ความรู้ ความเข้าใจด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ
กรณีศึกษา: ข้าราชการ กองบัญชาการกองทัพไทย

ศรวัสย์ สนธิ

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชาเทคโนโลยีคอมพิวเตอร์และการสื่อสาร คณะวิศวกรรมศาสตร์
มหาวิทยาลัยธุรกิจบัณฑิตย์
พ.ศ. 2557

Knowledge and Understanding of Information Security Case Study: Govertment officer, Royal Thai Armed Forces Headquarters

Sorawat Sonti

A Thematic Paper Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science

Department of Computer and Communication Technology

Faculty of Engineering, Dhurakij Pundit University

2014

หัวข้อสารนิพนธ์ ความรู้ ความเข้าใจด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ
กรณีศึกษา: ข้าราชการ กองบัญชาการกองทัพไทย
ชื่อผู้เขียน ศรวัสย์ สนธิ
อาจารย์ที่ปรึกษา ผู้ช่วยศาสตราจารย์ ดร.วรพล พงษ์เพ็ชร
สาขาวิชา เทคโนโลยีคอมพิวเตอร์และการสื่อสาร
ปีการศึกษา 2556

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษาระดับความรู้ และพฤติกรรมด้านความเสี่ยงในการรักษาความมั่นคงปลอดภัยสารสนเทศ ของ กองบัญชาการกองทัพไทย

การเก็บข้อมูลรวบรวมจากกลุ่มตัวอย่างข้าราชการจำนวน 392 คน โดยใช้แบบสอบถาม ซึ่งได้แบ่งออกเป็น 5 ส่วน คือ ส่วนที่ 1 สอบถามถึงลักษณะข้อมูลส่วนบุคคล ส่วนที่ 2 พฤติกรรมการใช้คอมพิวเตอร์และเครือข่ายในกองบัญชาการกองทัพไทย ส่วนที่ 3 บททดสอบความรู้ด้านการรักษาความปลอดภัยสารสนเทศในแต่ละด้าน ส่วนที่ 4 การทดสอบพฤติกรรมเสี่ยงต่อภัยคุกคาม เช่น การเก็บรักษาและป้องกันข้อมูล กฎระเบียบ และข้อบังคับต่างๆ ส่วนที่ 5 ความคิดเห็นข้อเสนอแนะต่างๆ เพิ่มเติม โดยใช้โปรแกรม SPSS Statistics 17.0 เพื่อการรวบรวมวิเคราะห์ข้อมูลทางด้านสถิติ

การศึกษาครั้งนี้แสดงให้เห็นว่าการใช้งานคอมพิวเตอร์ตามปกติ ของกลุ่มตัวอย่างคือการค้นหาข้อมูลทางอินเทอร์เน็ต และพิมพ์งานด้านเอกสาร นอกจากนั้นยังพบว่าเจ้าหน้าที่ที่ผ่านการฝึกอบรมมาแล้ว จะมีความรู้ความเข้าใจในด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและพฤติกรรมความเสี่ยงด้านของข้อมูลต่างๆ ได้ดีกว่า เจ้าหน้าที่ที่ยังไม่ได้รับการฝึกอบรม แต่อย่างไรก็ตามก็ยังพบว่าเจ้าหน้าที่ส่วนมากจะไม่เข้าใจในเรื่องของข้อกำหนดกฎหมาย นโยบาย และมีพฤติกรรมความเสี่ยง ส่วนมากอาจเป็นเพราะว่าเจ้าหน้าที่จะต้องทำงาน เพื่อตอบสนองให้ทันต่อผู้บังคับบัญชาชั้นสูง

Thematic Paper Title	Knowledge and Understanding of Information Security Case Study: Govertment officer, Royal Thai Armed Forces Headquarters
Author	Sorawat Sonti
Thematic Paper Advisor	Asst.Prof. Dr.Worrapol Phongpech
Department	Computer and Communication Technology
Academic Year	2013

ABSTRACT

This research aims to study level of knowledge and behavior on information security of the Royal Thai Armed Forces Headquarters.

We have collected data from 392 government employees using questionnaire, which has been divided into five parts. The fisrt part is about the personal information, the second part is the general behavior once using computer or internet network, the third part is the knowledge testing of each field referring to the information security, while the fourth part is for the risk behavior testing such as the general information, the methodology of keeping information, the laws and policy, and others concerned regulations, and the fifth part is about the further comment and other required recommendation respectively. This study utilized SPSS Statstics 17.0, to statistical analysis the collected data.

The study shown that normal computer usage of these officers is to gather information over the internet, and to perform routine paper work. We have found that the trained officers, do have a better understaning of various information security risks than those untrained officers. However, it was also found that most officers do not have a solid grasp of the laws and policies involving hazardous behavior. Many officers have ignored these security policies such that they can respond promptly to the demand of the higher ranking officers.

กิตติกรรมประกาศ

งานค้นคว้าอิสระนี้ สำเร็จได้ด้วยความกรุณาจาก ผู้ช่วยศาสตราจารย์ ดร.วรพล พงษ์เพ็ชร รองคณะบดีฝ่ายวิชาการ และผู้อำนวยการหลักสูตรมหาบัณฑิต สาขาเทคโนโลยีคอมพิวเตอร์และการสื่อสาร คณะวิศวรรมศาสตร์ ที่ได้กรุณาให้คำปรึกษา แนะนำ ช่วยเหลือ และแก้ไขข้อบกพร่องต่าง ๆ ด้วยความเอาใจใส่อย่างดีมาโดยตลอด ทำให้งานศึกษานี้มีความสมบูรณ์มากยิ่งขึ้น ผู้ศึกษารู้สึกซาบซึ้งในความกรุณาของท่านเป็นอย่างยิ่งและขอกราบขอบพระคุณเป็นอย่างสูง

ขอขอบพระคุณ มหาวิทยาลัยธุรกิจบัณฑิตย์ ที่ได้มอบทุนการศึกษา ซึ่งทำให้ผู้ศึกษาได้มีโอกาสศึกษาในระดับปริญญาโท และขอขอบพระคุณ กองบัญชาการกองทัพไทย ที่ได้กรุณา ให้ความร่วมมือในการสนับสนุนข้อมูลต่าง ๆ ในการศึกษาและการเก็บข้อมูลอย่างดียิ่ง

สุดท้ายนี้ ผู้ศึกษาขอกราบขอบพระคุณ คุณบิดา มารดา ที่คอยเป็นกำลังใจให้สำเร็จการศึกษาในครั้งนี้ และขอขอบคุณ พ.อ.สุชาติ เว่บ้านแพ้ว เสธ.สทพ.นทพ. และเพื่อนร่วมงานที่ให้โอกาสในการทำวิจัยช่วยเหลือ ให้สำเร็จลุล่วงไปด้วยดี และขอขอบคุณ เลขาคณะ ที่ได้ให้การสนับสนุนติดต่อจัดการประสานงานทุก ๆ ด้าน และเป็นกำลังใจในการทำการศึกษาครั้งนี้มาโดยตลอด

ศรวัสย์ สนธิ

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญตาราง (ต่อ)

ตารางที่ **หน้า**

สารบัญภาพ

ภาพที่ **หน้า**

สารบัญภาพ (ต่อ)

ภาพที่ **หน้า**

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญของปัญหา

กองบัญชาการกองทัพไทย ได้มีการนำระบบสารสนเทศเข้ามาใช้ในองค์กร เพื่ออำนวย ความสะดวกในการบริหารจัดการข้อมูลระบบงานและ Email ภายในองค์กร มีทั้งระบบ Intranet และ Internet จึงทำให้ กองบัญชาการกองทัพไทย ได้นำมาตรฐานและแนวทางปฏิบัติงานนโยบาย ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ มาใช้ภายในองค์กร จากปัญหาที่พบภัยคุกคามในระบบสารสนเทศ ซึ่งเป็น ภัยคุกคาม ทางด้านต่างๆ ที่อาจเกิดจากบุคลากรภายในองค์กร ที่ขาดความรู้และความเข้าใจ ทางด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ เช่น บุคลากรติดตั้ง Software โดยไม่ได้รับอนุญาต Software ที่ไม่มี license เป็นที่มาของ Program ที่แอบแฝงมากับ Software ที่ติดตั้งได้ มีการนำ Email ภายนอกมาใช้ในการรับส่งข้อมูลข่าวสารแทนการใช้ Email ของทางราชการ ที่ได้กำหนด บุคลากรยังขาดการป้องกันในด้านการเข้าถึงข้อมูล โดยไม่ได้ใช้รหัสผ่านแสดงสิทธิ์ในการเข้าถึงข้อมูลของคอมพิวเตอร์ หรือมีการตั้งรหัสผ่านที่คาดเดาง่าย และจดบันทึกรหัสผ่านไว้กับโต๊ะที่ทำงาน เพื่อความสะดวกง่ายต่อการจดจำรหัสผ่านของตนเอง และมีการใช้ Internet ในการดูเว็บไซต์ หรือสื่อต่าง ๆ รวมทั้งดาวน์โหลดข้อมูลต่างๆ ที่มีความเสี่ยงต่อภัยคุกคาม โดยขาดความรู้และความเข้าใจ ซึ่งอาจแอบแฝงมากับเว็บบราวเซอร์หน้าเว็บไซต์นั่น ๆ

พฤติกรรมความเสี่ยงของบุคลากรดังกล่าว ทำให้ หน่วยงานผู้รับผิดชอบ ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ตรวจค้นพบไวรัส (Viruses) เวิร์ม (Worms) โทรจันฮอร์ส (Trojan horse) สปายแวร์ (Spyware) แบ็คดอร์ (Backdoors) ในระบบของ กองบัญชาการกองทัพไทย เป็นปัญหาที่มาของบุคลากร ที่ขาดความรู้และความเข้าใจ ในด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ตามนโยบายที่ กองบัญชาการกองทัพไทย กำหนด

จากปัญหาเกี่ยวกับความรู้และความเข้าใจของบุคลากรอาจจะเป็นพฤติกรรมความเสี่ยงในด้านสารสนเทศ และรวมไปถึงการใช้งานอุปกรณ์ติดต่อสื่อสารที่นำมาเชื่อมต่อใช้ภายในองค์กร ก็เกิดความเสี่ยงต่อองค์กรได้ ซึ่งบุคลากรอาจละเลยในการใส่ใจ ความรู้และความเข้าใจ ในด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ จึงเป็นช่องโหว่ขององค์กรได้

ดังนั้นผู้วิจัยจึงมีความสนใจที่จะศึกษาถึง ความรู้และความเข้าใจของบุคลากรที่มีต่อการรักษาความมั่นคงปลอดภัยสารสนเทศของ กองบัญชาการกองทัพไทย เพื่ออยากทราบว่าบุคลากรใน กองบัญชาการกองทัพไทย มีความรู้ และความเข้าใจ ทางด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ภายในกองบัญชาการกองทัพไทย มากน้อยเพียงใดอย่างไร อีกทั้งผลงานวิจัยของผู้จัดทำนี้อาจเป็นประโยชน์ต่อผู้ที่สนใจศึกษาต่อไป

1.2 วัตถุประสงค์ของการวิจัย

วัตถุประสงค์ของการวิจัย มีดังต่อไปนี้

1) เพื่อศึกษาพฤติกรรมการใช้อินเตอร์เน็ตภายในองค์กรของ กองทัพไทย ในการติดต่อสื่อสารภายนอกปัจจัยความเสี่ยงต่าง ๆ ในด้านสารสนเทศ

2) เพื่อศึกษาแนวทางและวิธีการป้องกันการรักษาความปลอดภัยสารสนเทศ ของข้าราชการ กองทัพไทย

3) เพื่อศึกษาแนวทางการจัดการฝึกอบรมให้กับบุคลากรของ กองทัพไทย ให้มีความรู้ความสามารถในการรักษาความปลอดภัยเบื้องต้น เป็นไปตามกฎระเบียบของ กองทัพไทย

4) เพื่อรับทราบความคิดเห็นเสนอแนะต่าง ๆ ของข้าราชการ กองทัพไทย

1.3 ขอบเขตของการวิจัย

ศึกษาเฉพาะพฤติกรรมการใช้อินเตอร์เน็ตเพื่อการเชื่อมโยงสื่อสารภายนอก กองทัพไทย ปัญหาด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ และความรู้ความเข้าใจเกี่ยวกับ การรักษาความมั่นคงปลอดภัยสารสนเทศ ข้าราชการของ กองทัพไทย จำนวน 18,519 นาย กลุ่มตัวอย่างที่ใช้ในการศึกษาครั้งนี้ ได้แก่ นายทหารชั้นสัญญาบัตร จำนวน 123 นาย นายทหารชั้นประทวน จำนวน 211 นาย และลูกจ้างพนักงาน จำนวน 58 นาย รวมทั้งสิ้น 392 นาย เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูลได้แก่ แบบสอบถามประมวลผลด้วยโปรแกรมสำเร็จรูป SPSS และวิเคราะห์ข้อมูลโดยการแจกแจงความถี่ ค่าร้อยละ และค่าเฉลี่ย โดยศึกษาในช่วงเดือนมีนาคม 2557 - พฤษภาคม 2557

1.4 ประโยชน์ที่คาดว่าจะได้รับ

ประโยชน์ที่คาดว่าจะได้รับมีดังต่อไปนี้

1) เพื่อนำผลจากการศึกษาไปใช้ในการแก้ไขปัญหาควบคุมกำกับดูแลด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศ ของ กองทัพไทย ให้ตรงตามวัตถุประสงค์ได้ดียิ่งขึ้น

2) เพื่อนำผลจากการศึกษาไปใช้เป็นข้อมูลพื้นฐานในการเพิ่มเติมหลักสูตรการฝึกอบรมการรักษาความมั่นคงปลอดภัยสารสนเทศ ของ กองทัพไทย ต่อไป

3) นำผลที่ได้จากการวิจัยนี้ไปใช้ในการออก กฎระเบียบ นโยบาย เพื่อให้สอดคล้องกับแนวทางการป้องกันกำลังพลในเรื่อง การรักษาความมั่นคงปลอดภัยสารสนเทศ ได้ตรงตามวัตถุประสงค์ ของ กองทัพไทย เพื่อให้เป็นแนวทางป้องกันที่ถูกต้อง

4) เพื่อเป็นแนวทางอันเป็นประโยชน์ในการศึกษาเกี่ยวกับการใช้ข้อมูลด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ของ กองทัพไทย ด้านอื่น ๆ ต่อไป

บทที่ 2
แนวคิด ทฤษฎี และผลงานวิจัยที่เกี่ยวข้อง

การศึกษาครั้งนี้มุ่งศึกษาวิเคราะห์ความรู้และความเข้าใจของบุคลากรใน กองบัญชาการกองทัพไทย เกี่ยวกับพฤติกรรม ความเสี่ยง และความรู้ความเข้าใจ ของบุคลากรในการใช้ระบบงานสารสนเทศ ว่ามีพฤติกรรมความเสี่ยงต่อภัยคุกคามในการใช้ระบบงานสารสนเทศของ กองบัญชาการกองทัพไทย มากน้อยเพียงไร มีความเสี่ยงมากแค่ไหน และไปในทิศทางด้านใด เพื่อนำผลประโยชน์ที่ได้รับสำหรับข้อมูลนี้ ไปจัดการฝึกอบรมเจ้าหน้าที่ในการรักษาความมั่นคงปลอดภัยสารสนเทศ บุคลากร ของ กองบัญชาการกองทัพไทย ต่อไป เพื่อพัฒนาหลักสูตรให้ตรงกับกลุ่มเป้าหมาย และขอบเขตความรู้ ความเข้าใจ ที่บุคลากร ใน กองบัญชาการกองทัพไทย ต้องการรู้เพิ่มเติม และความคิดเห็นต่าง ๆ เพื่อที่เป็นแนวทางให้กับ กองรักษาความปลอดภัยสารสนเทศ ผู้รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ นำข้อมูลที่ได้ไปศึกษาและอุดช่องโหว่ ด้านบุคลกร ใน กองบัญชาการกองทัพไทย ผู้จัดทำได้รวบรวมทฤษฎีและความรู้ ความเข้าใจในด้านต่าง ๆ เกี่ยวกับงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ รวบรวมข้อมูลจากการศึกษาทฤษฎี ทบทวนวรรณกรรม รวมถึงการค้นคว้าเอกสารทางวิชาการที่เกี่ยวข้องกับงานที่ทำการศึกษาโดยสรุปเป็นหัวข้อต่างๆ ดังนี้

แนวคิดทางทฤษฎีที่เกี่ยวข้อง

1) แนวคิดทฤษฎีเรื่องความรู้ (Knowledge) และความเข้าใจ (Understanding)

2) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

3) แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร ของ กองทัพไทย พ.ศ.2553 – 2556

4) ระเบียบ กองบัญชาการทหารสูงสุด ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของ กองทัพไทย พ.ศ. 2547

5) ทฤษฎีความปลอดภัยคอมพิวเตอร์

บทความและงานวิจัยที่เกี่ยวข้อง

1) บทความและงานความมั่นคงปลอดภัยสารสนเทศ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยฟาร์อีสเทอร์น

