly official identify the individuals accessing confidential information, e.g. personal profiles, documents and places, 2) rigorously use an authentication system before accessing information systems,3) organize reserve information repository and establish a special responsible unit, and 4) use copyrighted software products.

Keywords: ISO/IEC27001, information security behavior, Royal Thai Armed Forces information security practice

ความเป็นมาและความสำคัญของปัญหา

กองบัญชาการกองทัพไทย เป็นหน่วยงานด้านความมั่นคง เป็นหน่วยงานภายใต้สังกัดกระทรวงกลาโหม มีภารกิจหลักในการสร้างความมั่นคง ความสงบเรียบร้อย และอำนวยการรบร่วมของกองทัพไทย และรักษาไว้ซึ่งสถาบันหลักของชาติ ปัจจุบันความมั่นคงปลอดภัยสารสนเทศเป็นปรากฏการณ์สำคัญอย่างหนึ่ง ที่กองทัพไทยกำลังเผชิญหน้า และได้รับรายงานการโจมตีเว็บไซต์และการเจาะระบบการรักษาความปลอดภัยสารสนเทศของกองบัญชาการกองทัพไทย ในช่วงเดือนเมษายน พ.ศ.2558 ถึงสิงหาคม พ.ศ.2559 พบว่ามีการโจมตี จำนวน 2,348 ครั้ง (กองรักษาความปลอดภัยสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศ กรมการสื่อสารทหาร, 2559) เป็นการโจมตีจากในประเทศเป็นส่วนใหญ่ผู้โจมตีมีจุดมุ่งหมายที่จะเปลี่ยนแปลงหน้าเว็บไซต์ของกองทัพไทย มีข้อมูลขั้นความลับที่ถูกเปิดเผยแก่ผู้ไม่มีส่วนเกี่ยวข้องในหลายวาระด้วยกัน อาทิ จำนวนกำลังพล ฎีกาเงินเดือนผู้บังคับบัญชา คำสั่งแต่งตั้งกรรมการสอบสวนคดีความต่างๆ คำสั่งแต่งตั้งคณะกรรมการสอบราคาการจัดซื้อจัดจ้าง จากการสำรวจเบื้องต้นพบว่า ข้าราชการสังกัดกองบัญชาการกองทัพไทยส่วนมากไม่ตระหนักและไม่ให้ความสำคัญในการใช้ระบบ

ไปรษณีย์อิเล็กทรอนิกส์ของกองทัพ (Rtarf Mail) ให้ปลอดภัย และใช้แอปพลิเคชัน (Line) ในการสื่อสารข้อมูลการดำเนินงานของกองทัพ ปัจจุบันรัฐบาลได้พัฒนาแอปพลิเคชัน G–Chat เพื่อให้ข้าราชการและพนักงานของรัฐได้ใช้เป็นเครื่องมือในการสื่อสารงานทางราชการ เพื่อป้องกันความเสี่ยงต่อการที่ความลับทางราชการจะรั่วไหลสู่ผู้ที่ไม่หวังดีและง่ายต่อการถูกโจมตี

ตามที่ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 มาตรา 5 ได้กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และ มาตรา 7 กำหนดให้หน่วยงานของรัฐต้องจัดทำเป็นประกาศ และต้องได้รับความเห็นชอบจากคณะกรรมการ หรือหน่วยงานที่คณะกรรมการมอบหมายจึงมีผลบังคับได้นั้น กองบัญชาการกองทัพไทยได้จัดทำนโยบายดังกล่าว โดยเริ่มจากการศึกษามาตรการด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่เป็นมาตรฐานสากล เพื่อหาแนวทางในการประยุกต์ใช้มาตรฐานดังกล่าวให้เหมาะสมกับสภาพการณ์ปัจจุบันของกองบัญชาการกองทัพไทยในหลายมาตรฐาน ได้แก่ ISO79990:2005 , BS17999:2005, COBIT5 และ ISO/IEC 27001 และพบว่ามาตรฐาน ISO/IEC 27001 เป็นมาตรฐานที่เหมาะสมที่สุดในสถานการณ์ปัจจุบันของกองบัญชาการกองทัพไทย ด้วยเหตุผลที่ว่าการรักษาความปลอดภัยสารสนเทศตามกรอบมาตรฐาน ISO/IEC 27001 มีมาตรการที่สอดคล้องกับบริบทของกิจกรรมด้านสารสนเทศของกองบัญชาการกองทัพไทย

จากที่กล่าวมาข้างต้นกองบัญชาการกองทัพไทยได้จัดทำนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศขึ้นโดยประยุกต์ใช้มาตรฐาน ISO/IEC 27001 และได้รับการรับรองจากกระทรวงดิจิทัลและเศรษฐกิจเรียบร้อยแล้ว และประกาศใช้เมื่อวันที่19 กันยายน พ.ศ.2559 แม้ว่ากองบัญชาการกองทัพไทยจะมีนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ แล้วนั้น แต่ข้าราชการส่วนใหญ่ก็ยังไม่ตระหนักอยู่ดีและมองข้ามนโยบายอีกทั้งยังละเมิดอยู่เป็นปกติโดยไม่คำนึงผลกระทบ

จากความเป็นมาและสภาพปัญหาข้างต้นยังไม่เคยมีการศึกษาวิจัยในประเด็นนี้มาก่อน ผู้วิจัยเห็นควรที่ศึกษาวิจัย แนวทางการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศของกองบัญชาการกองทัพไทยบนพื้นฐานมาตรฐานสากล ISO/IEC 27001 ผ่านมุมมองของข้าราชการกองทัพไทยในบริบทของพฤติกรรมปัจจุบันในการรักษาความมั่นคงปลอดภัยสารสนเทศ สภาพปัญหาที่ประสบ และแนวทางที่เหมาะสมในการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อให้ได้ผลลัพธ์มาปรับใช้กับบริบทของกองบัญชาการกองทัพไทย และเพื่อนำข้อค้นพบไปเป็นแนวทางพื้นฐานในการดำเนินการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศต่อไปในอนาคต