2) บทความภัยคุกคามความมั่นคงระบบสารสนเทศ ของ พ.อ.รศ.ดร.เศรษฐพงค์ มะลิสุวรรณ พ.ศ. 2552

3) ภัยคุกคาม ช่องโหว่ และการโจมตี ของ มหาวิทยาลัยฟาร์อิสเทอร์น

4) ผลงานวิจัยที่เกี่ยวกับพฤติกรรมการใช้สังคมออนไลน์เวลาจริงของนักศึกษาปริญญาตรีมหาวิทยาลัยธุรกิจบัณฑิตย์ ของนักศึกษา สุพรรษา เกษสีแก้ว จาก มหาวิทยาลัยธุรกิจบัณฑิตย์ ปีการศึกษา 2552

5) ผลงานวิจัยที่เกี่ยวกับ ความรู้ ทัศนคติต่อพฤติกรรมด้านความปลอดภัยของพนักงานอู่ทหารเรือ พระจุลจอมเกล้า กรมอู่ทหารเรือ กรณีศึกษา : ในสายงานฝ่ายผลิต ของนักศึกษา ศิริพงศ์ ศรีสุขกาญจน์ จากมหาวิทยาลัย ธุรกิจบัณฑิตย์ ปีการศึกษา 2553

6) ผลงานวิจัยที่เกี่ยวกับการใช้ประโยชน์และความพึงพอใจต่อระบบอินทราเน็ตเพื่อการสื่อสารภายในองค์กร กรณีศึกษา : ข้าราชการโรงพยาบาลพระมงกุฎเกล้า ของนักศึกษา วรรณษา บุนนาค จาก มหาวิทยาลัยธุรกิจบัณฑิตย์ ปีการศึกษา 2554

7) ผลงานวิจัยที่เกี่ยวกับความรู้ความเข้าใจในความปลอดภัยของข้อมูลส่วนบุคคลทางระบบคอมพิวเตอร์ กรณีศึกษาในเขต กรุงเทพมหานคร ของนักศึกษา นวรัตน์ พัฒโนทัย จาก มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี ปีการศึกษา 2555

8) ผลงานวิจัยที่เกี่ยวกับการวิเคราะห์ความคุ้มทุนและประโยชน์ที่ชุมชนได้รับในการจัดตั้งศูนย์การเรียนรู้ ICT ชุมชน กรณีศึกษา ศูนย์การเรียนรู้ ICT ชุมชนตำบลบางเพรียง อำเภอบางบ่อ จังหวัดสมุทรปราการ ของนักศึกษา ปิยะนาถ คล่องดี จาก มหาวิทยาลัยธุรกิจบัณฑิตย์ ปีการศึกษา 2556

2.1 แนวคิดทางทฤษฎีที่เกี่ยวข้อง

ทฤษฎีเรื่องความรู้ (Knowledge) และความเข้าใจ (Understanding)

ความรู้ เป็นการรับรู้เบื้องต้น ซึ่งบุคคลส่วนมากจะได้รับผ่านประสบการณ์ โดยการเรียนรู้จากการตอบสนองต่อสิ่งเร้า (S-R) แล้วจัดระบบเป็นโครงสร้างของความรู้สร้างสรรค์ให้ระหว่างความจำ (ข้อมูล) กับสภาพจิตวิทยา ด้วยเหตุนี้ ความรู้ จึงเป็นความจำเป็นที่สร้างสรรค์ให้สอดคล้องกับสภาพจิตใจของตนเอง ความรู้จึงเป็นกระบวนการภายใน อย่างไรก็ตามความรู้ก็อาจส่งผลต่อพฤติกรรมที่แสดงออกของมนุษย์ได้ (สุรพงษ์ โสธนะเสถียร, 2553, น. 120)

ความรู้เป็นพฤติกรรมเบื้องต้นที่ผู้เรียนสามารถจดจำได้ หรือระลึกได้โดยการมองเห็น หรือได้ยิน ซึ่งความรู้ในที่นี้ คือ ข้อเท็จจริง กฎเกณฑ์ คำจำกัดความ เป็นต้น โดยทั้งนี้ความรู้จึงเป็นพฤติกรรมขั้นต้นที่คนเราเพียงแต่จำได้โดยนึกได้ ความรู้ขั้นนี้ ได้แก่ ความรู้เกี่ยวกับคำจำกัดความ ความหมาย ข้อเท็จจริง กฎโครงสร้าง และวิธีการแก้ปัญหา ดังนั้นอาจกล่าวรวม ๆ ได้ว่า ความรู้หมายถึง การเรียนรู้ที่เน้นความจำและการระลึกถึงได้ของคนเราที่มีความคิด ปรากฏการณ์หรือวัตถุต่าง ๆ ความจำนี้อาจจะเริ่มจากสิ่งที่ง่ายไม่ซับซ้อนไปจนถึงเรื่องยุ่งยากซับซ้อนหลายขั้นได้ (สุตชาติ วงษ์หุ่น, 2539, น. 28)

ความเข้าใจ หมายถึง เป็นขั้นตอนของความรู้ (Knowledge) ขั้นตอนนี้จะต้องใช้ความสามารถทางสมอง และทักษะที่สูงขึ้นจนถึงกับที่สื่อความหมาย ซึ่งมักเกิดขึ้นหลักจากที่บุคคลได้รับข่าวสารต่าง ๆ และความเข้าใจนี้เองจะแสดงออกในรูปของทักษะต่าง ๆ ซึ่งแยกได้เป็น 3 ลักษณะ ดังนี้ (อรรวรรณ ปิลันธน์โอวาท, 2549, น. 40)

1) การแปลความหมาย หมายถึง เป็นการจับใจความให้ถูกต้องเกี่ยวกับสิ่งที่สื่อความหมายหรือภาษาหนึ่งของการสื่อสารไปสู่อีกรูปแบบหนึ่ง

2) การตีความหมาย หมายถึง เป็นการอธิบายความหมายหรือสรุปเรื่องราว โดยการจัดระเบียบใหม่ รวบรวมเรียบเรียงเนื้อหาใหม่

3) การขยายความ เป็นการขยายเนื้อหาที่เหนือไปกว่าขอบเขตที่รู้เป็นการขยายขีดการอ้างอิงหรือแนวโน้มที่เกินเลยจากข้อมูล

Rosenberg and Hovland (1960, p. 4) อธิบายความหมายของ การเข้าใจ ไว้ว่า ความรับรู้ ความนึกคิด และความเชื่อ ตามแนวทัศนคติ ซึ่งสิ่งเหล่านี้สามารถแสดงออกมาได้ โดยคำถามที่อยู่ในรูปการพิมพ์หรือคำพูด เช่น ถ้าผู้ที่สนใจอยากรู้ว่าประชาชนมีความเข้าใจและมีทัศนคติต่อเรื่องใด ๆ ผู้นั้นสามารถสำรวจความคิดเห็นได้ โดยการสัมภาษณ์ หรือกรอกแบบสอบถามได้ เป็นต้น

Bertrang Russell (1926) ได้ให้ความหมายของความรู้ ซึ่งหมายถึง อาจกำหนดไว้ให้เชื่อสิ่งที่อยู่ในข้อตกลงกับข้อเท็จจริง แต่ปัญหาคือการที่ไม่มีใครรู้ในสิ่งที่เชื่อ คือ ไม่มีผู้ใดรู้สิ่งที่เป็นจริงและไม่มีผู้ใดรู้ในสิ่งที่จัดเรียงไว้ตามข้อตกลง

Bloom el al. (1956, PP.28-80) ได้ให้คำนิยามว่า

ความรู้ (Knowledge) เป็นสิ่งที่เกี่ยวข้องกับการระลึกถึงเฉพาะเรื่องหรือเรื่องทั่ว ๆ ไป ระลึกถึงวิธี กระบวนการหรือสถานการณ์ต่าง ๆ โดยเน้นความจำและการเกิดความรู้ไม่ว่าระดับใดย่อมมีความสัมพันธ์กับความรู้สึก ซึ่งส่งผลให้เชื่อมโยงกับสภาพจิตใจของบุคคล โดยปัจจัยที่ทำให้ส่งผลนี้ คือ สภาพแวดล้อม ประสบการณ์ที่สะสม จึงทำให้แสดงออกต่อการกระทำของบุคคล

ความเข้าใจ (Comprehension Or Understand) หมายถึง บุคคลสามารถทำบางสิ่งบางอย่างได้มากกว่าข้อมูลที่ได้รับ สามารถเขียนเรียบเรียงใหม่ พร้อมแสดงความคิดเห็นเพิ่มเติมแปลความเปรียบเทียบความเห็นอื่น ๆ หรือคาดผลของเหตุการณ์ที่จะเกิดได้เป็นพฤติกรรมในขั้นที่ต่อจากความรู้ เป็นขั้นตอนที่สมอง และความสามารถของทักษะ ได้เข้ามาเกี่ยวข้องด้วย จะส่งผลต่อการสื่อสารตีความ แปลความ ขยายความของเหตุเหล่านั้นที่สัมพันธ์กันอีกระดับหนึ่ง โดยความรู้ต้องเกิดจากข้อมูลหรือประสบการณ์ที่เพียงพอ ดังนั้น ความรู้ สามารถกล่าวได้ว่าเป็นการวัดความรู้และความเข้าใจไปด้วยกัน

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ จึงมีผู้ไม่หวังดีเกิดขึ้นอย่างแน่นอน โดยการกระทำใด ๆ ให้ระบบคอมพิวเตอร์ไม่สามารทำงานหรือให้ทำงานผิดพลาด ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคง สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว ประเทศไทยจึงมีการออกพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ขึ้นมาโดยมีบทลงโทษดังนี้

มาตรา 5 ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจาคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 6 ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้ อื่นจัดทาขึ้นเป็นการเฉพาะถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นต้องระวางโทษจาคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 7 ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ

มาตรา 8 ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ตองระวางโทษจาคุกไม่เกินสามปีหรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 9 ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมด หรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาทหรือทั้งจำทั้งปรับ

มาตรา 10 ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจาคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา 11 ผู้ใดส่งข้อมูลคอมพิวเตอร์ หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา 12 หากมีการกระทำความผิดตาม มาตรา 9 หรือมาตรา 10

1) ก่อให้เกิดความเสียหายแก่ประชาชนเกิดขึ้นทันทีหรือภายหลัง ต้องระวางโทษปรับไม่เกินสองแสนบาท หรือต้องระวางโทษจำไม่เกิน 10 ปี

2) น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศและเศรษฐกิจ ต้องระวางโทษจำคุกตั้งแต่สามปี ถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

3) ถ้าการกระทำความผิดตาม 2) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่สิบปี ถึงยีสิบปีมาตรา 13 ผู้ใดจำหน่ายหรือเผยแพร่ ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 มาตรา 9 มาตรา 10 หรือมาตรา 11 ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 14 ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

1) นำเข้าสู่ ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วนหรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

2) นำเข้าสู่ ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนักแก่ประชาชน

3) นำเข้าสู่ ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็น ความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

4) นำเข้าสู่ ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์ นั้นประชาชนทั่วไปอาจเข้าถึงได้

5) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม 1) 2) 3) หรือ 4)

มาตรา 15 ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14

มาตรา 16 ผู้ใดนำเข้าสู่ ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ ถ้าการกระทำตามวรรคหนึ่ง เป็นการนำเข้าข้อมูลคอมพิวเตอร์ โดยสุจริต ผู้กระทำไม่มีความผิด ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้ ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

มาตรา 17 ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ

1) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษหรือ

2) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหายและผู้เสียหายได้ร้องขอให้ลงโทษ จะต้องรับโทษภายในราชอาณาจักร

แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร ของ กองทัพไทย พ.ศ.2553 – 2556

แผนแม่บทการปฏิบัติการต่อเครือข่ายคอมพิวเตอร์ กองทัพไทย เป็นการเริ่มต้นในการกำหนดกรอบ แนวทางในการปฏิบัติ เพื่อให้ทุกส่วนราชการสามารถที่จะแลกเปลี่ยนข้อมูลและปฏิบัติงานด้านการปฏิบัติการต่อเครือข่ายคอมพิวเตอร์ ร่วมกันได้อย่างมีประสิทธิภาพ ซึ่งเป็นไปตามแผนแม่บท การปฏิบัติการต่อเครือข่ายต่อคอมพิวเตอร์ จำเป็นอย่างยิ่งในการทำให้การแลกเปลี่ยนข้อมูลระหว่าง ส่วนราชการ บก.กองทัพไทย กองทัพบก กองทัพเรือ และกองทัพอากาศ มีความปลอดภัย และเชื่อถือได้ ดังนั้นจึงมีความจำเป็นที่ต้องอาศัยความร่วมมือจากบุคลากร ในทุกระดับ โดยจะต้องยึดถือและปฏิบัติตาม กฎ ระเบียบ ข้อบังคับ ต่างๆ ที่เกี่ยวข้องกับการรักษาความปลอดภัยด้านสารสนเทศ และระเบียบอื่นๆ ที่เกี่ยวข้อง อย่างเคร่งครัด

จุดมุ่งหมายของแผนแม่บทเพื่อให้ส่วนราชการ บก.กองทัพไทย กองทัพบก กองทัพเรือ กองทัพอากาศ ยึดถือเป็นแนวทางในการปฏิบัติต่อเครือข่ายคอมพิวเตอร์ ตามหลักนิยมการปฏิบัติการข่าวสาร กองทัพไทย

วัตถุประสงค์ เพื่อให้ข้าราชการ บก.กองทัพไทย กองทัพบก กองทัพเรือ และกองทัพอากาศ มีจิตสำนึกในการรักษาความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้ส่วนราชการ บก.กองทัพไทย กองทัพบก กองทัพเรือ และกองทัพอากาศ มีแนวทางในการดำเนินงานเกี่ยวกับการปฏิบัติการเครือข่ายคอมพิวเตอร์ ที่เป็นรูปธรรมและสามารถวัดผลการปฏิบัติได้ เพื่อให้ระบบเครือข่ายคอมพิวเตอร์ ของ ส่วนราชการ บก.กองทัพไทย กองทัพบกกองทัพเรือ และกองทัพอากาศ มีความปลอดภัยจากภัยคุกคาม สามารถปฏิบัติงานตลอดเวลารวมทั้งสนับสนุนการปฏิบัติการทางทหารได้อย่างมีประสิทธิภาพ

ระเบียบ กองบัญชาการทหารสูงสุด ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของ กองทัพไทย พ.ศ.2547

ระเบียบนี้ให้ใช้บังคับแก่ส่วนราชการ ข้าราชการ และลูกจ้าง ที่มีการปฏิบัติเกี่ยวกับระบบสารสนเทศ รวมทั้งบุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศ ของกองบัญชาการทหารสูงสุด และเหล่าทัพ

ความมุ่งหมายของระเบียบนี้ เพื่อกำหนดหลักการและมาตรการในการรักษาความปลอดภัยระบบสารสนเทศ ของกองทัพไทย พิทักษ์รักษาและป้องกัน มิให้ข้อมูลและสิ่งที่เป็นความลับของทางราชการ รั่วไหลหรือรู้ไปถึง หรือตกไปอยู่ในมือของฝ่ายตรงข้ามหรือบุคคลผู้ไม่มีอำนาจหน้าที่ป้องกันการจารกรรมทั้งจากบุคคลภายในและภายนอกส่วนราชการ พิทักษ์รักษาและป้องกันการก่อวินาศกรรม แก่ เครื่องจักรคำนวณ อุปกรณ์ เครื่องใช้ อาคาร สถานที่ และเอกสาร เป็นต้น หัวหน้าส่วนราชการสามารถกำหนดมาตรการรักษาความปลอดภัยให้ระบบสารสนเทศของส่วนราชการ และแต่งตั้งเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยระบบสารสนเทศ ของ ส่วนราชการเพิ่มเติมได้โดยให้สอดคล้อง และไม่ขัด หรือ แย้งกับระเบียบนี้

เหตุผลในการประกาศใช้ระเบียบนี้ คือ วางระเบียบ กองบัญชาการทหารสูงสุด ในการรักษาความปลอดภัยระบบสารสนเทศของกองทัพไทย เกี่ยวกับระบบคอมพิวเตอร์ ระบบสื่อสาร สารสนเทศเครือข่ายระบบสารสนเทศ เพื่อให้ใช้บังคับแก่ส่วนราชการ ข้าราชการ และลูกจ้าง ที่มีการปฏิบัติเกี่ยวกับระบบสารสนเทศ รวมทั้งบุคคลภายนอก ที่เข้ามาดำเนินการ เกี่ยวกับระบบสารสนเทศ ของ กองบัญชาการทหารสูงสุด และเหล่าทัพ ในการกำหนดชั้นความลับของสารสนเทศให้เป็นไปตาม พรบ. ข้อมูลข่าวสาร ของ ทางราชการ พ.ศ.๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ หรืออื่น ๆ ที่ได้ประกาศใช้ทดแทน

1) การรักษาความปลอดภัยเกี่ยวกับบุคคล

2) การรักษาความปลอดภัย สถานที่

3) การรักษาความปลอดภัยระบบสารสนเทศ

4) การรักษาความปลอดภัยในการพัฒนาระบบสารสนเทศ

5) การปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ

ทฤษฎีความมั่นคงปลอดภัยสารสนเทศ

สารสนเทศ (information) เป็นผลลัพธ์ของการประมวลผล การจัดดำเนินการ และการเข้าประเภทข้อมูลโดยการรวมความรู้เข้าไปต่อผู้รับสารสนเทศนั้น สารสนเทศ มีความหมายหรือแนวคิดที่กว้าง และหลากหลาย ตั้งแต่การใช้คำว่าสารสนเทศ ในชีวิตประจำวัน จนถึงความหมายเชิงเทคนิค ตามปกติในภาษาพูด แนวคิดของสารสนเทศใกล้เคียงกับความหมายของการสื่อสาร

ความมั่นคงปลอดภัยของสารสนเทศคืออะไร

1) ความมั่นคงปลอดภัย (Security) คือ สถานะที่มีความปลอดภัย ไร้กังวลอยู่ในสถานะที่ไม่มีอันตรายและได้รับการป้องกันจากภัยอันตรายทั้งที่เกิดขึ้นโดยตั้งใจหรือบังเอิญ

2) การรักษาความปลอดภัยทางข้อมูล Information Security คือ ผลที่เกิดขึ้นจากการใช้ระบบของนโยบายและ/หรือ ระเบียบปฏิบัติที่ใช้ในการพิสูจน์ทราบ ควบคุม และป้องกันการเปิดเผยข้อมูล (ที่ได้รับคำสั่งให้มีการป้องกัน) โดยไม่ได้รับอนุญาต : นิยามโดย ThaiCERT (ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย)

2.2 บทความและงานวิจัยที่เกี่ยวข้อง

บทความและงานความมั่นคงปลอดภัยสารสนเทศ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยฟาร์อีสเทอร์น

ความมั่นคงปลอดภัยขององค์กร

1) ความมั่นคงปลอดภัยทางกายภาย Physical Security

2) ความมั่นคงปลอดภัยส่วนบุคคล Personal Security

3) ความมั่นคงปลอดภัยในการปฏิบัติงาน Operations Security

4) ความมั่นคงปลอดภัยในการติดต่อสื่อสาร Communication Security

5) ความมั่นคงปลอดภัยของเครือข่าย Network Security

6) ความมั่นคงปลอดภัยของสารสนเทศ Information Security

แนวคิดหลักของความมั่นคงปลอดภัยของสารสนเทศ

กลุ่มอุตสาหกรรมความมั่นคงปลอดภัยของคอมพิวเตอร์ ได้กำหนดแนวคิดหลักของความมั่นคงปลอดภัยของคอมพิวเตอร์ขึ้นประกอบด้วย

1) ความลับ Confidentiality

2) ความสมบูรณ์ Integrity

3) ความพร้อมใช้ Availability

4) ความถูกต้องแม่นยำ Accuracy

5) เป็นของแท้ Authenticity

6) ความเป็นส่วนตัว Privacy

ความลับ Confidentiality เป็นการรับประกันว่าผู้มีสิทธิ์และได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้ องค์กรต้องมีมาตรการป้องกันการเข้าถึงสารสนเทศที่เป็นความลับ เช่น การจัดประเภทของสารสนเทศ การรักษาความปลอดภัยในกับแหล่งจัดเก็บข้อมูล กำหนดนโยบายรักษาความมั่นคงปลอดภัย และนำไปใช้ให้การศึกษาแก่ทีมงานความมั่นคงปลอดภัยและผู้ใช้ ภัยคุกคามที่เพิ่มมากขึ้นในปัจจุบัน มีสาเหตุมาจากความก้าวหน้าทางเทคโนโลยี ประกอบกับความต้องการความสะดวกสบายในการสั่งซื้อสินค้าของลูกค้า โดยการยอมให้สารสนเทศส่วนบุคคลแก่ website เพื่อสิทธิ์สนการทำธุรกรรมต่าง ๆ โดยลืมไปว่าเว็บไซต์ เป็นแหล่งข้อมูลที่สามารถขโมยสารสนเทศไปได้ไม่ยากนัก

ความสมบูรณ์ Integrity ความสมบูรณ์ คือ ความครบถ้วน ถูกต้อง และไม่มีสิ่งแปลกปลอม สารสนเทศที่มีความสมบูรณ์จึงเป็นสารสนเทศที่นำไปใช้ประโยชน์ได้อย่างถูกต้องครบถ้วน สารสนเทศจะขาดความสมบูรณ์ ก็ต่อเมื่อสารสนเทศนั้นถูกนำไปเปลี่ยนแปลง ปลอมปนด้วยสารสนเทศอื่น ถูกทำให้เสียหาย ถูกทำลาย หรือถูกกระทำในรูปแบบอื่น ๆ เพื่อขัดขวางการพิสูจน์การเป็นสารสนเทศจริง

ความพร้อมใช้ Availability ความพร้อมใช้ หมายถึง สารสนเทศจะถูกเข้าถึงหรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้หรือระบบอื่นที่ได้รับอนุญาตเท่านั้นหากเป็นผู้ใช้หรือระบบที่ไม่ได้รับอนุญาต การเข้าถึงหรือเรียกใช้งานจะถูกขัดขวางและล้มเหลวในที่สุด

ความถูกต้องแม่นยำ Accuracy หมายถึง สารสนเทศต้องไม่มีความผิดพลาด และต้องมีค่าตรงกับความคาดหวังของผู้ใช้เสมอ เมื่อใดก็ตามที่สารสนเทศมีค่าผิดเพี้ยนไปจากความคาดหวังของผู้ใช้ ไม่ว่าจะเกิดจากการแก้ไขด้วยความตั้งใจหรือไม่ก็ตาม เมื่อนั้นจะถือว่าสารสนเทศ “ไม่มีความถูกต้องแม่นยำ”

ความเป็นของแท้ Authenticity คือ สารสนเทศที่ถูกจัดทำขึ้นจากแหล่งที่ถูกต้อง ไม่ถูกทำซ้ำโดยแหล่งอื่นที่ไม่ได้รับอนุญาต หรือแหล่งที่ไม่คุ้นเคยและไม่เคยทราบมาก่อน

ความเป็นส่วนตัว Privacy คือ สารสนเทศที่ถูกรวบรวม เรียกใช้ และจัดเก็บโดยองค์กรจะต้องถูกใช้ในวัตถุประสงค์ที่ผู้เป็นเข้าของสารสนเทศรับทราบ ณ ขณะที่มีการรวบรวมสารสนเทศนั้นมิฉะนั้นจะถือว่าเป็นการละเมิดสิทธิส่วนบุคคลด้านสารสนเทศ

องค์ประกอบของระบบสารสนเทศกับความมั่นคงปลอดภัย

1) Software ย่อมต้องอยู่ภายใต้เงื่อนไขของการบริหารโครงการ ภายใต้เวลา ต้นทุนและกำลังคนที่จำกัด ซึ่งมักจะทำภายหลังจากการพัฒนาซอฟต์แวร์เสร็จแล้ว

2) Hardware จะใช้นโยบายเดียวกับสินทรัพย์ที่จับต้องได้ขององค์กร คือการป้องกันจากการลักขโมยหรือภัยอันตรายต่าง ๆ รวมถึงการจัดสถานที่ที่ปลอดภัยให้กับอุปกรณ์หรือฮาร์ดแวร์

3) Data ข้อมูล/สารสนเทศ เป็นทรัพยากรที่มีค่าขององค์กร การป้องกันที่แน่นหนาก็มีความจำเป็นสำหรับข้อมูลที่เป็นความลับ ซึ่งต้องอาศัยนโยบายความปลอดภัยและกลไกป้องกันที่ดีควบคู่กัน

4) People บุคลากร คือภัยคุกคามต่อสารสนเทศที่ถูกมองข้ามมากที่สุด โดยเฉพาะบุคลากรที่ไม่มีจรรยาบรรณในอาชีพ ก็เป็นจุดอ่อนต่อการโจมตีได้ จึงได้มีการศึกษากันอย่างจริงจังเรียกว่า Social Engineering ซึ่งเป็นการป้องการการหลอกหลวงบุคลากร เพื่อเปิดเผยข้อมูลบางอย่างเข้าสู่ระบบได้

5) Procedure ขั้นตอนการทำงาน เป็นอีกหนึ่งองค์ประกอบที่ถูกมองข้าม หากมิจฉาชีพทราบขั้นตอนการทำงาน ก็จะสามารถค้นหาจุดอ่อนเพื่อนกระทำการอันก่อนให้เกิดความเสียหายต่อองค์กรและลูกค้าขององค์กรได้

6) Network เครือข่ายคอมพิวเตอร์ การเชื่อมต่อระหว่างคอมพิวเตอร์และระหว่างเครือข่ายคอมพิวเตอร์ ทำให้เกิดอาชญากรรมและภัยคุกคามคอมพิวเตอร์ โดยเฉพาะการเชื่อมต่อระบบสารสนเทศเข้ากับเครือข่ายอินเตอร์เน็ต

อุปสรรคของงานความมั่นคงปลอดภัยของสารสนเทศ

1) ความมั่นคงปลอดภัย คือ ความไม่สะดวก เนื่องจากต้องเสียเวลาในการป้อน password และกระบวนการอื่น ๆ ในการพิสูจน์ตัวผู้ใช้

2) มีความซับซ้อนบางอย่างในคอมพิวเตอร์ที่ผู้ใช้ทั่วไปไม่ทราบ เช่น Registry , Port, Service ที่เหล่านี้จะทราบในแวดวงของ Programmer หรือผู้ดูแลระบบ

3) ผู้ใช้คอมไม่ระแวดระวัง

4) การพัฒนาซอฟต์แวร์ไม่คำนึงถึงความปลอดภัยภายหลัง

5) แนวโน้มเทคโนโลยีสารสนเทศคือการแบ่งปัน ไม่ใช่ การป้องกัน

6) มีการเข้าถึงข้อมูลได้จากทุกสถานที่

7) ความมั่นคงปลอดภัยไม่ได้เกิดขึ้นที่ซอฟแวร์และฮาร์ดแวร์เพียงอย่างเดียว

8) มิจฉาชีพมีความเชี่ยวชาญ (ในการเจาะข้อมูลของผู้อื่นมากเป็นพิเศษ)

9) ฝ่ายบริหารมักจะไม่ให้ความสำคัญแก่ความมั่นคงปลอดภัย

บทความภัยคุกคามความมั่นคงระบบสารสนเทศ ของ พ.อ.รศ.ดร.เศรษฐพงค์ มะลิสุวรรณ

ประมาณ 500 ปี ก่อนคริตศักราช ชาวจีนชื่อ ซัน ซุน วู ได้เขียนเรื่อง Art of war ให้ความสำคัญกับการรู้จักตัวเองรวมถึงภัยคุกคามที่ต้องเผชิญ เพื่อจะได้รู้ว่าควรปกป้องข้อมูลขององค์กรอย่างไร สิ่งที่ควรรู้ คือ

1) รู้จักตัวเอง คือ รู้จักการปกป้องข้อมูลและระบบให้มีความมั่นคง ระบบขนส่ง และขั้นตอนต่างๆ

2) การรู้ถึงภัยคุกคามที่ต้องเผชิญ ศึกษาจากแหล่งข้อมูลที่น่าเชื่อถือทำให้สามารถตัดสินใจจัดการกับภัยคุกคามต่างๆที่มีผลกับ พนักงาน โปรแกรม ข้อมูล และระบบสารสนเทศขององค์กร การรักษาความปลอดภัยข้อมูล กล่าวถึงอันตรายจากภัยคุกคามที่ส่งผลกับคน และทรัพย์สิน

มีการสำรวจประเภทของภัยคุกคาม เมื่อการเชื่อมต่ออินเตอร์เน็ตขยายไปทั่วโลก ศึกษาถึงแนวทางปฏิบัติในการป้องกันภัยคุกคามต่างๆ มีการสำรวจเปรียบเทียบประเภทของภัยคุกคามทำให้เกิดความเข้าใจร่วมกันว่าภัยคุกคามที่เพิ่มขึ้นมาจากการที่องค์กรเชื่อมต่ออินเตอร์เน็ต โดยจำนวนผู้ใช้อินเตอร์เน็ตเพิ่มขึ้นเรื่อยๆ คิดเป็น 17% ของคนทั้งโลก หรือ จากคนทั่วโลก 6.6 พันล้านคน มีคนที่เข้าใช้งานอินเตอร์เน็ตถึง 1.1 พันล้านคน

ข้อผิดพลาดจากการกระทำของมนุษย์ (Acts of human error or failure) ประเภทนี้มีการกระทำโดยเจตนา หรือ มีเจตนามุ่งร้ายโดยผู้ใช้ที่มีสิทธิเข้าใช้ระบบ เมื่อผู้ใช้ระบบทำงานผิดพลาด เนื่องจากขาดความชำนาญ ขาดการฝึกอบรม และการสันนิษฐานไม่ถูกต้อง สิ่งเล็กน้อยเหล่านี้สามารถสร้างความเสียหายอย่างมากการคุกคามที่อันตรายที่สุดต่อความปลอดภัยของข้อมูลองค์กร คือ พนักงานขององค์กรเองเพราะพนักงานใช้ข้อมูลในการดำเนินกิจกรรมทางธุรกิจขององค์กรทุกวัน สิ่งที่พนักงานจะต้องปฏิบัติอย่างเคร่งครัดคือ การรักษาความลับของข้อมูล ข้อมูลมีความถูกต้องครบถ้วน และข้อมูลพร้อมใช้งานได้ทุกเมื่อ รูปต่อไปเป็นการแนะนำเกี่ยวกับการคุกคามจาภายนอก เพราะความผิดพลาดเพียงเล็กน้อยของพนักงาน เช่น ไม่ได้ปิดประตูหน้าต่างทำให้หัวขโมยเข้ามาในองค์กรได้ การลบหรือแก้ไขข้อมูลที่เป็นเอกสารสำคัญ

นโยบายและกลยุทธ์ด้านเทคโนโลยีสารสนเทศ เพื่อสนับสนุนข้อมูลสารสนเทศ ซึ่งการโจมตีระบบข้อมูลสารสนเทศเป็นเหตุการณ์ที่เกิดขึ้นเป็นประจำทุกวัน และต้องการการรักษาความปลอดภัยของข้อมูลสารสนเทศที่เพิ่มมากขึ้นพร้อมกับการโจมตีที่มีความซับซ้อนมากขึ้น ดังนั้นองค์กรต้องเข้าใจในสิ่งแวดล้อมของการทำงานของระบบข้อมูลสารสนเทศ และกลยุทธ์ป้องกันภัยข้อมูลสารสนเทศจึงจะสามารถจัดการปัญหาต่างๆ ได้ ซึ่งเป็นต้นเหตุที่เกิดขึ้นกับข้อมูลสารสนเทศในองค์กร

ภัยคุกคาม ช่องโหว่ และการโจมตี ของ มหาวิทยาลัยฟาร์อิสเทอร์น

ภัยคุกคาม ช่องโหว่ และการโจมตี

1) ภัยคุกคาม

2) ช่องโหว่

3) การโจมตี

4) มัลแวร์

ภัยคุกคาม Threat คือ วัตถุ สิ่งของ ตัวบุคคล หรือสิ่งอื่นใดที่เป็นตัวแทนของการะทำอันตรายต่อทรัพย์สิน ภัยคุกคามมีหลายกลุ่ม เช่น ภัยคุกคามที่เกิดขึ้นโดยเจตนา หรือบางกลุ่มเป็นภัยคุกคามที่เกิดขึ้นโดยไม่ได้เจตนา เช่ยภัยคุกคามจากธรรมชาติ หรือจากผู้ใช้ในองค์กรเอง ภัยคุกคามที่สามารถทำลายช่องโหว่ ได้เท่านั้น จึงจะสามารถสร้างความเสียหายแก่ระบบได้ และจัดว่าภัยคุกคามนั้นเป็นความเสี่ยง Risk ที่อาจสร้างความเสียหายแก่สารสนเทศได้

ตารางที่ 2.1 ตารางสรุปประเภทของภัยคุกคาม

ประเภทของภัยคุกคาม	ตัวอย่างภัยคุกคาม
1) การทำลายหรือทำให้เสียหาย Subotage or Vandalism	1) การทำลายระบบหรือสารสนเทศ
2) การลักขโมย Theft	2) การลักขโมยหรือการโจรกรรมอุปกรณ์คอมพิวเตอร์หรือสารสนเทศ
3) ซอฟต์แวร์โจมตี Software Attack	3) ไวรัส เวิร์ม มาโคร Dos
4) ภัยธรรมชาติ Force of Nature	4) น้ำท่วม ไฟไหม้ แผ่นดินไหว ไฟดับ

ตารางที่ 2.1 (ต่อ)