วัตถุประสงค์ของการวิจัย

การวิจัยนี้มีวัตถุประสงค์เพื่อศึกษา ก) ระดับอิทธิพลของพฤติกรรมปัจจุบันในการรักษาความมั่นคงปลอดภัยสารสนเทศของข้าราชการกองบัญชาการกองทัพไทยต่อสภาพปัญหาและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ข) ระดับอิทธิพลของสภาพปัญหาต่อแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ และ ค) พัฒนาแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยที่เหมาะสมกับบริบทของกองบัญชาการกองทัพไทย

แนวคิดและทฤษฎีที่เป็นพื้นฐานของการวิจัย

แนวคิดและทฤษฎีที่เป็นพื้นฐานของการวิจัยในครั้งนี้ ประกอบด้วย

1) แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ ตามระบุไว้ในพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 มาตรา 5 และ 7

2) แนวคิดเกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศ ประกอบด้วย 3 ส่วน ตามแนวคิดของ Pender-Bey (Pender-Bey, 2015) คือ

ก. ความลับ - การไม่เปิดเผยข้อมูลต่อบุคคลหรือระบบที่ไม่ได้รับสิทธิ์ให้เข้าถึงข้อมูลนั้น เพราะฉะนั้น การรักษาความลับต้องมีมาตรการป้องกันการเข้าถึงสารสนเทศหรือข้อมูล

ข. ความสมบูรณ์ - ข้อมูลที่ไม่สามารถแก้ไขได้โดยไม่ได้รับอนุญาต เป็นข้อมูลคงที่ไม่มีการแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม เป็นสารสนเทศที่นำไปใช้ประโยชน์ได้อย่างถูกต้อง

ค. ความพร้อมใช้ - การที่ระบบมีความปลอดภัยจากภัยคุกคามทุกด้านไม่ว่าจะเป็น ไวรัสคอมพิวเตอร์ การเจาะระบบจากภายนอก รวมไปถึงการหยุดชะงักจากระบบไฟฟ้าสามารถใช้งานได้ตลอดเวลา

3) แนวคิดเกี่ยวกับมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001 เป็นมาตรฐานสากลที่มุ่งเน้นด้านการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กรและใช้เป็นมาตรฐานอ้างอิงเพื่อเป็นแนวทางในการเสริมสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กรอย่างแพร่หลาย ประกอบด้วย10 หัวข้อหลัก ดังนี้ (International Organization for Standardization (ISO) and the International Electrotechnical Commission (ISO/IEC, 2013)

ก) ขอบเขต (Scope) อธิบายให้เห็นว่า ISO/IEC 27001 มีขอบเขตครอบคลุมข้อกำหนดสำหรับการจัดตั้ง การดำเนินการ การบำรุงรักษาและปรับปรุงระบบการจัดการความมั่นคงปลอดภัย

สารสนเทศอย่างต่อเนื่องภายในบริบทขององค์กร รวมทั้งข้อกำหนดว่าด้วยการประเมินและการรักษาของความเสี่ยงด้านความปลอดภัยสารสนเทศที่ปรับให้เหมาะกับความต้องการขององค์กร

ข) การอ้างอิงเชิงปทัสถาน (Normative References) อธิบายถึงความจำเป็นในการอ้างอิงส่วนใดส่วนหนึ่งหรือทั้งหมดของเอกสารมาตรฐานนี้เมื่อจะนำไปประยุกต์ใช้

ค) ข้อกำหนดและคำจำกัดความ (Terms and Definitions) ในส่วนนี้ อธิบายสั้นๆ ให้ทราบว่าข้อกำหนดและคำจำกัดความต่างๆ ล้วนกำหนดไว้แล้วในการประยุกต์ใช้มาตรฐานนี้

ง) บริบทขององค์กร (Context of the Organization) อธิบายเกี่ยวกับความเข้าใจองค์กรและบริบทขององค์กร การกำหนดความจำเป็นและความคาดหวังของผู้ที่เกี่ยวข้อง การกำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

จ) ภาวะผู้นำ (Leadership) อธิบายเกี่ยวกับภาวะผู้นำและการให้ความสำคัญ นโยบาย บทบาทหน้าที่รับผิดชอบ และอำนาจหน้าที่

ฉ) การวางแผน (Planning) อธิบายเกี่ยวกับการจัดการความเสี่ยงและโอกาส วัตถุประสงค์และการบรรลุวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ

ช) การสนับสนุน (Support) อธิบายเกี่ยวกับทรัพยากร สมรรถนะ ความตระหนัก การสื่อสาร สารสนเทศที่เป็นลายลักษณ์อักษร

ซ) การดำเนินการ (Operation) อธิบายเกี่ยวกับการวางแผนดำเนินการและควบคุม การประเมิน และจัดการ ความเสี่ยง ด้านความมั่นคงปลอดภัยสารสนเทศ

ฌ) การประเมินการดำเนินงาน (Performance Evaluation) อธิบายเกี่ยวกับการติดตาม ตรวจสอบ การวัด การวิเคราะห์ และประเมิน การตรวจสอบภายใน การทบทวนด้านการจัดการ

ญ) การปรับปรุง (Improvement) อธิบายเกี่ยวกับการไม่ปฏิบัติตามและการแก้ไข การปรับปรุงองค์กรอย่างต่อเนื่อง

4) นโยบายการรักษาความปลอดภัยสารสนเทศ กองบัญชาการกองทัพไทย พ.ศ. 2559 ประกอบด้วย 6 ส่วน คือ

ก) คำนิยาม

ข) แนวปฏิบัติในการควบคุมการเข้าถึงและใช้งานสารสนเทศ

ค) แนวปฏิบัติในการควบคุมการเข้าถึงระบบสารสนเทศ

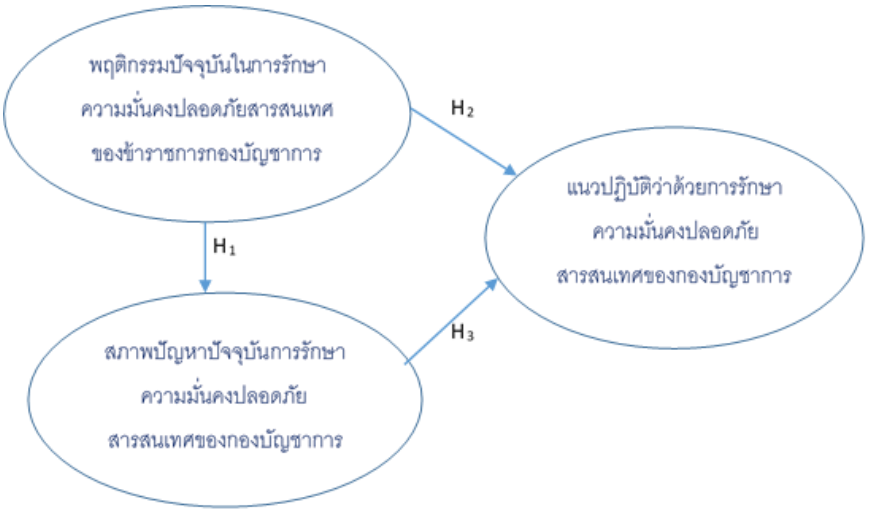
ง) แนวปฏิบัติในการใช้งานระบบสารสนเทศและระบบสำรองของสารสนเทศ

จ) แนวปฏิบัติในการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน และ

ฉ) แนวปฏิบัติในการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศ

จากแนวคิดและทฤษฎีที่กล่าวแล้วข้างต้น ผู้วิจัยได้นำมาพัฒนาเป็นกรอบการวิจัย ดังรูปที่ 1

กรอบแนวคิดในการวิจัย



รูปที่ 1 กรอบการวิจัย

จากกรอบการวิจัย มีรายละเอียดเกี่ยวกับตัวแปรดังนี้

งานวิจัยนี้มุ่งเน้นการวิเคราะห์ถดถอยพหุคูณ จึงเรียกตัวแปรอิสระว่า ตัวแปรพยากรณ์ (Predictor) และเรียกตัวแปรตามว่า ตัวแปรเกณฑ์ (Criterion Variable)

ตัวแปรเกณฑ์ คือ แนวปฏิบัติว่าด้วยการรักษาความมั่นคงปลอดภัยสารสนเทศของกองบัญชาการกองทัพไทย ประกอบด้วย 12 ตัวแปร คือ

1) การเขียนแผนปฏิบัติราชการให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและประกาศใช้โดยหัวหน้าหน่วยงาน (BT1)

2) การกำหนดตัวบุคคลอย่างชัดเจนเป็นลายลักษณ์อักษรในการเข้าถึงข้อมูลชั้นความลับของหน่วยงานทั้งที่เป็นข้อมูลเกี่ยวกับบุคคล เอกสาร และสถานที่ (BT2)

3) การใช้ระบบการพิสูจน์บุคคลก่อนเข้าใช้ระบบสารสนเทศของผู้ใช้อย่างเข้มงวด (BT3)

4) การจัดแหล่งเก็บข้อมูลสำรองของหน่วยงานอย่างเป็นรูปธรรมและมีหน่วยงานที่รับผิดชอบโดยตรง (BT4)

5) การรวบรวมเหตุการณ์อย่างครบถ้วนของฝ่ายความมั่นคงปลอดภัยสารสนเทศเพื่อนำไปวิเคราะห์หาแนวทางป้องกันหรือแก้ไข อย่างน้อย 1 ครั้งทุก 6 เดือน เพื่อลดโอกาสและป้องกันไม่ให้เกิดเหตุการณ์ซ้ำ (BT5)

6) การกำหนดเป็นลายลักษณ์อักษรให้ทุกหน่วยงานต้องตรวจสอบและอัปเดตโปรแกรม AntiVirus ทุก 1 เดือน (BT6)

7) การฝึกอบรมบุคลากรและให้ความรู้ในเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอและต่อเนื่อง(BT7)

8) การทบทวนพัฒนา และปรับปรุงรูปแบบกระบวนการทำงานด้านความมั่นคงปลอดภัยสารสนเทศที่ประกาศใช้แล้ว อย่างน้อยปีละ 1 ครั้ง เพื่อให้เกิดความมั่นใจว่ารูปแบบการปฏิบัติงานมีความเหมาะสม และมีความต่อเนื่องในการดำเนินงานตามระเบียบราชการได้อย่างมีประสิทธิภาพ (BT8)

9) การมีมาตรการและบทลงโทษหากมีการละเมิดการรักษาความมั่นคงปลอดภัยสารสนเทศ (BT9)

10) การใช้ผลิตภัณฑ์ซอฟต์แวร์ที่ถูกต้องตามลิขสิทธิ์เท่านั้น (BT10)

11) การจัดทำ check-list หรือ สร้างสถานการณ์สมมุติ หรือตัดระบบเพื่อนำไปประเมินและปรับปรุงการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ อย่างน้อยปีละ1 ครั้ง (BT11)

12) การควบคุมและตรวจสอบระบบเทคโนโลยีสารสนเทศในเชิงเทคนิค เช่น การปิดช่องโหว่ หรือทดสอบการเจาะระบบ จากนั้นทำรายงานประเมินผล อย่างน้อยทุก 6 เดือน (BT12)

ตัวแปรพยากรณ์ ประกอบด้วย 2 กลุ่มตัวแปร รวมทั้งสิ้น 19 ตัวแปรย่อย ได้แก่

ก) พฤติกรรมปัจจุบันเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ มี 9 ตัวแปร คือ

1) การทราบและเข้าใจนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศของกองบัญชาการกองทัพไทย (BH1)

2) การปฏิบัติตามกฎระเบียบ ข้อบังคับด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (BH2)

3) การเข้ารับการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (BH3)

4) การมีส่วนร่วมในการร่างนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ (BH4)

5) การเปลี่ยน User Name และ Password ในการเข้าใช้ระบบสารสนเทศของข้าราชการแต่ละคนอย่างสม่ำเสมอ (BH5)

6) การสำรองข้อมูลไว้มากกว่า 1 ที่จัดเก็บ (BH6)

7) การใช้รหัสผ่านเข้าใช้เครื่องคอมพิวเตอร์ร่วมกันกับบุคคลอื่น (BH7)

8) การไม่แจ้งไปยังผู้รับผิดชอบงานด้านความมั่นคงปลอดภัยสารสนเทศเมื่อประสบกับภัยคุกคามบนเครื่องคอมพิวเตอร์ (BH8)

9) การถือครองลิขสิทธิ์ซอฟต์แวร์ถูกต้องตามกฎหมาย (BH9)