ประเภทของภัยคุกคาม	ตัวอย่างภัยคุกคาม
5) คุณธรรมของการบริการที่เบี่ยงเบนไป Deviation in Quality of Service	5) ISP, WAN, Service, Provider
6) ความผิดพลาดทางด้านเทคนิคฮาร์แวร์ Hardware	6) อุปกรณ์ทำงานผิดพลาด
7) ความผิดพลาดทางด้านเทคนิคซอฟต์แวร์ Technical Hardware Failures/Error	7) Bugs, ปัญหาของโค๊ด ลูปไม่รู้จบ
8) ความล้าสมัยของเทคโนโลยี Technological Obsolescence	8) เทคโนโลยีที่ใช้บางอย่างล้าสมัยไปแล้ว

ความผิดพลาดที่เกิดจากบุคคล Human Error/Failures

1) เป็นความผิดพลาดที่เกิดจากพนักงานหรือบุคคลที่ได้รับอนุญาตให้เข้าถึงสารสนเทศขององค์กรได้

2) อาจเกิดจากความไม่ได้ตั้งใจ เนื่องจากไม่มีประสบการณ์ หรือขาดการฝึกอบรม หรือคาดเดา เป็นต้น

3) ป้องกันภัยคุกคาม โดยการให้ความรู้ด้านความมั่นคงปลอดภัยของสารสนเทศ การฝึกอบรมอย่างสม่ำเสมอ

4) มีมาตรการควบคุม

ภัยร้ายต่อทรัพย์สินทางปัญญา Comromises to Intellectual Property

1) ทรัพย์สินทางปัญญา Intellectual Property คือทรัพย์สินที่จับต้องไม่ได้ ที่ถูกสร้างขึ้นมาโดยบุคคลหรือองค์กรใด ๆ หากต้องการนำทรัพย์สินทางปัญญาของผู้อื่นไปใช้ อาจต้องเสียค่าใช้จ่าย และจะต้องระบุแหล่งที่มาของทรัพย์สินดังกล่าวไว้อย่างชัดเจน

2) ในทางกฎหมาย การให้สิทธิในความเป็นเจ้าของทรัพย์สินทางปัญญา มี 4 ประเภทคือ ลิขสิทธิ์ (copyrights) ความลับทางการค้า (Trade Secrets) เครื่องหมายการค้า (Trade Marks) สิทธิบัตร (Patents)

3) การละเมิดความคุ้มครองทรัพย์สินทางปัญญาที่มากที่สุดคือ การละเมิดลิขสิทธิ์ซอฟต์แวร์

การจารกรรมหรือการรุกล้ำ Espionage or Trespass

1) การจารกรรมหรือการรุกล้ำ (Espionage or Trespass) การจารกรรม Espionage เป็นการที่กระทำซึ่งใช้อุปกรณ์อิเลคทรอนิกส์ หรือตัวบุคคลในการจารกรรมสารสนเทศที่เป็นความลับ

2) ผู้จารกรรมจะใช้วิธีการต่าง ๆ เพื่อให้ถึงซึ่งสารสนเทศที่จัดเก็บไว้ และรวมรวมสารสนเทศนั้น โดยไม่ได้รับอนุญาต

3) Industrial Espionage วิธีนี้เป็นการใช้เทคนิคที่ถูกกฎหมายแต่ก้ำกึ่งความไม่ชอบธรรม เพื่อรวบรวมสารสนเทศที่สำคัญหรือความลับทางการค้าของคู่แข่งเพื่อนำมาหาผลประโยชน์

4) Shoulder Surfing คือการแอบดูข้อมูลส่วนตัวของผู้อื่นขณะทำธุรกรรมผ่านตู้ ATM

5) การรุกล้ำ Trespass คือ การกระทำที่ทำให้ผู้อื่นสามารถเข้าสู่ระบบเพื่อรวมรวมสารสนเทศที่ต้องการ โดยไม่ได้รับอนุญาต

ประเภทของ Espionage และ Trespass

1) Hacker บุคคลผู้ซึ่งสร้างซอฟต์แวร์คอมพิวเตอร์ขึ้นมา เพื่อให้ตนสามารถเข้าถึงสารสนเทศของผู้อื่นอย่างผิดกฎหมาย

แบ่งออกได้เป็น 2 ประเภท

Expert Hacker เป็นแฮคเกอร์ที่มีทักษะสูง ทำการพัฒนาโปรแกรมขนาดเล็กหรือซอฟต์แวร์สคริปต์ที่ใช้ในการเข้าถึงสารสนเทศในระบบของผู้อื่น ให้พวก Unskilled Hacker ใช้

Unskill Hacker คือ พวกแฮคเกอร์ที่มีทักษะน้อย ไม่สามารถสร้างโปรแกรมเจาะระบบได้เอง จึงเป็นผู้นำโปรแกรมไปเจาะระบบ หรือเข้าถึงสารสนเทศของผู้อื่น

2) Script Kiddies คือ แฮคเกอร์มือใหม่ ที่ไม่มีความชำนาญ เป็นผู้นำ ซอฟต์แวร์ของ Expert Hacker มาใช้ในการโจมตีหรือก่อกวนระบบของผู้อื่น

3) Packet Monkeys คือ script Kiddies ที่ใช้โปรแกรมอัตโนมัติโจมตีระบบแบบปฏิเสธการให้บริการ Distributed Denial of Service ทำให้ระบบไม่สามารถให้บริการทำตามคำร้องขอที่ส่งมาได้ ซึ่งอาจทำให้ผู้ใช้เข้าใจว่าระบบล้มเหลว

4) Cracker คือผู้ที่ทำลายหรือทำซ้ำซอฟต์แวร์รักษาความมั่นคงปลอดภัยของระบบอื่น

ความแตกต่างระหว่าง Hacker / Cracker

Hacker มีเป้าหมายเพื่อทดสอบความสามารถหรือต้องการท้าท้ายโดยการเจาะระบบให้สำเร็จ

Cracker มีจุดประสงค์คือ ต้องการทำลายระบบความมั่นคงปลอดภัยของระบบคอมพิวเตอร์หรือระบบสารสนเทศ

5) Phreaker คือ ผู้เจาะระบบเครือข่ายโทรศัพท์สาธารณะ เพื่อให้ตนเองใช้โทรศัพท์โดยไม่เสียค่าใช้จ่าย หรือเพื่อรบกวนสัญญาณโทรศัพท์

การกรรโชกสารสนเทศInformation Extortion คือ การที่มีผู้ขโมยข้อมูลหรือ สารสนเทศที่เป็นความลับจากคอมพิวเตอร์ แล้วต้องการเงินเป็นค่าตอบแทน เพื่อแลกกับการคืนสารสนเทศนั้นหรือแลกกับการไม่เปิดเผยสารสนเทศดังกล่าว เรียกว่า Blackmail

การทำลายหรือทำให้เสียหาย

1) เป็นการทำลายหรือก่อให้เกิดความเสียหายต่อระบบคอมพิวเตอร์เว็บไซต์ ภาพลักษณ์ ธุรกิจ และทรัพย์สินขององค์กร ซึ่งอาจเกิดจากผู้อื่นที่ไม่หวังดี หรือแม้กระทั่งจากพนักงานขององค์กรเอง

2) การทำลายเช่น การขีดเขียนทำลายหน้าเว็บไซต์

3) ภัยคุกคามประเภทนี้เรียกว่า ปฏิบัติการ Hacktivist หรือ Cyberactivist เป็นปฏิบัติการที่แซกแทรง หรือสร้างความสับสนให้กับระบบการทำงานบางอย่างในองค์กร เพื่อคัดค้านการดำเนินงาน นโยบาย หรือกิจกรรมบางอย่างขององค์กร หรือหน่วยงานของรัฐ

4) การก่อการร้ายบนโลกไซเบอร์ Cyberterrorism เป็นภัยคุกคามอีกรูปแบบหนึ่ง เป็นการก่อการร้ายผ่านระบบเครือข่ายหรือระบบอินเตอร์เน็ต

5) FBI ได้ให้นิยามของ Cybertierriorsm ว่า เป็นการโจมตีแบบไตร่ตรองไว้ก่อนต่อสารสนเทศ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ และข้อมูลซึ่งจะก่อให้เกิดความรุนแรงหรือทำลายเป้าหมาย โดยกลุ่มบุคคล หรือตัวแทนที่ไม่เปิดเผยนาม ที่มีเหตุจูงใจจากประเด็นการเมือง

การลักขโมย Theif คือการถือเอาของผู้อื่นโดยผิดกฎหมาย เช่นอุปกรณ์ต่าง ๆ ทั้งแบบธรรมดาและแบบอิเล็คทรอนิค แล้ว ยังรวมถึง สารสนเทศขององค์กร และทรัพย์สินทางปัญญาอื่น ๆ

ซอฟต์แวร์โจมตี Software Attack

1) เรียกว่า การโจมตีโดยซอฟต์แวร์ เกิดจากบุคคลหรือกลุ่มบุคคลออกแบบซอฟต์แวร์ให้ทำหน้าที่โจมตีระบบ เรียกว่า Malicious Code หรือ Malicious Software หรือ Malware

2) มัลแวร์ Malware ถูกออกแบบเพื่อสร้างความเสียหาย ทำลาย หรือระงับ การให้บริการของระบบเป้าหมาย มีหลายชนิด เช่น virus worm, Zombie, Trojan Horse, Logic Bomb, Back door เป็นต้น

ภัยธรรมชาติ Force of Nature

ภัยธรรมชาติต่าง ๆ สามารถสร้างความเสียหายให้กับสารสนเทศขององค์กรได้ หากไม่มีการป้องกันหรือวางแผนรับมือกับภัยธรรมชาติ อาจก่อให้เกิดความเสียหายแก่องค์กรได้อย่างมหาศาล สามารถป้องกันหรือจำกัดความเสียหาย โดยการวางแผนรับสถานการณ์ฉุกเฉินและภัยพิบัติ Contingency Plan

คุณภาพของการบริการที่เบี่ยงเบนไป Deviations in Quality of Service

เกิดขึ้นจากการที่องค์กรรับมาเพื่อการทำงานของระบบสารสนเทศไม่เป็นไปตามความคาดหวัง ซึ่งอาจเกิดจากความผิดพลาดของการให้บริการ ที่อาจจะเกี่ยวเนื่องจากอุปกรณ์ในระบบให้บริการผิดพลาด อาจกล่าวได้ว่า เป็นภัยคุกคามต่อความพร้อมใช้ Availability Disruption

ความผิดพลาดทางเทคนิคฮาร์แวร์ (Technical Hardware Failure / Error)

เกิดขึ้นเมื่อผู้ผลิตปล่อยฮาร์ดแวร์ที่มีข้อบกพร่องออกสู่ตลาด ทำให้องค์กรได้ฮาร์ดแวร์ดังกล่าวมา ได้รับผลกระทบจากการทำงานที่บกพร่องของฮาร์ดแวร์ อาจทำให้ระบบงานหยุดชะงักไม่สามารถให้บริการแก่ลูกค้าได้ องค์กรอาจสูญเสียยอดการสั่งซื้อ และที่สำคัญความน่าเชื่อถือในที่สุด

ความผิดพลาดทางเทคนิคด้านซอฟต์แวร์ Technical Software Failures/Error

เกิดจากองค์ซื้อ ซอฟต์แวร์ โดยไม่รู้ว่า ซอฟต์แวร์นั้นมีความผิดพลาด ซึ่งก็สามารถสร้างความเสียหายแก่องค์กร เช่นเดียวกันกับความผิดพลาดทางเทคนิคด้านฮาร์ดแวร์ เช่น ความผิดพลาดที่พบส่วนใหญ่ คือ Bug ในซอฟต์แวร์

ความล้าสมัยของเทคโนโลยี Technical Obsolescence

เทคโนโลยีพื้นฐานของคอมพิวเตอร์ หรือระบบสารสนเทศ ล้าสมัยจะส่งผลให้ระบบไม่น่าไว้ใจ และอาจเกิดความเสี่ยงต่อการรักษาความมั่นคงของสารสนเทศ เนื่องจากอาจถูกโจมตีได้โดยง่ายด้วยเทคโนโลยีที่ทันสมัยกว่า

ช่องโหว่

ช่องโหว่ Vulnerabilities หรือ ความล่อแหลม ซึ่งหมายถึง ความอ่อนแอของระบบคอมพิวเตอร์ หรือระบบเครือข่ายที่เปิดโอกาสให้สิ่งที่เป็นภัยคุกคามสามารถเข้าถึงสารสนเทศในระบบได้ ซึ่งจะนำไปสู่ความเสียหายแก่สารสนเทศ หรือแม้แต่การทำงานของระบบ

การถูกโจมตี

การโจมตี Attack คือการกระทำบางอย่างที่อาศัยความได้เปรียบจากช่องโหว่ของระบบ เพื่อเข้าควบคุมการทำงานของระบบ เพื่อให้ระบบเกิดความเสียหาย หรือเพื่อโจรกรรมสารสนเทศ

รูปแบบการโจมตีของ Malicious Code

1) สแกนหมายเลข IP Adress เพื่อหาหมายเลขช่องโหว่ แล้วทำการติดตั้ง Back door

2) ท่องเว็บไซต์ ระบบที่มี Malicious ฝังตัวอยู่ จะสร้างเว็บเพจชนิดต่าง ๆ เมื่อผู้ใช้เข้าได้เยี่ยมชมเว็บเพจที่มีอันตรายดังกล่าว ก็จะได้รับ Malicious Code ไปได้

3) Virus คัดลอกตัวเองไปอยู่กับโปรแกรม ที่ผู้ใช้รันโปรแกรมนั้นๆ

4) Email ส่งอีเมล์ที่มี Malicious Code ซึ่งทันทีที่เปิดเมลอ่าน Malicious Code ก็จะทำงานทันที

รูปแบบการโจมตี

เครื่องมือที่ใช้โจมตี แบบ Distributed Denial of Service (DDoS) DDoS มีใช้กันอย่างแพร่หลายมานานหลายปีแล้วย้อนหลังเป็น 10 ปี มาแล้ว (แต่บรรดาผู้ผลิตอุปกรณ์คอมพิวเตอร์ต่างก็มีวิธีป้องกันการโจมตีเช่นเดียวกัน)

รูปแบบการโจมตีที่นิยมใช้กันก็มีอย่าง SYN flood, UDP flood, ICMP flood, Smurf, Fraggle เป็นต้น

การโจมตีแบบ SYN Flood เป็นการโจมตีโดยการส่ง แพ็คเก็ต TCP ที่ตั้งค่า SYN บิตไว้ไปยังเป้าหมาย เสมือนกับการเริ่มต้นร้องขอการติดต่อแบบ TCP ตามปกติ (ผู้โจมตีสามารถปลอมไอพีของ source address ได้) เครื่องที่เป็นเป้าหมายก็จะตอบสนองโดยการส่ง SYN-ACK กลับมายัง source IP address ที่ระบุไว้ ซึ่งผู้โจมตีจะควบคุมเครื่องที่ถูกระบุใน source IP address ไม่ให้ส่งข้อมูลตอบกลับ ทำให้เกิดสภาวะ half-open ขึ้นที่เครื่องเป้าหมาย หากมีการส่ง SYN flood จำนวนมาก ก็จะทำให้คิวของการให้บริการของเครื่องเป้าหมายเต็ม ทำให้ไม่สามารถให้บริการตามปกติได้ นอกจากนี้ SYN flood ที่ส่งไปจำนวนมาก ยังอาจจะทำให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่อีกด้วย

การโจมตีแบบ ICMP Flood เป็นการส่งแพ็คเก็ต ICMP ขนาดใหญ่จำนวนมากไปยังเป้าหมาย ทำให้เกิดการใช้งานแบนด์วิดธ์เต็มที่

การโจมตีแบบ UDP Flood เป็นการส่งแพ็คเก็ต UDP จำนวนมากไปยังเป้าหมาย ซึ่งทำให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่ และหรือทำให้ทรัพยากรของเป้าหมายถูกใช้ไปจนหมด โดยจะส่ง UDP packet ไปยัง port ที่กำหนดไว้ เช่น 53 (DNS)

การโจมตีแบบ Teardrop โดยปกติ เราเตอร์จะไม่ยอม ให้แพ็กเก็ตขนาดใหญ่ผ่านได้ จะต้องทำ Fragment เสียก่อนจึงจะยอมให้ผ่านได้ และเมื่อผ่านไปแล้วเครื่องของผู้รับปลายทาง จะนำแพ็กเก็ตที่ถูกแบ่งออกเป็น ชิ้นส่วนต่าง ๆ ด้วยวิธีการ Fragment มารวมเข้าด้วยกันเป็น แพ็กเก็ตที่สมบูรณ์ การที่สามารถนำมารวมกันได้นี้จะต้องอาศัยค่า Offset ที่ปรากฏอยู่ในแพ็กเก็ต แรกและแพ็กเก็ตต่อๆ ไป สำหรับการโจมตีแบบ Teardrop นี้ ผู้โจมตีจะส่งค่า Offset ในแพ็กเก็ตที่ สองและต่อ ๆ ไปที่จะทำให้เครื่องรับปลายทางเกิดความสับสน หากระบบปฏิบัติการไม่สามารถ รับมือกับปัญหานี้ก็จะทำให้ระบบหยุดการทำงานใน ทันที