ข) สภาพปัญหาด้านการรักษาความมั่นคงปลอดภัยสารสนเทศมี 10 ตัวแปร คือ

1) ขาดการประชาสัมพันธ์ให้ทราบถึงนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ (PB1)

2) ขาดการควบคุมบัญชีอุปกรณ์และ/หรือหลักฐานด้านสารสนเทศ (PB2)

3) ไม่เข้มงวดในการใช้ระบบการพิสูจน์บุคคลก่อนเข้าใช้ระบบสารสนเทศของผู้ใช้ (PB3)

4) ไม่กำกับดูแลอย่างเข้มงวดให้ทุกคนต้องใช้โปรแกรมอรรถประโยชน์ที่ถือครองลิขสิทธิ์โดยกองบัญชาการกองทัพไทย (PB4)

5) สภาพปัญหาด้านฮาร์ดแวร์ อาทิ สายส่งสัญญาณชำรุด กระแสไฟฟ้าตก คอมพิวเตอร์สูญหาย ฯลฯ (PB5)

6) ไม่มีข้อมูลสำรองไว้ใช้ในกรณีเกิดเหตุการณ์ที่ไม่คาดคิด เช่น ภัยพิบัติธรรมชาติ หรือ เกิดจากฝีมือมนุษย์ (PB6)

7) หน่วยงานไม่มีข้อกำหนดที่เป็นลายลักษณ์อักษรในการถ่ายโอนข้อมูล/สารสนเทศ (PB7)

8) ขาดการบำรุงรักษาระบบสารสนเทศอย่างต่อเนื่อง (PB8)

9) เมื่อเกิดเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศที่ส่งผลเสียต่อหน่วยงาน ผู้ประสบเหตุมักเพิกเฉยที่จะแจ้งให้หน่วยงานที่รับผิดชอบทราบทันที (PB9)

10) การละเมิดลิขสิทธิ์ซอฟต์แวร์ (PB10)

ระเบียบวิธีวิจัย

ก) ประชากรและกลุ่มตัวอย่าง

ประชากรการวิจัยครั้งนี้คือ ข้าราชการของกองบัญชาการกองทัพไทยที่ปฏิบัติงานอยู่ในพื้นที่กรุงเทพมหานครและปริมณฑล จำนวน 20,099 คน (กรมกำลังพลทหาร กองบัญชาการกองทัพไทย, 2559) จำนวน 32 หน่วยงาน ผู้วิจัยกำหนดขนาดกลุ่มตัวอย่างด้วยการใช้สูตรคำนวณของยามาเน (Yamane, 1973) ได้ขนาดตัวอย่างจำนวน 400 คนโดยใช้วิธีการสุ่มตัวอย่างโดยใช้หลักความน่าจะเป็นด้วยการสุ่มตัวอย่างแบบชั้นภูมิ (Stratified Sampling) โดยแยกข้าราชการกองบัญชาการกองทัพไทยออกเป็นกลุ่มชั้นภูมิตามหน่วยงานที่สังกัด

ข) เครื่องมือที่ใช้ในการวิจัย

ผู้วิจัยได้พัฒนาแบบสอบถามเพื่อใช้เป็นเครื่องมือในการเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่าง โดยใช้มาตรฐาน ISO/IEC 27001 : 2013 และ นโยบายการรักษาความปลอดภัยสารสนเทศ กองบัญชาการกองทัพ

ไทย พ.ศ.2559 เป็นกรอบแนวคิดในการกำหนดข้อคำถามในแบบสอบถาม ในแบบสอบถามประกอบด้วย 4 ตอน ตอนที่ 1 ใช้สอบถามเกี่ยวกับภูมิหลังของผู้ตอบแบบสอบถาม ตอนที่ 2-4 ใช้สอบถามมุมมองของผู้ตอบแบบสอบถามเกี่ยวกับพฤติกรรมปัจจุบัน สภาพปัญหาและแนวปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศของกองบัญชาการกองทัพไทย แบ่งระดับคำตอบออกเป็น 7 ระดับ (1 = น้อยที่สุด, 2 = น้อย, 3= ค่อนข้างน้อย, 4 = ปานกลาง, 5 = ค่อนข้างมาก, 6 = มาก, 7 = มากที่สุด) ตามมาตรวัดของ Likert (Likert, 1932)

ค) การตรวจสอบคุณภาพเครื่องมือวิจัย

ผู้วิจัยได้ทดสอบความเที่ยงตรงเชิงโครงสร้างและเนื้อหาของแบบสอบถาม โดยนำแบบสอบถามไปให้ผู้เชี่ยวชาญจำนวน 5 ท่าน ร่วมตรวจสอบความเที่ยงตรงดังกล่าว ผลการตรวจสอบ ได้ค่าดัชนีความสอดคล้อง (IOC) เท่ากับ 0.85 หมายความว่า แบบสอบถามมีความเที่ยงตรงทั้งในเชิงโครงสร้างและเนื้อหา จากนั้นได้นำแบบสอบถามไปทดลองกับกลุ่มตัวอย่างจำนวน 30 คน แล้วนำคำตอบที่ได้ไปคำนวณหาค่าความเชื่อมั่นตามวิธีการของครอนบัค (Cronbach, 1951) ได้ค่าสัมประสิทธิ์อัลฟาเท่ากับ 0.84 หมายความว่าแบบสอบถามนี้มีค่าความเชื่อมั่นอยู่ในระดับสูงสามารถใช้เป็นเครื่องมือในเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่างได้

ง) การเก็บรวบรวมข้อมูลและวิเคราะห์ข้อมูล

ผู้วิจัยใช้วิธีการสุ่มตัวอย่างโดยใช้หลักความน่าจะเป็นด้วยการสุ่มตัวอย่างแบบชั้นภูมิ (Stratified Sampling) โดยแยกข้าราชการกองบัญชาการกองทัพไทยออกเป็นกลุ่มชั้นภูมิตามหน่วยงานที่สังกัด จากนั้นจึงสุ่มอย่างง่ายเพื่อให้ได้จำนวนกลุ่มตัวอย่างตามสัดส่วนของขนาดกลุ่มตัวอย่างและกลุ่มประชากร และแจกแบบสอบถามด้วยวิธีฝากลิงค์แบบสอบถามในรูปแบบ Google Form ไว้บนเว็บเพจของกองบัญชาการกองทัพไทย ได้รับการตอบแบบสอบถามครบทั้ง 400 ฉบับ (ร้อยละ 100) และวิเคราะห์ข้อมูลการวิจัยโดยการใช้ สถิติทดสอบแบบที (t-test) การทดสอบค่า F และ การวิเคราะห์การถดถอยพหุคูณ (Multiple Regression Analysis)

ข้อค้นพบจากการวิจัย

ในการวิจัยครั้งนี้ ผู้ตอบแบบสอบถามส่วนใหญ่ร้อยละ 69.8 เป็นเพศชาย มีอายุงานระหว่าง 12 ปี ถึง 22 ปี มีชั้นยศประทวนและลูกจ้าง สำเร็จการศึกษาระดับปริญญาตรี มีคะแนนระดับความรอบรู้ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศเฉลี่ยเท่ากับ 7.41 จากคะแนนเต็ม 10 ส่วนใหญ่มีความรอบรู้ในการรักษาความปลอดภัยสารสนเทศอยู่ในระดับปานกลาง มีพฤติกรรมด้านการรักษาความมั่นคงปลอดภัยสารสนเทศค่อนข้างน้อย ประสบปัญหาด้านการรักษาความมั่นคงปลอดภัยสารสนเทศค่อนข้างมาก และ

มีมุมมองต่อแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศในระดับค่อนข้างมาก

ในทดสอบสมมติฐานด้วยเทคนิคการวิเคราะห์ถดถอยพหุคูณเพื่อพยากรณ์อิทธิพลของพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศต่อสภาพปัญหาด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (H_1) และพฤติกรรม/สภาพปัญหาด้านการรักษาความมั่นคงปลอดภัยสารสนเทศต่อแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (H_2และ H_3) ผู้วิจัยใช้วิธี Stepwise ในการคัดเลือกตัวแปรเข้าสมการ และทดสอบข้อตกลงเบื้องต้นในการวิเคราะห์ถดถอยพหุคูณตามลำดับ ดังนี้

1. ทดสอบว่าตัวแปรพยากรณ์และตัวแปรเกณฑ์มีการสุ่มมาจากประชากรที่มีการแจกแจงแบบปกติ
2. ทดสอบการไม่มีสภาวะร่วม (Multicollinearity) ของตัวแปรพยากรณ์
3. ทดสอบการไม่มีความสัมพันธ์ภายในของข้อมูล (Autocorrelation) ที่เก็บรวบรวมมาจากกลุ่มตัวอย่าง
4. ทดสอบความคลาดเคลื่อนที่เกิดขึ้นจากการพยากรณ์ โดยพิจารณาจากหลักเกณฑ์ต่อไปนี้ : มีการแจกแจงปกติมีค่าเฉลี่ยเท่ากับศูนย์และมีความแปรปรวนคงที่

ผลการทดสอบสมมติฐาน มีรายละเอียดดังต่อไปนี้

สมมติฐานที่ 1

H_1: พฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศมีอิทธิพลต่อสภาพปัญหาด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

ตารางที่ 1 การวิเคราะห์ถดถอยพหุคูณเพื่อพยากรณ์อิทธิพลพฤติกรรมปัจจุบันเกี่ยวกับการรักษาความมั่นคง ปลอดภัยสารสนเทศต่อปัญหาการรักษาความมั่นคงปลอดภัยสารสนเทศ

พฤติกรรม	b	SE_b	**β**	t	p-value
BH2	-.466	.035	-.500	-13.369	.000
BH3	.102	.027	.141	3.840	.000
BH6	-.073	.024	-.096	-3.088	.002
BH7	.149	.025	.236	6.044	.000
BH8	-.167	.024	-.273	-7.011	.000

ค่าคงที่ =7.997; SE_{est} = ±.5456

R=.862; R^2=.744; F=151.678; p-value=.000

จากตารางที่ 1 จะเห็นว่าพฤติกรรมปัจจุบันด้านความมั่นคงปลอดภัยสารสนเทศของผู้ตอบแบบสอบถามทั้ง 5 ด้าน (BH2, BH3, BH6, BH7 และ BH8) มีอิทธิพลต่อสภาพปัญหาการรักษาความมั่นคงปลอดภัยสารสนเทศ กล่าวคือพฤติกรรมทั้ง 5 ด้านดังกล่าวสามารถพยากรณ์สภาพปัญหาด้านการรักษาความมั่นคงปลอดภัยสารสนเทศได้แม่นยำถึงร้อยละ 74.4 (R^2 =.744) อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 โดยมีความคลาดเคลื่อนมาตรฐานในการพยากรณ์ที่ ±.5456 เมื่อพิจารณา ค่าสัมประสิทธิ์การถดถอย พบว่า BH2 สามารถพยากรณ์สภาพปัญหาการรักษาความมั่นคงปลอดภัยสารสนเทศได้สูงสุด ดังสมการที่ 1

$$\widehat{\text{สภาพปัญหาโดยรวม}} = 7.997 - .466\text{BH2} + .102\text{BH3} - .073\text{BH6} + .149\text{BH7} - .167\text{BH8} \ldots\ldots\ldots\ldots (1)$$

จากสมการที่ 1 อธิบายได้ว่า เมื่อพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ ทั้ง 5 ด้าน มีค่าเป็น 0 จะมีสภาพปัญหารักษาความมั่นคงปลอดภัยสารสนเทศที่ระดับ 7.997 เมื่อ BH3 และ BH7 เพิ่มขึ้น 1 หน่วย จะทำให้สภาพปัญหาด้านการรักษาความมั่นคงปลอดภัยสารสนเทศเพิ่มขึ้น .102 และ .149 หน่วย ตามลำดับ และ เมื่อ BH2, BH6 และ BH8 ลดลง 1 หน่วย จะทำให้สภาพปัญหาด้านการรักษาความมั่นคงปลอดภัยสารสนเทศลดลง .466, .073 และ .167 ตามลำดับ

สมมติฐานที่ 2

H_2: พฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศมีอิทธิพลต่อแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

ตารางที่ 2 การวิเคราะห์ถดถอยพหุคูณเพื่อพยากรณ์อิทธิพลพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศต่อแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

พฤติกรรม	b	SE_b	**β**	t	p-value
BH2	.067	.031	.107	2.160	.031
BH3	.131	.026	.267	4.984	.000
BH6	-.163	.024	.188	3.292	.001
BH7	.078	.023	-.319	-6.976	.000
BH8	.137	.021	.317	6.538	.000