การโจมตีแบบ Land Attack ลักษณะการโจมตีประเภทนี้ เป็นการส่ง SYN ไปที่ เครื่องเป้าหมายเพื่อขอการเชื่อมต่อ ซึ่งเครื่องที่เป็นเป้าหมายจะต้องตอบรับคำขอการเชื่อมต่อด้วย SYN ACK ไปที่เครื่องคอมพิวเตอร์ต้นทางเสมอ แต่เนื่องจากว่า IP Address ของเครื่องต้นทางกับ เครื่องที่เป็น เป้าหมายนี้มี IP Address เดียวกัน โดยการใช้วิธีการสร้าง IP Address ลวง (โดยข้อเท็จจริงแล้วเครื่องของ Hacker จะมี IP Address ที่ต่างกับเครื่องเป้าหมายอยู่แล้ว แต่จะใช้ วิธีการทางซอฟต์แวร์ในการส่งแพ็กเก็ตที่ประกอบด้วยคำขอการเชื่อมต่อ พร้อมด้วย IP Address ปลอม) ซึ่งโปรโตคอลของเครื่องเป้าหมายไม่สามารถแยกแยะได้ว่า IP Address ที่เข้ามาเป็นเครื่อง ปัจจุบันหรือไม่ ก็จะทำการตอบสนองด้วย SYN ACK ออกไป หากแอดเดรสที่ขอเชื่อมต่อเข้ามา เป็นแอดเดรสเดียวกับเครื่องเป้าหมาย ผลก็คือ SYN ACK นี้จะย้อนเข้าหาตนเอง และเช่นกันที่การ ปล่อย SYN ACK แต่ละครั้งจะต้องมีการปันส่วนของหน่วยความจำเพื่อการนี้ จำนวนหนึ่ง ซึ่งหาก ผู้โจมตีส่งคำขอเชื่อมต่อออกมาอย่างต่อเนื่องก็จะเกิดปัญหาการจัดสรร หน่วยความจำ

การโจมตี แบบ Smurf ผู้โจมตีจะส่ง ICMP Echo Request ไปยัง broadcast address ในเครือข่ายที่เป็นตัวกลาง (ปกติจะเรียกว่า amplifier) โดยปลอม source IP address เป็น IP address ของระบบที่ต้องการโจมตี ซึ่งจะทำให้เครือข่ายที่เป็นตัวกลางส่ง ICMP Echo Reply กลับไปยัง IP address ของเป้าหมายทันที ซึ่งทำให้มีการใช้งานแบนด์วิดธ์อย่างเต็มที่ความเสียหายที่เกิด โดยการโจมตีในรูปแบบ DoS ความเสียหายที่เกิดจาก DoS ส่งผลให้ผู้ใช้งานแต่ละส่วนไม่ เหมือนกัน แล้วแต่ว่าเขาจะอยู่ในส่วนใด เช่น เป็นผู้เข้าไปใช้งาน เป็นพนักงานในองค์กรที่ โดนโจมตีหรือเป็น เจ้าของเครื่องที่ถูกใช้ในการโจมตี หรือจะมองในแง่ขององค์กรที่โดนโจมตี ทุกๆ ฝ่ายล้วนแล้วแต่เป็นฝ่ายเสียทั้งนั้น ยกเว้นคนที่ทำให้เหตุการณ์นี้ เกิดขึ้น หรือคนที่เป็นคน บงการอยู่เบื้องหลังเท่านั้นที่ได้ประโยชน์จากการโจมตีนั้น จะจัดความเสียหาย ของ DoS นั้น ก็สามารถจัดได้ตามประเภทของการทำงานของตัว DoS เอง ซึ่งสามารถแบ่งได้เป็นสองประเภท ด้วยกันคือ

ความเสียหายกับเครื่องคอมพิวเตอร์ ในส่วนความเสียหายของ เครื่องคอมพิวเตอร์นั้น เราก็สามารถมองได้สองมุมด้วยกันคือ ในมุมของเครื่องที่ถูกใช้ในการโจมตีกับในมุมของเครื่องที่โดนโจมตี

1) เครื่องที่ถูกใช้เป็นเครื่องมือในการโจมตี อันดับแรกคือเราสูญเสียการควบคุมของเครื่องเราเองทำให้คนอื่นสามารถเข้ามาบงการเครื่องของเราให้ไปทำอย่างโน้นทำอย่างนี้ตามที่เขาต้องการได้ อันดับสองคือการเสียทรัพยากรของเครื่องเองไม่ว่าจะเป็น ซีพียู เมโมรี หรือแบนด์วิดธ์ เป็นต้น ทรัพยากรต่าง ๆ ของเครื่องที่กล่าวไปแล้วนั้นจะถูกใช้ไปรันโปรแกรมที่จะใช้ในการเข้าไปโจมตี เครื่องเหยื่อ ทำให้เครื่องคอมพิวเตอร์ของเรานั้นไม่สามารถใช้งานได้อย่างเต็มที่

2) เครื่องที่เป็นเหยื่อในการโจมตีครั้งนี้ แน่นอนว่าทำให้เครื่องนั้นไม่สามารถให้บริการต่อไปได้ เพราะจุดประสงค์หลักของ DoS ก็คือสิ่งนี้ เพราะเครื่องนั้นมัวแต่ประมวลผล Request จำนวนมากที่ถูกส่งเข้ามาทำให้เครื่องนั้นทำงานหนักจนไม่สามารถรับงานได้อีกต่อไปบางเครื่องอาจจะแฮงก์ไปเฉย ๆ หรือระบบอาจจะ Crash เลยก็เป็นไปได้ทำให้เครื่องนั้นไม่สามารถให้บริการได้อีก

ความเสียหายกับระบบเน็ตเวิร์ก ความเสียหายที่เกิดขึ้น กับระบบเน็ตเวิร์กนั้นเราก็สามารถมองได้สองมุมเช่นกัน คือ มองในมุมของผู้ที่ถูกใช้เป็นเครื่องมือในการโจมตี และผู้ที่ถูกโจมตี มุมที่ผู้ถูกใช้เป็นเครื่องมือ ทำให้แบนด์วิดธ์ที่เราควรจะมีเหลือไว้ ใช้นั้นถูกใช้ไปกับการโจมตีเสียหมด บางครั้งก็กินแบนด์วิดธ์ทั้งหมด ที่เรามีอยู่เพื่อใช้ในการโจมตีทำให้เครื่อง หรือระบบที่ถูกใช้เป็นเครื่องมือในการโจมตีนั้นไม่สามารถใช้งานระบบ เน็ตเวิร์กได้อีกต่อไป มุมที่ผู้ถูกโจมตี เช่นเดียวกับแบนด์วิดธ์ของผู้ที่ถูกโจมตีนั้นก็จะใช้ไปอย่างรวดเร็วจนหมด ทำให้บริการที่เตรียมไว้ที่เครื่องที่ถูกโจมตีนั้นไม่สามารถใช้งานได้อีกต่อไป เครื่องที่ต้องการที่จะติดต่อเข้ามาที่เครื่องนี้ หรือผ่านเครื่องนี้เพื่อเข้าไปในระบบข้างใน (ในกรณีที่เป็นไฟร์วอลล์) ไม่สามารถใช้งานได้ ผู้ที่อยู่ด้านในของระบบก็จะไม่สามารถเชื่อมต่อกับ ระบบภายนอกได้เช่นเดียวกัน แต่ระบบ LAN ภายในก็ยังสามารถใช้งานได้ตามปกติ

ความเสียหายกับองค์กร เมื่อเกิดการโจมตีขึ้นแล้วก็มีแต่เสียกับเสียเท่านั้น ยิ่งองค์กรที่ถูกโจมตีด้วยแล้วความเสียหายนั้นก็เกิดขึ้นอย่างมากมายทีเดียว เริ่มตั้งแต่ความเสียหายของตัวเครื่องคอมพิวเตอร์หรือระบบที่โดนโจมตีเองทำให้ ต้องเสียเวลาเสียค่าใช้จ่ายในการซ่อมแซม เพื่อที่ให้สามารถกลับมาให้บริการได้อย่างเดิม เสียโอกาสทางธุรกิจโอกาสที่จะทำธุรกรรมกับเครื่องที่โดนโจมตี หรือการทำธุรกรรมอื่นๆ กับระบบภายในที่จำเป็นต้องต่อเชื่อมกับอินเตอร์เน็ตสูญเสียโอกาสที่จะทำธุรกรรมทางอินเตอร์เน็ต โอกาสที่ลูกค้าจะเข้ามาในเว็บโอกาสที่จะปิด การขาย โอกาสที่จะสร้างรายได้ และอีกหลาย ๆ โอกาสที่ทางองค์กรจะต้องเสียไป

เสียภาพลักษณ์ขององค์กร องค์กรที่ถูกโจมตีด้วยการโจมตีประเภท DoS นั้น ทำให้การบริการที่องค์กรนั้นเตรียมพร้อมไว้ให้บริการไม่สามารถให้บริการ ได้ทำให้ภาพลักษณ์ขององค์กรนั้นเสียไป เพราะไม่สามารถป้องกัน เหตุที่เกิดขึ้นได้ หรือไม่มีวิธีการแก้ไขที่รวดเร็วจนทำให้เกิดความ เสียหายขึ้น ทำให้ลูกค้าขาดความเชื่อมั่นในองค์กรว่าจะสามารถตอบสนอง ความต้องการของตนได้ อาจเป็นเหตุให้ลูกค้าเปลี่ยนใจไปใช้บริการของ องค์กรอื่นแทนในที่สุด

วงจรชีวิตของไวรัสคอมพิวเตอร์ มี 4 ระยะ คือ

1) ระยะไม่เคลื่อนไหว Dormant Phase เป็นระยะที่โปรแกรมไวรัสจะหยุดนิ่งไม่กระทำการใดๆ เป็นระยะที่ยังไม่ถูกกระตุ้นให้ทำงานนั่นเอง

2) ระยะแพร่กระจาย Propagation Phase เป็นระยะที่โปรแกรมไวรัสคัดลอกตัวเองหรือฝังตัวอยู่กับโปรแกรมอื่น หรือหน่วยความจำ ใด ๆ ขึ้นอยู่กับหน้าที่ของไวรัส สำหรับโปรแกรมที่ติดไวรัส ก็คือโปรแกรมที่มีโค๊ดไวรัสฝังอยู่หรือแนบอยู่ ก็จะเข้าสู่ระยะแพร่กระจายต่อไป

3) ระยะถูกกระตุ้น Triggering Phase เป็นระยะที่โปรแกรมไวรัสดถูกกระตุ้นให้ทำงานตามคำสั่ง โดยเหตุการณ์ต่าง ๆ ที่จะเป็นตัวกระตุ้นการทำงาน เช่น ถึงวันที่ที่ถูกกำหนดไว้ในโปรแกรมไวรัส

4) ระยะทำงาน Execution Phase เป็นระยะทำงานของโปรแกรมไวรัส เป็นระยะที่เห็นผลของการทำงาน เช่นมีข้อความปรากฏบนจอภาพ หรือ รูปภาพในโฟลเดอร์หายไป เป็นต้น

ประเภทของไวรัส

1) Memory Resident Virus เป็นไวรัสที่ฝังตัวอยู่ในหน่วยความจำหลัก

2) Program File Virus เป็น ไวรัส ที่ฝังตัวอยู่ในโปรแกรมใด ๆ เช่น File ที่มี นามสกุล .exe, .com, .sys เป็นต้น

3) Polymorphic Virus เป็นไวรัสที่สามารถซ่อนลักษณะและเปลี่ยนพฤติกรรมไปเรื่อยๆ เพื่อหลีกเลี่ยงการตรวจจับของซอฟต์แวร์ AntiVirus

4) Boot Sector เป็นไวรัสที่ฝังตัวอยู่ในส่วนของ Boot Sector ของ Hard disk ที่จัดเก็บโปรแกรมระบบปฏิบัติการ ซึ่งจะถูกอ่านเมื่อเริ่มต้นเปิดเครื่อง การทำงานของไวรัสชนิดนี้ จะทำการเคลื่อนย้ายชุดคำสั่งที่อยู่บริเวณ Boot Sector ไปไว้บริเวณอื่น จากนั้นโปรแกรมไวรัสจะวางโค๊ดของตนไว้ใน Boot Sector แทน เมื่อระบบเริ่มทำงาน คือเริ่มเปิดเครื่อง โค๊ดโปรแกรมไวรัสจะถูกโหลดไปไว้ที่หน่วยความจำหลัก เพื่อเริ่มทำการประมวลผลตามคำสั่งมุ่งร้ายที่ได้กำหนดไว้ และขณะเดียวกันไวรัสก็ได้ถูกฝังตัวอยู่ในหน่วยความจำหลักเรียบร้อยแล้ว

5) Macro Virus มาโคร คือชุดคำสั่ง ที่ทำงานได้เองอัตโนมัติ บนโปรแกรมหรือ application เฉพาะ นั่นคือในกลุ่ม Microsoft Office แบ่งออกเป็น Auto Execute, Auto Macro, Command Macro

6) E-mail Virus เป็นไวรัสที่แนบตัวเองไปกับอีเมล์ เช่น อาจแบบไปกับเนื้อหาอีเมล์ หรือฝังตัวไปกับไฟล์ที่แนบไปกับอีเมล์

ปัญหาจากสปายแวร์ เมื่อสปายแวร์ได้แอบเข้ามาติดตั้งอยู่ในเครื่องคอมพิวเตอร์ของคุณแล้ว มันจะพยายามรัน process พิเศษบางอย่างซึ่งจะเป็นผลให้เครื่องคอมพิวเตอร์ของคุณทำงานช้าลงหรืออาจทำการเข้าสู่เว็บไซต์ต่างๆได้ช้า หรืออาจเข้าสู่เว็บไซต์ที่ต้องการไม่ได้เลย นอกจากนี้ ยังส่งผลเกี่ยวเนื่องกับเรื่องของข้อมูลส่วนบุคคล (privacy) ในประเด็นต่อไปนี้ด้วย ไม่สามารถทราบได้เลยว่าข้อมูลที่ถูกนำไปมีอะไรบ้างไม่อาจทราบได้เลยว่าใครเป็นผู้นำข้อมูลเหล่านั้นไปและจะไม่ทราบเช่นกันว่า ข้อมูลเหล่านั้นจะถูกนำไปใช้อย่างไรบ้าง

ข้อสังเกตเมื่อมีสปายแวร์เข้ามาติดตั้งอยู่ในเครื่องคอมพิวเตอร์ มีหน้าต่างเล็กๆ ที่เป็นโฆษณาป๊อบอัพขึ้นมาเองบ่อยครั้งจนนับไม่ถ้วน เมื่อต้องการเข้าสู่เว็บไซต์ใดเว็บไซต์หนึ่งและพิมพ์ที่อยู่แอดเดรส (URL) ลงไปอย่างถูกต้องแล้วแต่เว็บบราวเซอร์จะเข้าสู่เว็บไซต์ที่สปายแวร์ได้ตั้งไว้และแสดงหน้าเว็บเหล่านั้น แทนที่จะเข้าไปยังเว็บไซต์ที่ต้องการสังเกตเห็นว่ามีแถบเครื่องมือใหม่ๆ ที่ไม่เคยเห็น หรือไม่คุ้นเคยเกิดขึ้นบนเว็บบราวเซอร์ บริเวณ task tray ในส่วนแสดงการเปิดโปรแกรมที่กำลังรันอยู่ด้านล่างของหน้าต่างวินโดว์จะปรากฏแถบแสดงเครื่องมือหรือไอคอนที่ไม่เคยเห็นมาก่อน หรือไอคอนแปลกๆ หน้าหลักของบราวเซอร์ที่คุณเซ็ตค่าไว้ถูกเปลี่ยนไปในทันที เมื่อเรียก search engine ที่เคยใช้ในการค้นหาขึ้นมา และทำการค้นหา หรือทันทีที่คลิกปุ่ม search เว็บบราวเซอร์จะไปเรียกหน้าเว็บที่แตกต่างไปจากเดิมฟังก์ชั่นบนคีย์บอร์ดบางอย่างที่เคยใช้งานจะเกิดอาการผิดปกติ เช่น เคยกดปุ่ม tab เพื่อเลื่อนไปยังช่องกรอกข้อความในฟิลด์ถัดไปบนหน้าเว็บจะไม่สามารถใช้ในการเลื่อนตำแหน่งได้เหมือนเดิม เป็นต้น ข้อความแสดงความผิดพลาดของซอฟต์แวร์วินส์โดว์จะเริ่มปรากฏบ่อยมากขึ้น เครื่องคอมพิวเตอร์ของคุณจะทำงานช้าลงอย่างเห็นได้ชัดเมื่อสั่งเปิดโปรแกรมหลายโปรแกรม หรือทำงานหลายอย่าง โดยเฉพาะในระหว่างการบันทึกแฟ้มข้อมูล เป็นต้น