ค่าคงที่ =4.707; SE_{est} = ±.5446

R=.666; R^2=.443; F=59.515; p-value=.000

จากตารางที่ 2 แสดงให้เห็นว่าพฤติกรรมปัจจุบันด้านความมั่นคงความปลอดภัยสารสนเทศ 5 ด้าน (BH2, BH3, BH6, BH7 และ BH8) มีอิทธิพลต่อแนวปฏิบัติโดยรวมด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ และสามารถพยากรณ์แนวปฏิบัติดังกล่าวได้ร้อยละ 44.3 (R^2=.443)โดยมีความคลาดเคลื่อนมาตรฐานในการพยากรณ์ที่ ±.5446 เมื่อพิจารณาค่า สัมประสิทธิ์การถดถอยของตัวพยากรณ์ พบว่า BH6 สามารถพยากรณ์แนวปฏิบัติโดยรวมด้านการรักษาความมั่นคงปลอดภัยสารสนเทศได้สูงสุด ดังสมการที่ 2

$$\widehat{\text{แนวปฏิบัติโดยรวม}} = 4.707 + .067BH2 + .131BH3 - .163BH6 + .078BH7 + .137BH8 \ldots\ldots\ldots (2)$$

จากสมการดังกล่าวอธิบายได้ว่า เมื่อพฤติกรรมด้านการรักษาความมั่นคงปลอดภัยสารสนเทศทั้ง 5 ด้าน มีค่าเป็น 0 จะมีแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่ระดับ 4.707 เมื่อ BH2, BH3, BH7 และ BH8 เพิ่มขึ้น 1 หน่วย จะทำให้แนวปฏิบัติด้านการักษาความมั่นคงปลอดภัยสารสนเทศดังกล่าวเพิ่มขึ้นไปในทิศทางเดียวกันที่ .067, .131, .078 และ .137 ตามลำดับ และถ้า BH6 ลดลง 1 หน่วย จะทำให้แนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศลดลง .167 หน่วย

สมมติฐานที่ 3

H_3: สภาพปัญหาการรักษาความมั่นคงปลอดภัยสารสนเทศมีอิทธิพลต่อแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

ตารางที่ 3 การวิเคราะห์ถดถอยพหุคูณเพื่อพยากรณ์อิทธิพลของสภาพปัญหาเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศต่อแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

สภาพปัญหา	b	SE_b	**β**	t	p-value
PB2	.065	.029	.129	2.265	.024
PB3	.070	.026	.176	2.691	.007
PB6	-.069	.023	-.160	-3.012	.003
PB7	.138	.024	.334	5.834	.000
PB10	.117	.020	.289	5.829	.000

ค่าคงที่ =4.617; SE_{est} = ±.4681

R=.677; R^2=.445; F=51.560; p-value=.000

จากตารางที่ 3 จะเห็นว่าสภาพปัญหาด้านความมั่นคงปลอดภัยสารสนเทศของผู้ตอบแบบสอบถามทั้ง 5 ด้าน มีอิทธิพลต่อแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ สามารถพยากรณ์แนวปฏิบัติดังกล่าวได้ร้อยละ 44.5 (R^2=.445) โดยมีความคลาดเคลื่อนมาตรฐานในการพยากรณ์ที่ ±.4681เมื่อพิจารณาค่าสัมประสิทธิ์การถดถอยพบว่า PB2 สามารถพยากรณ์แนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศได้สูงสุดอย่างมีนัยสำคัญทางสถิติ ดังสมการที่ 3

$$\widehat{\text{แนวปฏิบัติโดยรวม}} = 4.617 + .065PB2 + .070PB3 - .069PB6 + .138PB7 + .117PB10 \ldots\ldots\ldots (3)$$

จากสมการดังกล่าวอธิบายได้ว่าเมื่อสภาพปัญหาด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ 5 ด้าน มีค่าเป็น 0 จะมีแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่ระดับ 4.617 เมื่อ PB2, PB3, PB7 และ PB10 เพิ่มขึ้น 1 หน่วย จะทำให้แนวปฏิบัติด้านการักษาความมั่นคงปลอดภัยสารสนเทศดังกล่าวเพิ่มขึ้น .065, .070, .138 และ .117 หน่วย ตามลำดับและถ้า PB6 ลดลง 1 หน่วย จะทำให้แนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศลดลง .069

สรุปและอภิปรายผลการวิจัย

จากผลการทดสอบสมมติฐานพบว่าทั้ง 3 สมการ (ตัวแบบ) มีพฤติกรรมด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ(BH) จำนวน 5 ด้าน และมีสภาพปัญหาด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (PB) จำนวน 5 ด้านที่ถูกคัดเลือกเข้าสู่ตัวแบบการรักษาความมั่นคงปลอดภัยของกองบัญชาการกองทัพไทย ดังนี้

1) การปฏิบัติตามกฎระเบียบ ข้อบังคับด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (BH2)
2) การเข้ารับการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (BH3)
3) การสำรองข้อมูลไว้มากกว่า 1 ที่จัดเก็บ (BH6)
4) การใช้รหัสผ่านเข้าใช้เครื่องคอมพิวเตอร์ร่วมกันกับบุคคลอื่น (BH7)
5) การไม่แจ้งไปยังผู้รับผิดชอบงานด้านความมั่นคงปลอดภัยสารสนเทศเมื่อประสบกับภัยคุกคามบนเครื่องคอมพิวเตอร์ (BH8)
6) การขาดการควบคุมบัญชีอุปกรณ์และ/หรือหลักฐานด้านสารสนเทศ (PB2)
7) การไม่เข้มงวดในการใช้ระบบการพิสูจน์บุคคลก่อนเข้าใช้ระบบสารสนเทศของผู้ใช้ (PB3)
8) การไม่มีข้อมูลสำรองไว้ใช้ในกรณีเกิดเหตุการณ์ที่ไม่คาดคิด เช่น ภัยพิบัติธรรมชาติ หรือเกิดจากฝีมือมนุษย์ (PB6)

9) หน่วยงานไม่มีข้อกำหนดที่เป็นลายลักษณ์อักษรในการถ่ายโอนข้อมูล/สารสนเทศ (PB7)