การป้องกันสปายแวร์ ไม่คลิ๊กลิ้งบนหน้าต่างเล็กๆ ที่ปรากฏขึ้นมาอัตโนมัติหรือโฆษณาที่ป๊อบอัพขึ้นมา เพราะป๊อบอัพเหล่านั้นมักจะมีตัวสปายแวร์ฝังอยู่ การคลิ๊กลิ้งเหล่านั้นจะทำให้สปายแวร์ถูกนำเข้ามาติดตั้งบนเครื่องของคุณผ่านวินโดวส์ได้ในทันที ส่วนวิธีการปิดหน้าต่างป๊อบอัพเหล่านั้นควรคลิ้กที่ปุ่ม “X” บนแถบเมนู Title bar แทนที่จะปิดด้วยคำสั่ง close บนแถบแสดงเครื่องมือมาตรฐานของวินโดว์ (standard toolbar) ควรเลือกที่คำตอบ “No” ทุกครั้งที่มีคำถามต่างๆ ถามขึ้นมาจากป๊อบอัพเหล่านั้น คุณต้องระมัดระวังเป็นอย่างมากกับคำถามที่ปรากฏขึ้นมาเป็นไดอะล็อกบ็อกซ์ต่างๆ แม้ว่าไดอะล็อกบ๊อกซ์เหล่านั้นจะเกิดขึ้นตอนคุณกำลังรันโปรแกรมเฉพาะที่คุณจะใช้งาน หรือใช้โปรแกรมอื่นอยู่ก็ตาม ควรปิดหน้าต่างป๊อบอัพเหล่านั้นด้วยวิธีคลิ้กที่ปุ่ม “X” บนแถบเมนู Title bar แทนที่จะปิดด้วยคำสั่ง close บนแถบแสดงเครื่องมือมาตรฐานของวินโดว์ (standard toolbar) ควรระมัดระวังอย่างมากในการดาวน์โหลดซอฟต์แวร์ที่จัดให้ดาวน์โหลดฟรี เพราะมีหลายเว็บไซต์ที่จัดหาแถบเครื่องมือแบบที่ให้ผู้ใช้ปรับแต่งเองหรือมีคุณสมบัติอื่นๆ ที่เหมาะสำหรับผู้ใช้ให้ปรับแต่งเองไว้ให้ดาวน์โหลดบนอินเทอร์เน็ต สำหรับท่านที่ต้องการใช้คุณสมบัติของเครื่องมือเหล่านี้ ไม่ควรจะดาวน์โหลด เครื่องมือเหล่านี้มาจากเว็บไซต์ที่ไม่น่าเชื่อถือ และต้องตระหนักเสมอว่ามันเป็นการปล่อยให้สปายแวร์ผ่านเข้ามายังเครื่องคุณได้ด้วย ไม่ควรติดตามอีเมล์ลิ้งที่ให้ข้อมูลว่ามีการเสนอซอฟต์แวร์ป้องกันสปายแวร์ เหมือนกับอีเมล์ที่ให้ข้อมูลว่า มีการเสนอซอฟต์แวร์ป้องกันไวรัส ซึ่งอันที่จริงลิ้งเหล่านั้นจะนำไปสู่แนวทางที่ตรงกันข้าม คือเป็นการถามเพื่อให้คุณคลิ้กอนุญาตให้สปายแวร์เข้ามาดำเนินการติดตั้งในเครื่องโดยไม่ถูกขัดขวาง

วิธีกำจัดสปายแวร์ ทำการสแกนเครื่องคอมพิวเตอร์อย่างถี่ถ้วน ด้วยโปรแกรมแอนติไวรัส ซึ่งแอนติไวรัสบางยี่ห้อจะมีคุณสมบัติในการค้นหาและกำจัดสปายแวร์ แต่แอนติไวรัสอาจไม่สามารถมองหาสปายแวร์พบแบบ real time ได้ ดังนั้นควรกำหนดให้โปรแกรมแอนติไวรัสของคุณทำการสแกนหาไวรัสเมื่อเครื่องอยู่ในสภาวะปลอดจากการใช้งานใดๆ และควรทำการสแกนอย่างถี่ถ้วนและสม่ำเสมอ เช่น วันละครั้งหลังเลิกงาน เป็นต้น) ทำการติดตั้งโปรแกรมแอนติสปายแวร์ที่มีลิขสิทธิ์และถูกออกแบบมาเพื่อกำจัดสปายแวร์โดยเฉพาะมีผู้ผลิตหลายรายที่เสนอผลิตภัณฑ์ที่มีคุณสมบัตินี้ ซึ่งจะสแกนหาสปายแวร์บนเครื่องและกำจัดสปายแวร์ออกจากเครื่องได้ สำหรับผลิตภัณฑ์แอนติสปายแวร์ที่เป็นที่นิยม ได้แก่ LavaSoft’Adaware,Webroot’s SpySweeper, PestPatrol, Spybot Search and Destroy (ตามลิ้งก์ด้านล่าง) สร้างความรำคาญ ให้กับผู้ที่รู้ว่ามันคือของปลอม เพราะต้องเปลืองแรงลบเมล์ในอินบ็อกซ์ (Inbox) อยู่เสมอๆ แต่สำหรับผู้ที่หลงเชื่ออาจสร้างความตื่นตระหนก จนต้องรีบตรวจสอบเครื่องตัวเองอย่างเร่งด่วน เมื่อตรวจสอบพบตามที่ข้อความในอีเมล์แจ้งมาแล้ว จะให้ผู้ดูแลระบบมาจัดการกำจัดไวรัสโดยด่วน เมื่อผู้ดูแลระบบมาถึง แล้วบอกว่านี่ไม่ใช่ไวรัส แต่มันเป็นแค่จดหมายหลอกลวง ก็กลับไม่เชื่อ และ ที่ร้ายแรงกว่านั้นคือ เมื่อตนเองได้รับอีเมล์นั้น ก็หวังดีส่งต่อ

ข้อความไปเรื่อยๆทำให้เปลืองทรัพยากรของระบบเครือข่ายโดยไม่จำเป็น และอาจกลายเป็นจดหมายลูกโซ่ที่ไม่มีวันจบสิ้นในที่สุด

วิธีการสังเกตมีดังนี้

1) อีเมล์ดังกล่าวจะไม่มีไฟล์แนบ

2) ส่วนใหญ่อ้างว่าได้ข้อมูลมาจากแหล่งข่าวที่มีชื่อเสียง แต่ไม่มีลิงค์ไปยังแหล่งข้อมูลนั้น

3) ประกอบไปด้วยข้อความอวดอ้างเกินจริง เน้นย้ำว่ามีอันตรายมาก

4) เนื้อความในตอนท้ายเน้นว่าต้องส่งอีเมล์นี้ต่อให้ผู้อื่น เป็นต้น

5) พบเห็นจดหมายอิเล็กทรอนิกส์ที่มีข้อความในทำนองที่กล่าวข้างต้น ชื่อเรื่อง หรือเนื้อหาที่มีในรายการดังต่อไปนี้ ควรลบทิ้งทันทีและไม่ควรส่งต่อให้ผู้อื่น เนื่องจากเป็นข่าวที่ไม่เป็นความจริง และอาจก่อให้เกิดความเสียหายต่อผู้อื่นที่ได้รับข้อความเหล่านี้

ผลงานวิจัยที่เกี่ยวกับพฤติกรรมการใช้สังคมออนไลน์เวลาจริงของนักศึกษาปริญญาตรีมหาวิทยาลัยธุรกิจบัณฑิตย์ ของนักศึกษา สุพรรษา เกษสีแก้ว (2552) จาก มหาวิทยาลัยธุรกิจบัณฑิตย์ เป็นการศึกษาพฤติกรรมการใช้สังคมออนไลน์เวลาจริงของนักศึกษามหาวิทยาลัยธุรกิจบัณฑิตย์ และเปรียบเทียบพฤติกรรมการใช้สังคมออนไลน์เวลาจริง จำแนกตามปัจจัยส่วนบุคคลของนักศึกษา กลุ่มตัวอย่างเป็นนักศึกษาปริญญาตรีมหาวิทยาลัยธุรกิจบัณฑิตย์ จำนวน 400 คน พบว่าส่วนใหญ่ ใช้สังคมออนไลน์เวลาจริงด้วยโปรแกรม msn เพื่อแลกเปลี่ยนข่าวสาร ที่บ้าน ส่วนใหญ่รู้จักสังคมออนไลน์จากเพื่อน ด้านประโยชน์ของสังคมออนไลน์เวลาจริงที่พอใจมากที่สุด ช่วงเวลาที่ใช้ คือ 18.01 – 24.00 น. ใช้ในการติดต่อกับบุคคลที่รู้จัก

ผลงานวิจัยที่เกี่ยวกับ ความรู้ ทัศนคติต่อพฤติกรรมด้านความปลอดภัยของพนักงานอู่ทหารเรือพระจุลจอมเกล้า กรมอู่ทหารเรือ กรณีศึกษา : ในสายงานฝ่ายผลิต ของนักศึกษา ศิริพงศ์ ศรีสุขกาญจน์ (2553) นักศึกษามหาวิทยาลัยธุรกิจบัณฑิตย์ เป็นการศึกษาพฤติกรรมด้านความปลอดภัยของพนักงาน เปรียบเทียบความรู้และทัศนคติของพนักงานที่มีลักษณะส่วนบุคคลแตกต่างกันและความสัมพันธ์ระหว่างความรู้ ทัศนคติ และพฤติกรรมด้านความปลอดภัย กลุ่มตัวอย่างคือพนักงานที่ปฏิบัติงานในสายงานฝ่ายผลิตของ อู่ทหารเรือพระจุลจอมเกล้า กรมอู่ทหารเรือ จำนวน 277 คน พนักงานมีระดับความรู้ด้านความปลอดภัยอยู่ในระดับปานกลาง ทัศนคติด้าน ความปลอดภัยอยู่ในระดับที่ดี และพฤติกรรมด้านความปลอดภัยอยู่ในระดับปานกลาง

ผลงานวิจัยที่เกี่ยวกับการใช้ประโยชน์และความพึงพอใจต่อระบบอินทราเน็ต การใช้ประโยชน์และความพอใจต่อระบบอินทราเน็ตเพื่อการสื่อสารภายในองค์กร กรณีศึกษา : ข้าราชการโรงพยาบาลพระมงกุฎเกล้า ของนักศึกษา วรรณยา บุนนาค (2554) นักศึกษามหาวิทยาลัยธุรกิจบัณฑิตย์ เป็นการศึกษาเรื่อง การศึกษาพฤติกรรมการใช้อินทราเน็ตเพื่อการสื่อการภายในองค์กร การใช้ประโยชน์ความพึงพอใจต่อการใช้ระบบอินทราเน็ตเพื่อการสื่อสารภายในองค์กร โดยใช้แบบสอบถามกับกลุ่มตัวอย่าง 358 คนแล้วนำมาวิเคราะห์ ค่าร้อยละ ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน ค่าไคสแควร์ และความแปรปรวนทางเดียว จากการสุ่มตัวอย่างดังกล่าว โรงพยาบาลพระมงกุฎเกล้าในการให้บริการบนระบบอินทราเน็ตและคอมพิวเตอร์ยังมีประสิทธิภาพต่ำ

ผลงานวิจัยที่เกี่ยวกับความรู้ความเข้าใจในความปลอดภัยของข้อมูลส่วนบุคคล ของนักศึกษา นวรัตน์ พัฒโนทัย (2555) นักศึกษามหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี เป็นการศึกษาเรื่อง ทางระบบคอมพิวเตอร์ กรณีศึกษาในเขต กรุงเทพมหานคร เป็นการศึกษาระดับความรู้ ความเข้าใจในความปลอดภัยของข้อมูลส่วนบุคคลในเขตกรุงเทพมหานคร จากกลุ่มตัวอย่างที่ใช้ในการศึกษา คือประชาชน ที่ใช้คอมพิวเตอร์ ในเขตกรุงเทพมหานคร โดยใช้แบบสอบถาม เป็นเครื่องมือในการสำรวจ สรุปได้ว่า ประชาชนที่ใช้คอมพิวเตอร์ในเขตกรุงเทพมหานคร ส่วนใหญ่มีระดับความรู้อยู่ในเกณฑ์มีความรู้ร้อยละ 68.6 ผลการทดสอบสมมติฐานพบว่า ปัจจัยส่วนบุคคลที่มีความแตกต่างกัน ด้านเพศ อายุ ระดับการศึกษา อาชีพ ประสบการณ์การทำงาน มีผลต่อความรู้ ความเข้าใจในความปลอดภัยของข้อมูลส่วนบุคคลทางระบบคอมพิวเตอร์แตกต่างกัน ยกเว้นปัจจัยส่วนบุคคลด้านรายได้ ซึ่งไม่ส่งผลต่อความรู้ความเข้าใจในความปลอดภัยของข้อมูลส่วนบุคคลทางระบบคอมพิวเตอร์

ผลงานวิจัยที่เกี่ยวกับการวิเคราะห์ความคุ้มทุนและประโยชน์ที่ชุมชนได้รับในการจัดตั้งศูนย์ ของนักศึกษา ปิยะนาถ คล่องดี (2556) นักศึกษามหาวิทยาลัยธุรกิจบัณฑิตย์ เป็นการศึกษาเรื่อง การวิเคราะห์ความคุ้มทุนและประโยชน์ที่ชุมชนได้รับในการจัดตั้งศูนย์การเรียนรู้ ICT ชุมชน กรณีศึกษา ศูนย์การเรียนรู้ ICT ชุมชนตำบลบางเพรียง อำเภอบางบ่อ จังหวัดสมุทรปราการ เป็นการศึกษาความคุ้มค่าในการลงทุนจัดตั้งศูนย์การเรียนรู้ ICT ชุมชนของภาครัฐกับมูลค่าการลงทุนที่เสียไป โดยมีการวิเคราะห์เป็น 2 แบบ คือ 1) การวิเคราะห์ข้อมูลเชิงปริมาณ โดยนำการวิเคราะห์ ทางการเงินมาใช้ 2) การวิเคราะห์แบบพรรณนา เป็นการวิเคราะห์ให้ทราบถึงผลประโยชน์ที่ชุมชนได้รับ และจากการเครื่องมือดังกล่าวพบว่า ผู้ใช้บริการส่วนใหญ่มีความพึงพอใจในการให้บริการของศูนย์การเรียนรู้ ICT ชุมชนร้อยละ 70 มีความพึงพอใจในการเข้าถึง สถานที่ตั้งศูนย์

บทที่ 3
วิธีดำเนินการวิจัย

การศึกษาครั้งนี้มุ่งศึกษาวิเคราะห์ความรู้และความเข้าใจของบุคลากรใน กองบัญชาการกองทัพไทย เกี่ยวกับพฤติกรรม ความเสี่ยง และความรู้ความเข้าใจ ของบุคลากรในการใช้ระบบงานสารสนเทศ ว่ามีพฤติกรรมความเสี่ยงต่อภัยคุกคามในการใช้ระบบงานสารสนเทศของ กองบัญชาการกองทัพไทย มากน้อยเพียงไร มีความเสี่ยงมากแค่ไหน และไปในทิศทางด้านใด เพื่อนำผลประโยชน์ที่ได้รับสำหรับข้อมูลนี้ ไปจัดการกับระบบการรักษาความปลอดภัยสารสนเทศ และจัดฝึกอบรมเจ้าหน้าที่ในการรักษาความมั่นคงปลอดภัยสารสนเทศ บุคลากร ของกองบัญชาการกองทัพไทย เนื้อหาของบทนี้กล่าวถึง ขั้นตอนการกำหนดกรอบแนวคิดในการศึกษา การกำหนดบุคลากรและวิธีสุ่มตัวอย่าง เครื่องมือที่ใช้ในการวิจัย เก็บรวบรวมข้อมูล วิเคราะห์ข้อมูล โดยมีรายละเอียดดังต่อไปนี้

3.1 ขั้นตอนการดำเนินการวิจัย

ขั้นตอนการดำเนินการวิจัย มีดังต่อไปนี้

1) กำหนดกรอบแนวคิดในการศึกษา
2) กำหนดบุคลากรและวิธีสุ่มตัวอย่าง
3) สร้างเครื่องมือในการวิจัย
4) เก็บรวบรวมข้อมูล
5) วิเคราะห์ข้อมูล
6) สรุปผลการศึกษาและข้อเสนอแนะ

3.2 กำหนดกรอบแนวคิดในการศึกษา

การศึกษานี้มุ่งศึกษาวิเคราะห์ความรู้และความเข้าใจของบุคลากรใน กองบัญชาการกองทัพไทย เกี่ยวกับพฤติกรรม ความเสี่ยง และความรู้ความเข้าใจ ของบุคลากรในการใช้ระบบงานสารสนเทศ ว่ามีพฤติกรรมความเสี่ยงต่อภัยคุกคามในการใช้ระบบงานสารสนเทศของกองบัญชาการกองทัพไทย มากน้อยเพียงไร มีความเสี่ยงมากแค่ไหน และไปในทิศทางด้านใด เพื่อนำผลประโยชน์ที่ได้รับสำหรับข้อมูลนี้ ไปประกอบการค้นหาช่องโหว่จุดอ่อนต่าง ๆ

และนำไปจัดการฝึกอบรมเจ้าหน้าที่ในการรักษาความมั่นคงปลอดภัยสารสนเทศ บุคลากร ของกองบัญชาการกองทัพไทย ต่อไป

3.3 กำหนดบุคลากรและวิธีสุ่มตัวอย่าง

บุคลากรที่ใช้ในการวิจัยครั้งนี้ ได้แก่ ข้าราชการกองบัญชาการกองทัพไทย จำนวน 18,519 คน ผู้วิจัยได้ทำการสุ่มตัวอย่างของข้าราชการกองบัญชาการกองทัพไทย จำนวน 392 คน โดยได้จากการคำนวณของสูตรของ ทาโร ยามาเน (Taro Yamane, 1973, น.125) ในการกำหนดตัวอย่าง โดยเลือกระดับความเชื่อมั่น 95% ค่าระดับความคลาดเคลื่อนยอมรับได้ไม่เกิน 5% หรือ 0.05 ของระดับนัยสำคัญ

การสุ่มตัวอย่างดังกล่าวของข้าราชการกองบัญชาการกองทัพไทยในแต่ละระดับได้ตามตารางดังต่อไปนี้

ตามวิธีของ ยามาเน่ (Taro Yamane)

$$n = \frac{N}{1 + Ne^2}$$

เมื่อ n คือ ขนาดกลุ่มตัวอย่าง

N คือ ขนาดประชากร

e คือ คลาดคลาดเคลื่อนของกลุ่มตัวอย่าง เช่น

ระดับความเชื่อมั่น90% สัดส่วนความคลาดเคลื่อนเท่ากับ 0.10

ระดับความเชื่อมั่น95% สัดส่วนความคลาดเคลื่อนเท่ากับ 0.05 (ปกตินิยมระดับความเชื่อมั่น 95%)

แทนค่าได้เท่ากับ

18,519/1+(18,519(0.0025))

18,519/1+46.29

= 39.160 จำนวน (392) สุ่มตัวอย่าง

ตารางที่ 3.3 ตารางแสดงจำนวนข้าราชการ และ กลุ่มตัวอย่างที่ได้

ข้าราชการกองบัญชาการกองทัพไทย	บุคลากร	กลุ่มตัวอย่าง
ข้าราชการทหารชั้นสัญญาบัตร	6,776	123
ข้าราชการทหารชั้นประทวน	11,234	211
ลูกจ้าง/พนักงานราชการ	509	58
รวม	18,519	329

3.4 สร้างเครื่องมือในการวิจัย

เครื่องมือที่ใช้ในการเก็บรวบรวมของงานค้นคว้าอิสระครั้งนี้ คือ แบบสอบถาม (Questionnaire) จำนวน 1 ชุด โดยให้กลุ่มตัวอย่างที่กำหนดไว้เป็นผู้ตอบคำถามเอง โดยคำถามจะเป็นลักษณะของคำถาม แบบปลายปิด (Close-ended Questionnaire) โดยจะออกแบบคำถามออกเป็นส่วนๆ ดังนี้

ส่วนที่ 1 คำถามเกี่ยวกับลักษณะทางบุคลากรของกลุ่มตัวอย่าง ข้อมูลทั่วไป อายุ เพศ ข้าราชการประเภท ระดับการศึกษา ลักษณะตำแหน่งงาน เป็นต้น

ส่วนที่ 2 คำถามพฤติกรรมการใช้ระบบอินทราเน็ตและอินเตอร์เน็ตภายในองค์กร

ส่วนที่ 3 แบบทดสอบความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ แบ่งเป็น 3 กลุ่ม ดังนี้ กลุ่มที่ 1 ทดสอบความรู้การรักษาความปลอดภัยสารสนเทศเกี่ยวกับข้อมูล กลุ่มที่ 2 ทดสอบความรู้การรักษาความปลอดภัยสารสนเทศเกี่ยวกับการป้องกัน Virus และช่องโหว่ด้านต่าง ๆ กลุ่มที่ 3 ทดสอบความรู้การรักษาความปลอดภัยสารสนเทศเกี่ยวกับด้านกฎหมาย ว่าด้วยการกระทำผิด พรบ. เกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 นโยบาย และระเบียบ ของ กองบัญชาการกองทัพไทย

ส่วนที่ 4 แบบทดสอบพฤติกรรมเสี่ยงต่อภัยคุกคามต่อเครือข่ายภายในกองบัญชาการกองทัพไทย

ส่วนที่ 5 ความคิดเห็นและข้อเสนอแนะอื่น ๆ เกี่ยวกับเรื่องระบบการรักษาความมั่นคงปลอดภัยสารสนเทศ ของ กองบัญชาการกองทัพไทย

การทดสอบเครื่องมือ ผู้ศึกษาได้นำแบบสอบถามที่สร้างขึ้นไปทดสอบหาความเที่ยงตรงและความเชื่อมัน ดังนี้

1) การหาความเที่ยงตรง (Validity) โดยการนำแบบสอบถามที่ผู้วิจัยได้จัดทำขึ้นไปเสนอต่ออาจารย์ที่ปรึกษา เพื่อพิจารณาตรวจสอบความถูกต้องในเนื้อหา (Content validity) นำมาแก้ไขข้อบกพร่อง

2) การทดสอบความเชื่อมั่น (Reliability) ของแบบสอบถามที่ปรับปรุงแก้ไขแล้ว ผู้ศึกษาจะทำการทดสอบ (Pre-Test) กับกลุ่มตัวอย่างที่คล้ายกับกลุ่มตัวอย่างจริง เพื่อทดสอบความเชื่อมั่นของแบบสอบถาม จำนวน 30 แบบสอบถาม โดยสิ่งที่จะพิจารณา ว่าผู้ตอบแบบสอบถามเข้าใจหรือไม่ มีปัญหาการตอบคำถามหรือไม่ และหลังจาก Pre-Test แล้ว พบว่าแบบสอบถามมีความเชื่อมั่น (Reliability) จึงนำไปใช้เป็นเครื่องมือในการเก็บรวบรวมข้อมูล

3.5 เก็บรวบรวมข้อมูล

การจัดเก็บข้อมูลของงานศึกษานี้ ผู้ศึกษาได้เก็บรวบรวมข้อมูลโดยออกแบบสอบถามที่สร้างไว้ไปสอบถามบุคลากรของ กองบัญชาการกองทัพไทย สุ่มไปยังพื้นที่หน่วยต่างๆให้ผู้ตอบกรอกแบบสอบถามเอง (Self-Administration)หลังจากกรอกเสร็จจะทำการรวบรวมผลเอาไว้ทันที และเมื่อได้จำนวนแบบสอบถามตามจำนวนที่ต้องการไว้แล้ว ผู้ศึกษาจะนำผลที่ได้มา ประมวลผลโดยโปรแกรมสาเร็จรูปทางสถิติ SPSS Statistics 17.0 เพื่อวิเคราะห์ข้อมูล

3.6 วิเคราะห์ข้อมูล

เมื่อได้รวบรวมข้อมูลเรียบร้อยแล้วในการศึกษาผู้ศึกษาได้ทำการลงรหัสและนำมาประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์ โดยการใช้โปรแกรมสาเร็จรูป SPSS Statistics 17.0 ซึ่งการวิเคราะห์ข้อมูล เพื่อนำเสนอและสรุปผลในการศึกษาครั้งนี้ได้ใช้การคำนวณค่าสถิติต่าง ๆ

1) สถิติเชิงพรรณนา (Descriptive Statistics) คือ เป็นสถิติที่ใช้ในการบรรยายหรืออธิบายลักษณะต่าง ๆ ในภาพรวมของกลุ่มตัวอย่างหรือบุคลากรที่ใช้ในการศึกษาเท่านั้น โดยไม่สนใจที่จะสรุปอ้างอิงไปยังบุคลากรอื่น อันได้แก่ ค่าร้อยละ ที่ผู้ศึกษากำหนดไว้ข้างต้น เพื่ออธิบายลักษณะบุคลากรภายในองค์กร ของกลุ่มตัวอย่าง อันได้แก่ เพศ อายุ ระดับประเภท และระดับการศึกษา เป็นต้น โดยจะนำเสนอรูปแบบเชิงบรรยาย เพื่ออธิบายข้อมูลที่ได้ของบุคลากรภายในองค์กร ของกลุ่มตัวอย่างต่อความรู้ ความเข้าใจ ในการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ ทางระบบคอมพิวเตอร์ ผ่านทางค่าร้อยละ (Percentage) เป็นข้อมูลประกอบการแปลความหมาย เชิงบรรยาย มีลักษณะเป็นแบบตรวจสอบรายการ (Check-List) ใช้วิธีการหาค่าความถี่ (Frequency) แล้วสรุปออกมาเป็นค่าร้อยละ (Percentage)

2) สถิติเชิงอนุมาน (Inferential Statistics) เพื่อทดสอบสมมติฐานเพื่อหาค่าความสัมพันธ์และความแตกต่างของตัวแปรโดยการใช้ค่าความถี่แบบสองทาง (Crosstabs) แล้ว สรุปออกมาเป็นค่าร้อยละ (Percentage)

3.7 สรุปผลการศึกษาและข้อเสนอแนะ

เป็นการสรุปถึงผลการศึกษาในหัวข้อเรื่อง ความรู้และความเข้าใจด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ กรณีศึกษา ข้าราชการ กองบัญชาการกองทัพไทย เกี่ยวกับพฤติกรรม ความรู้ความเข้าใจ ของกำลังพลในการใช้งานระบบสารสนเทศ เพื่อการรักษาความมั่นคงปลอดภัยสนเทศ ของ กองบัญชาการกองทัพไทย ว่ามีความรู้ในเรื่องต่าง ๆ มากน้อยเพียงใด และมีความเสี่ยงหรือไม่ เปรียบเทียบข้าราชการชั้นทุกระดับชั้น เปรียบเทียบกับข้าราชการที่ผ่านการฝึกอบรมมาแล้ว กับข้าราชการที่ยังไม่ผ่านการฝึกอบรม ว่ามีความรู้แตกต่างกันอย่างไร และมีพฤติกรรมความเสี่ยงต่อภัยคุกคามในการใช้ระบบงานสารสนเทศ ของ กองบัญชาการกองทัพไทย มากน้อยเพียงใด เพื่อนำมาใช้ในการหาช่องโหว่ และจัดการเปิดหลักสูตรการฝึกอบรมเกี่ยวกับ ความมั่นคงรักษาความปลอดภัยสารสนเทศ ในส่วนที่บุคลากรยังขาดความใส่ใจในการเรียนรู้ต่อไป บุคลากรจะได้มีการพัฒนา ความรู้และความเข้าใจ ปัจจัยสาเหตุที่ทำให้เกิดความเสียหายต่อความเสี่ยงต่างๆ ที่นำไปสู่ความเสียหาย แก่ ทางราชการ ของ กองบัญชาการกองทัพไทย

บทที่ 4
ผลการศึกษา

4.1 การนำเสนอผลการศึกษา

การศึกษาเรื่อง “ความรู้ ความเข้าใจ ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ กรณีศึกษา ข้าราชการกองบัญชาการกองทัพไทย” ในครั้งนี้ผู้วิจัยได้ใช้โปรแกรมสำเร็จรูปทางสถิติ SPSS Statistics 17.0 ในการประมวลผล จากกลุ่มตัวอย่าง จำนวนทั้งสิ้น 392 ชุด
โดยแบ่งออกเป็น 4 ตอน คือ

ตอนที่ 1 แสดงข้อมูลลักษณะทั่วไปของข้าราชการกองบัญชาการกองทัพไทย

ตอนที่ 2 แสดงข้อมูลพฤติกรรมการใช้ระบบอินทราเน็ตและอินเตอร์เน็ตในองค์กร

ตอนที่ 3 แสดงข้อมูลผลการทดสอบความรู้ความมั่นคงรักษาความปลอดภัยสารสนเทศ

1) เปรียบเทียบผลวิเคราะห์ระหว่างทดสอบความรู้ตามตำแหน่งหน้าที่

2) เปรียบเทียบผลวิเคราะห์ระหว่างทดสอบความรู้ของ ผู้เข้ารับการฝึกอบรม กับผู้ที่ไม่เคยผ่านการฝึกอบรม

ตอนที่ 4 แสดงข้อมูลผลการทดสอบความเสี่ยงต่อภัยคุกคามภายในองค์กร

1) เปรียบเทียบผลวิเคราะห์ระหว่างทดสอบความรู้ตามตำแหน่งหน้าที่

2) เปรียบเทียบผลวิเคราะห์ระหว่างทดสอบความรู้ของ ผู้เข้ารับการฝึกอบรม กับผู้ที่ไม่เคยผ่านการฝึกอบรม

4.2 ผลการศึกษา

ตอนที่ 1 แสดงข้อมูลลักษณะทั่วไปของข้าราชการกองบัญชาการกองทัพไทย
จากข้อมูลผลการศึกษาพบว่า ลักษณะทางด้านปัจจัยส่วนบุคคลของผู้ตอบแบบสอบถาม มีรายละเอียดดังนี้

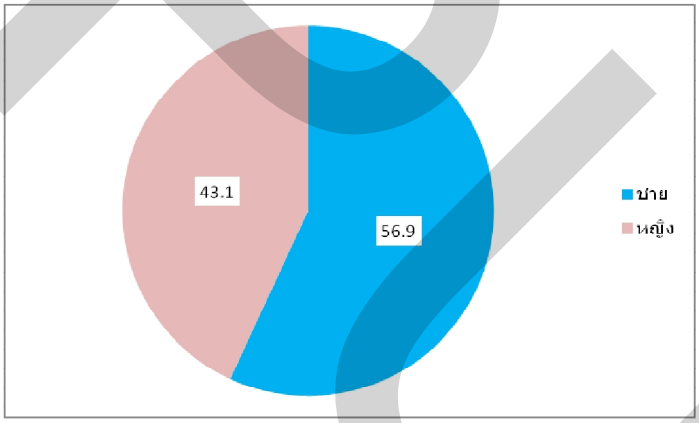
ตารางที่ 4.1 ผลการศึกษาข้อมูลปัจจัยส่วนบุคคล ด้านเพศ

เพศ

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ชาย	223	56.9	56.9	56.9
	หญิง	169	43.1	43.1	100.0
	Total	392	100.0	100.0	

ผลจากตารางที่ 4.1 แสดงให้เห็นถึง ผลการศึกษาข้อมูลปัจจัยส่วนบุคคล ด้านเพศ ของกลุ่มตัวอย่างผู้ตอบแบบสอบถามเป็น ข้าราชการ กองบัญชาการกองทัพไทย จำนวนทั้งสิ้น 392 คน พบว่าเป็นกลุ่มตัวอย่างที่ตอบแบบสอบถามเป็นเพศชาย จำนวน 223 คน คิดเป็นร้อยละ 56.9 และเป็นเพศหญิง จำนวน 169 คน คิดเป็นร้อยละ 43.1 สรุปได้ว่ากลุ่มตัวอย่างที่ตอบแบบสอบถามส่วนใหญ่เป็นเพศชายมากกว่าเป็นเพศหญิง

ภาพที่ 4.1 ผลการศึกษาข้อมูลปัจจัยส่วนบุคคล ด้านเพศ



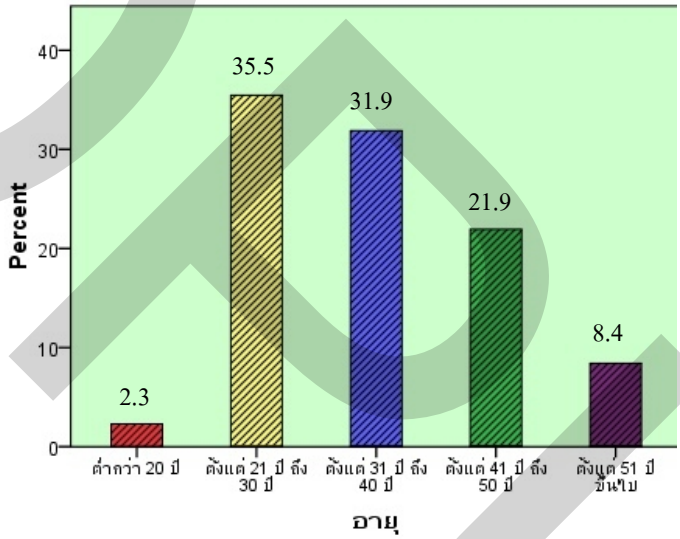
ตารางที่ 4.2 ผลการศึกษาข้อมูลปัจจัยส่วนบุคคล ด้านอายุ

อายุ

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ต่ำกว่า 20 ปี	9	2.3	2.3	2.3
	ตั้งแต่ 21 ปี ถึง 30 ปี	139	35.5	35.5	37.8
	ตั้งแต่ 31 ปี ถึง 40 ปี	125	31.9	31.9	69.6
	ตั้งแต่ 41 ปี ถึง 50 ปี	86	21.9	21.9	91.6
	ตั้งแต่ 51 ปี ขึ้นไป	33	8.4	8.4	100.0
	Total	392	100.0	100.0	