10) การละเมิดลิขสิทธิ์ซอฟต์แวร์ (PB10)

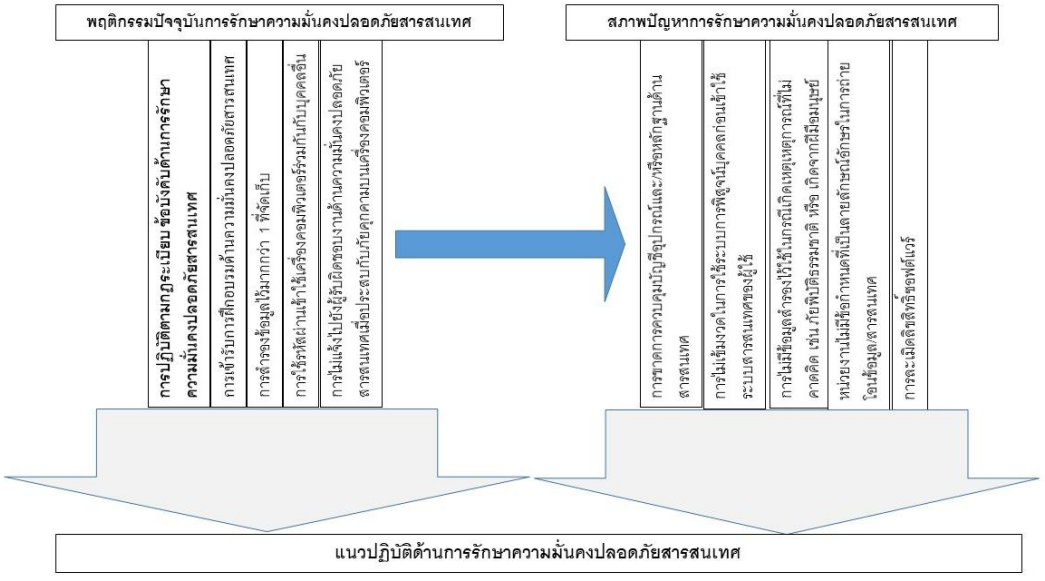
นอกจากนี้ ผลการทดสอบสมมติฐานยังเผยให้เห็นว่าพฤติกรรมเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศทั้ง 5 ด้านมีอิทธิพลต่อสภาพปัญหาด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอีกด้วย

ผลการวิจัยข้างต้นสอดคล้องกับข้อค้นพบของ Lampson (2004) ที่พบว่า การไม่ตระหนักหรือมองข้ามการรักษาความปลอดภัยสารสนเทศก่อให้เกิดปัญหาตามมา เช่น การถูกโจมตีระบบสารสนเทศหรือเครือข่าย การโจมตีมาจากทุกที่ทุกเวลาและอาจมาจากการแบ่งปันข้อมูลบนสื่ออินเทอร์เน็ตการติดไวรัส สภาพแวดล้อมด้านกายภาพสามารถเป็นภัยร้ายต่ออุปกรณ์หรือระบบสารสนเทศได้หากไม่มีความใส่ใจในการป้องกันและสอดคล้องกับงานวิจัยของ AbuSaad, Saeed, Alghathbar, and Khan (2011) ที่ว่า การไม่ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศก่อให้เกิดปัญหาด้านสารสนเทศ อาทิ การขาดการบริหารจัดการบัญชีควบคุมสิ่งอุปกรณ์ด้านสารสนเทศ การละเมิดการเข้าใช้โดยไม่ได้รับอนุญาต หรือแม้กระทั่งการไม่ตระหนักถึงความปลอดภัยด้านสารสนเทศ เหล่านี้ล้วนก่อให้เกิดความเสียหายต่อองค์กรได้ และยังสอดคล้องกับผลการวิจัยของ King (2000) ที่ว่าการละเมิดการรักษาความมั่นคงปลอดภัยสารสนเทศ และการไม่สำรองข้อมูลมากกว่า 1 ที่จัดเก็บก่อให้เกิดปัญหาในด้านการขาดแผนการรองรับเมื่อเกิดเหตุการณ์ฉุกเฉิน และ Brodie (2013) ชี้ว่าสิ่งสำคัญในการป้องกันปัญหาด้านสารสนเทศหรือภัยคุกคามนั้นขึ้นอยู่กับพฤติกรรมของบุคคลในองค์กร เพราะบุคคลเป็นทั้งผู้กำหนดแนวทางการรักษาความมั่นคงปลอดภัยและเป็นผู้ปฏิบัติตามนโยบายที่กำหนด

นอกจากนี้พฤติกรรมเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศทั้ง 5 ด้านยังมีอิทธิพลต่อแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอีกด้วยสอดคล้องกับผลการวิจัยของนักวิชาการหลายท่าน อาทิ การไม่ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศจะก่อให้เกิดปัญหาสารสนเทศในหลายด้านตามมา (Best, 2014) แนวปฏิบัติที่ดีคือการปฏิบัติตามกฎระเบียบความมั่นคงปลอดภัยสารสนเทศออย่างเคร่งครัด และมีบทลงโทษเมื่อกระทำผิด (Knapp, Marshall, Rainer, & Morrow, 2006) ระดับความรอบรู้และประสบการณ์มีผลต่อพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ (Blythe, Coventry, & Little, 2015) การขาดแผนการรองรับเมื่อเกิดภัยพิบัติที่ก่อความเสียหายแก่ข้อมูล รวมทั้งการขาดข้อมูลสำรองแม้ว่าจะพยายามกู้คืน แต่ผู้ประกอบการมีความสามารถไม่เพียงพอ (Ng, Ahmed, & Maynard, 2013) การขาดข้อกำหนดสิทธิ์ในการถ่ายโอนข้อมูลหรือเข้าใช้ระบบก่อให้เกิดความเสียหายต่อองค์กร (Alfawaz, Nelson, & Mohannak, 2010) การใช้ไฟล์ข้อมูลร่วมกันก่อให้เกิดความเสียหายแก่องค์กรได้ (Bojmeah, 2015) การตรวจสอบสิทธิ์การเข้าใช้งานระบบสารสนเทศขององค์กรเป็นปัญหาที่พบได้ในทุกหน่วยงานทั่วโลก (Loranger & Ingwalson, 2012) และสอดคล้องกับนโยบาย

การรักษาความมั่นคงปลอดภัยสารสนเทศ ที่คณะทำงานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สถาบันวิจัยแสงชินโครตรอน (คณะทำงานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ, 2559) ที่กำหนดให้องค์กรต้องจัดแหล่งเก็บข้อมูลสำรองอย่างเป็นรูปธรรมและมีหน่วยงานที่รับผิดชอบโดยเฉพาะ

จากข้อค้นพบตามที่กล่าวแล้วข้างต้น นำเสนอในรูปแบบแผนภาพได้ดังนี้



รูปที่ 2 แผนภาพตัวแบบการรักษาความมั่นคงปลอดภัยสารสนเทศ กองบัญชาการกองทัพไทย

ข้อเสนอแนะในการวิจัยครั้งต่อไป

ควรศึกษาเปรียบเทียบมาตรการสากลว่าด้วยการรักษาความมั่นคงปลอดภัยสารสนเทศต่างๆ ผ่านมุมมองผู้มีประสบการณ์จากหน่วยงานต่างๆ และควรศึกษาปัจจัยด้านอื่นๆ ที่นอกเหนือไปจากระดับความรอบรู้ พฤติกรรม และสภาพปัญหา เกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ เช่นงบประมาณ วัฒนธรรมองค์กร ยุทธศาสตร์องค์กรนโยบายการพัฒนาเศรษฐกิจแห่งชาติ

.....

เอกสารอ้างอิง

กรมกำลังพลทหาร กองบัญชาการกองทัพไทย. (2559). *หนังสือภายใน เรื่อง รายงานยอดกำลังพลประจำเดือน พ.ค. 59.*

กองรักษาความปลอดภัยสารสนเทศกองบัญชาการกองทัพไทย. (2559). *นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ กองบัญชาการกองทัพไทย พ.ศ.2559.* สืบค้น 12 มีนาคม 2560, จาก http://www.rtarf.mi.th/index.php/th/2016-06-23-07-36-482

คณะทำงานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ.(2559). *ประกาศ เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2559.* สืบค้น 12 มีนาคม 2560, จาก http://www.slri.or.th/th/index.php/aboutus/2012-07-16-03-51-01/corporate-website/it-contingency-plan.html

สำนักนายกรัฐมนตรี. (2550). *พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 (เล่ม 124 ตอนที่ 4 ก).* สืบค้น 14 มีนาคม 2560, จาก http://www.etda.or.th/content_files/2files/decree-defines-rules-procedures-electronic-government -transactions-2549.pdf

AbuSaad, B., Saeed, F. A., Alghathbar, K. & Khan, B. (2011). Implementation of ISO 27001 in Saudi Arabia–obstacles, motivations, outcomes, and lessons learned. *Proceedings of the 9th Australian Information Security Management Conference.* Perth: Edith Cowan University. doi: 10.4225/75b52709 cd8b2

Alfawaz, S., Nelson, K. & Mohannak, K. (2010). Information security culture: A Behaviour Compliance Conceptual Framework. *Proc. Proceedings of the 8th Australasian Information Security Conference (AISC 2010)*(pp.45-55). Brisbane, Australia. Retrieved March 17, 2017, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.664.1848&ep=rep1&type=pdf

Best, B. B. (2014). *Influencing employees' compliance behavior towards information security policy*. (Master's thesis). Netherlands: Maastricht School of Management. Retrieved April 18, 2017, from http://www.fhrinstitute.org/

Blythe, J. M., Coventry.L. & Little, L. (2015). Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. Proceedings of the *2015 Symposium on Usable Privacy and Security*. USENIX Association. Retrieved April 20, 2017, from https://www.usenix.org/sites/default/files/soups15_full_proceedings.pdf#page=125

Bojmaeh, H. Y. (2015). The Main Factors Influencing Information Security Behavior. *International Journal of Science and Engineering Applications,* 4(6), 353-356.

Brodie, C. (2009). The importance of information security awareness training. SANS Institute. Retrieved April 19, 2017, from https://www.sans.org/reading-room/whitepapers/awareness/importance-security-awareness-training-33013

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika,* 16(3), 297-334.

King, G. (2000). Best security practice: An overview. Proceedings of the *23rd National Information Systems Security Conference*. Retrieved May 18, 2017, from https://csrc.nist.gov/csrc/media/publications/conference-paper/2000/10/19/proceedings-of-the-23rd-nissc-2000/documents/papers/ 022.pdf

Knapp, K. J., Marshall, T. E., Rainer, R. K. & Morrow, D. W. (2006, September/October).The top information security issues facing organizations: what can government do to help? *Information Security and Risk Magazine, 51-58*. Retrieved from http://www.infosectoday.com/Articles/topissues.pdf

Lampson, W. B. (2004, June). *Computer security in the real world. IEEE Computer Society, 37-46.* Retrieved May 23, 2017, from https://www.cs.cornell.edu/courses/cs513/2005fa/NL02.Lampson.pdf

Likert, R. (1932). A Technique for the Measurement of Attitudes. *Archives of Psychology* (140), 1–55. Retrirved June 5, 2017, from https://legacy.voteview.com/pdf/Likert_1932.pdf

Loranger, P. & Ingwalson, R. (2012). IT Security:threats, vulnerabilities and countermeasures. Retrieved September 15, 2017, from https://ifap.ed.gov/presentations/attachments/30ITSecurityThreatsVulnerabilitiesandCountermeasuresV1.pdf

Ng, ZhiXian, Ahmed. A & Maynard, S. B. (2013). Information Security Management: Factors that influence security investments in SMES. Proceedings of the *11th Australian Information Security Management Conference, Churchlands: Edith Cowan University.* Retrieved September 16, 2017, from https://www.researchgate.net/__publication/264898154_Information_Security_Management_Factors_That_Influence_Security_Investments_in_SMEs

Pender-Bey, G. (2015). The Parkerian Hexad: The CIA expanded (Master's Thesis) Lewis University. Retrieved September 19, 2017, from http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf

The International Organization for Standardization and the International Organization for Standardization [ISO/IEC].(2013). *ISO/IEC 27001*: Information technology – security techniques – information security management systems – requirements.

Yamane, T. (1973).*Statistics: An introductory analysis*. (3rd ed.). NY: Harper and Row .