ผลจากตารางที่ 4.2 แสดงให้เห็นถึง ผลการศึกษาข้อมูลปัจจัยส่วนบุคคล ด้านอายุ ของกลุ่มตัวอย่างผู้ตอบแบบสอบถาม จำนวน 392 คน อายุต่ำกว่า 20 ปี จำนวน 9 คน คิดเป็นร้อยละ 2.3 อายุตั้งแต่ 21 ปี ถึง 30 ปี จำนวน 139 คน คิดเป็นร้อยละ 35.5 อายุตั้งแต่ 31 ปี ถึง 40 ปี จำนวน 125 คน คิดเป็นร้อยละ 31.9 อายุตั้งแต่ 41 ปี ถึง 50 ปี จำนวน 86 คน คิดเป็นร้อยละ 21.9 และอายุตั้งแต่ 51 ปีขึ้นไป จำนวน 33 คน คิดเป็นร้อยละ 8.4 สรุปได้ว่ากลุ่มตัวอย่างที่ตอบแบบสอบถามส่วนใหญ่จะมีอายุอยู่ในช่วง ตั้งแต่ 21 ปี ถึง 30 ปี มากที่สุด และอายุต่ำกว่า 20 ปี น้อยที่สุด

ภาพที่ 4.2 ผลการศึกษาข้อมูลปัจจัยส่วนบุคคล ด้านอายุ



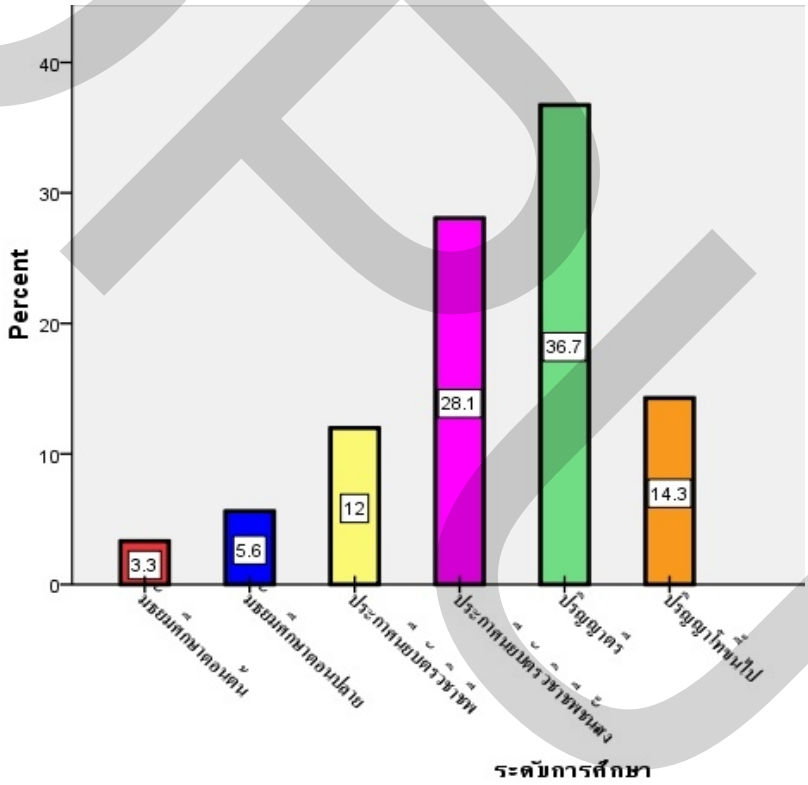
ตารางที่ 4.3 ผลการศึกษาข้อมูลปัจจัยส่วนบุคคล ด้านการศึกษา

ระดับการศึกษา

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ระดับมัธยมศึกษาตอนต้น	13	3.3	3.3	3.3
	ระดับมัธยมศึกษาตอนปลาย	22	5.6	5.6	8.9
	ระดับประกาศนียบัตรวิชาชีพ	47	12.0	12.0	20.9
	ระดับประกาศนียบัตรวิชาชีพชั้นสูง	110	28.1	28.1	49.0
	ระดับปริญญาตรี	144	36.7	36.7	85.7
	ระดับปริญญาโทขึ้นไป	56	14.3	14.3	100.0
	Total	392	100.0	100.0	

ผลจากตารางที่ 4.3 แสดงให้เห็นถึง ผลการศึกษาข้อมูลปัจจัยส่วนบุคคล ด้านการศึกษา ของกลุ่มตัวอย่างผู้ตอบแบบสอบถาม จำนวน 392 คน ระดับการศึกษามัธยมศึกษาตอนต้น จำนวน 13 คน คิดเป็นร้อยละ 3.3 ระดับการศึกษามัธยมศึกษาตอนปลาย จำนวน 22 คน คิดเป็นร้อยละ 5.6 ระดับการศึกษาประกาศนียบัตรวิชาชีพ จำนวน 47 คน คิดเป็นร้อยละ 12.0 ระดับการศึกษาประกาศนียบัตรวิชาชีพชั้นสูง จำนวน 110 คน คิดเป็นร้อยละ 28.1 ระดับการศึกษาปริญญาตรี จำนวน 144 คน คิดเป็นร้อยละ 28.1 และระดับการศึกษาปริญญาโทขึ้นไป จำนวน 56 คน คิดเป็นร้อยละ 14.3 สรุปได้ว่ากลุ่มตัวอย่างที่ตอบแบบสอบถามส่วนใหญ่จะมีระดับการศึกษาปริญญาตรี มากที่สุด และระดับการศึกษามัธยมศึกษาตอนต้นน้อยที่สุด

ภาพที่ 4.3 ผลการศึกษาข้อมูลปัจจัยส่วนบุคคล ด้านการศึกษา



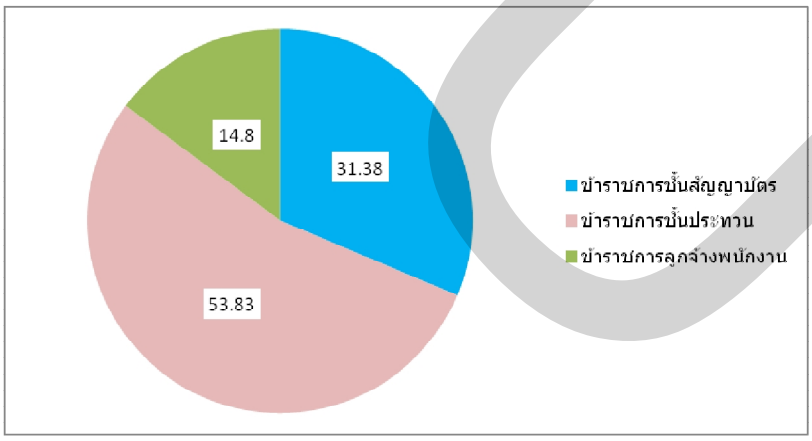
ตารางที่ 4.4 ผลการศึกษาข้อมูลปัจจัยส่วนบุคคล ด้านระดับหน้าที่การทำงาน

ระดับหน้าที่ทำงาน

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ระดับข้าราชการชั้นสัญญาบัตร	123	31.4	31.4	31.4
	ระดับข้าราชการชั้นประทวน	211	53.8	53.8	85.2
	ระดับข้าราชการลูกจ้างพนักงานราชการ	58	14.8	14.8	100.0
	Total	392	100.0	100.0	

ผลจากตารางที่ 4.4 แสดงให้เห็นถึง ผลการศึกษาข้อมูลปัจจัยส่วนบุคคล ด้านระดับหน้าที่การทำงานของกลุ่มตัวอย่างผู้ตอบแบบสอบถาม จำนวน 392 คน ระดับข้าราชการชั้นสัญญาบัตร จำนวน 123 คน คิดเป็นร้อยละ 31.4 ระดับข้าราชการชั้นประทวน จำนวน 211 คน คิดเป็นร้อยละ 53.8 และระดับข้าราชการลูกจ้างพนักงาน จำนวน 58 คน คิดเป็นร้อยละ 14.8 สรุปได้ว่ากลุ่มตัวอย่างที่ตอบแบบสอบถามส่วนใหญ่จะมีระดับข้าราชการชั้นประทวนมากที่สุด และระดับข้าราชการลูกจ้างพนักงานราชการน้อยที่สุด

ภาพที่ 4.4 ผลการศึกษาข้อมูลปัจจัยส่วนบุคคล ด้านระดับหน้าที่การทำงาน



ตารางที่ 4.5 ผลการศึกษาข้อมูลปัจจัยส่วนบุคคล ด้านหลักสูตรการฝึกอบรม

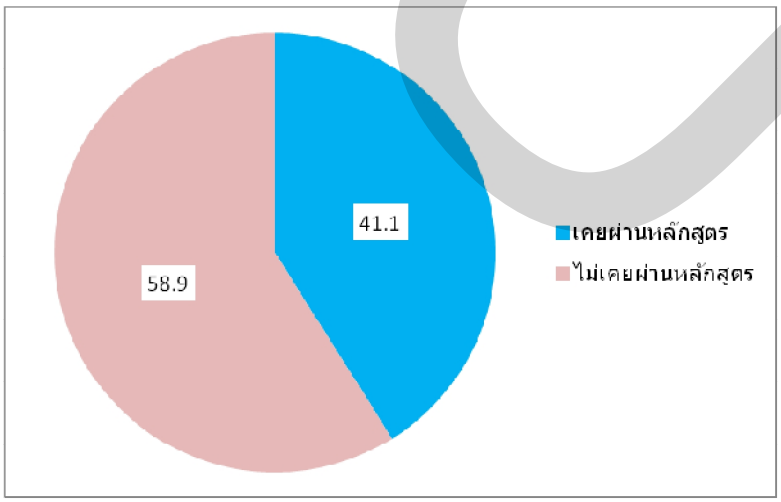
การฝึกอบรม

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	เคยผ่านหลักสูตร	161	41.1	41.1	41.1
	ไม่เคยผ่านหลักสูตร	231	58.9	58.9	100.0
	Total	392	100.0	100.0	

ผลจากตารางที่ 4.5 แสดงให้เห็นถึง ผลการศึกษาข้อมูลของกลุ่มตัวอย่างด้านการผ่านการศึกษาอบรมการรักษาความมั่นคงปลอดภัยสารสนเทศ ที่ทางกรมการสื่อสารทหาร จัดให้มีการฝึกอบรมเพื่อเพิ่มพูนความรู้ให้กับเจ้าหน้าที่ มีกำลังพลที่ผ่านการฝึกอบรมหลักสูตรการรักษาความมั่นคงปลอดภัยสารสนเทศ จำนวนทั้งสิ้น 161 คน คิดเป็นร้อยละ 41.1 และผู้ที่ไม่ได้ผ่านการฝึกอบรมหลักสูตรการรักษาความมั่นคงปลอดภัยสารสนเทศจากกลุ่มตัวอย่าง มีจำนวนทั้งสิ้น 231คน คิดเป็นร้อยละ 58.9 จากตารางที่ 4.5 จะเห็นได้ว่ายังมีบุคลากรข้าราชการอีกจำนวนมากที่ยังไม่ได้รับการเข้าฝึกอบรมหลักสูตรการรักษาความมั่นคงสารสนเทศ ดังกล่าว

ตอนที่ 2 แสดงข้อมูลพฤติกรรมการใช้ระบบอินทราเน็ตและอินเตอร์เน็ตภายในองค์กรของข้าราชการกองบัญชาการกองทัพไทย จากข้อมูลผลการศึกษาพบว่า ลักษณะทางด้านพฤติกรรมการใช้งานคอมพิวเตอร์ในระบบเครือข่ายของผู้ตอบแบบสอบถาม มีรายละเอียดดังนี้

ภาพที่ 4.5 ผลการศึกษาข้อมูลปัจจัยส่วนบุคคล ด้านหลักสูตรการฝึกอบรม



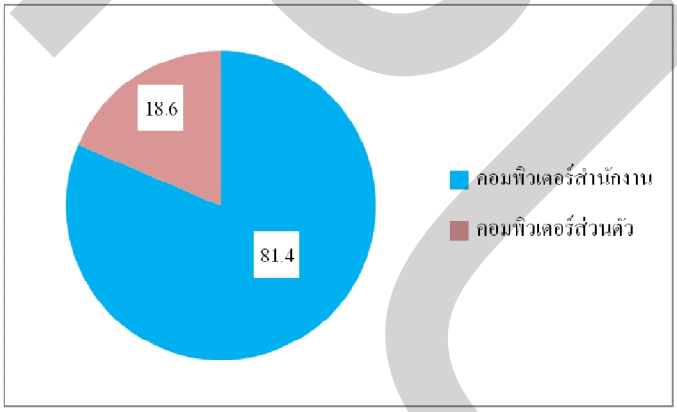
ตารางที่ 4.6 ผลการศึกษาข้อมูลพฤติกรรมการใช้งานภายในองค์กรด้านการใช้เครื่องคอมพิวเตอร์

ใช้คอมพิวเตอร์

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	สำนักงาน	319	81.4	81.4	81.4
	ส่วนตัว	73	18.6	18.6	100.0
	Total	392	100.0	100.0	

ผลจากตารางที่ 4.6 แสดงให้เห็นว่าจำนวนกลุ่มตัวอย่างของข้าราชการกองบัญชาการกองทัพไทยทั้งสิ้น 392 คน มีผู้ที่ใช้คอมพิวเตอร์ของทางราชการเพื่อใช้เชื่อมต่อผ่านเครือข่ายของ กองบัญชาการกองทัพไทย จำนวน 319 คน คิดเป็นร้อยละ 81.4 และอีกบางส่วนเป็นข้าราชการที่ นำ Notebook ส่วนตัวมาใช้เพื่อทำงานเอง จำนวน 73 คน คิดเป็นร้อยละ 18.6 เพื่อสะดวกแก่การทำงานและความคล่องตัว ในการจัดทำเอกสารงานเสนอเพื่อเข้าประชุม

ภาพที่ 4.6 ผลการศึกษาข้อมูลพฤติกรรมการใช้งานภายในองค์กรด้านการใช้เครื่องคอมพิวเตอร์



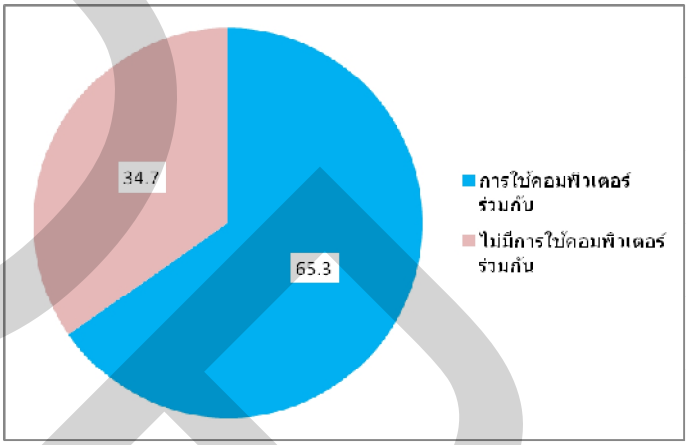
ตารางที่ 4.7 ผลการศึกษาข้อมูลพฤติกรรมการใช้งานเครื่องคอมพิวเตอร์**ร่วมกัน**

คนมาใช้ร่วม

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	มีคนมาใช้ร่วม	256	65.3	65.3	65.3
	ไม่มีคนมาใช้ร่วม	136	34.7	34.7	100.0
	Total	392	100.0	100.0	

ผลจากตารางที่ 4.7 แสดงให้เห็นว่าจำนวนกลุ่มตัวอย่างของข้าราชการกองบัญชาการกองทัพไทยทั้งสิ้น 392 คน มีผู้มาใช้เครื่องร่วมในการทำงาน จำนวน 256 คน คิดเป็นร้อยละ 65.3 และนอกนั้นอีก จำนวน 136 คน ไม่มีคนอื่นมาร่วมใช้งานด้วย คิดเป็นร้อยละ 34.7

ภาพที่ 4.7 ผลการศึกษาข้อมูลพฤติกรรมการใช้งานเครื่องคอมพิวเตอร์**ร่วมกัน**



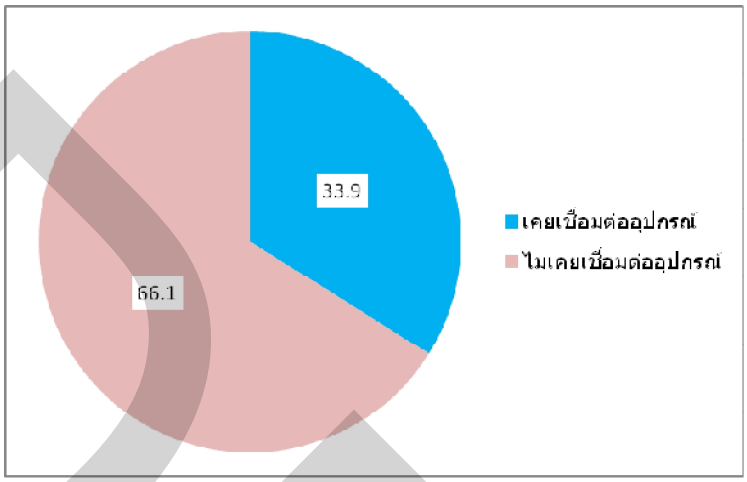
ตารางที่ 4.8 ผลการศึกษาข้อมูลพฤติกรรมการเชื่อมต่อภายในองค์กร

ใช้อุปกรณ์ชนิดอื่นเชื่อมต่อ

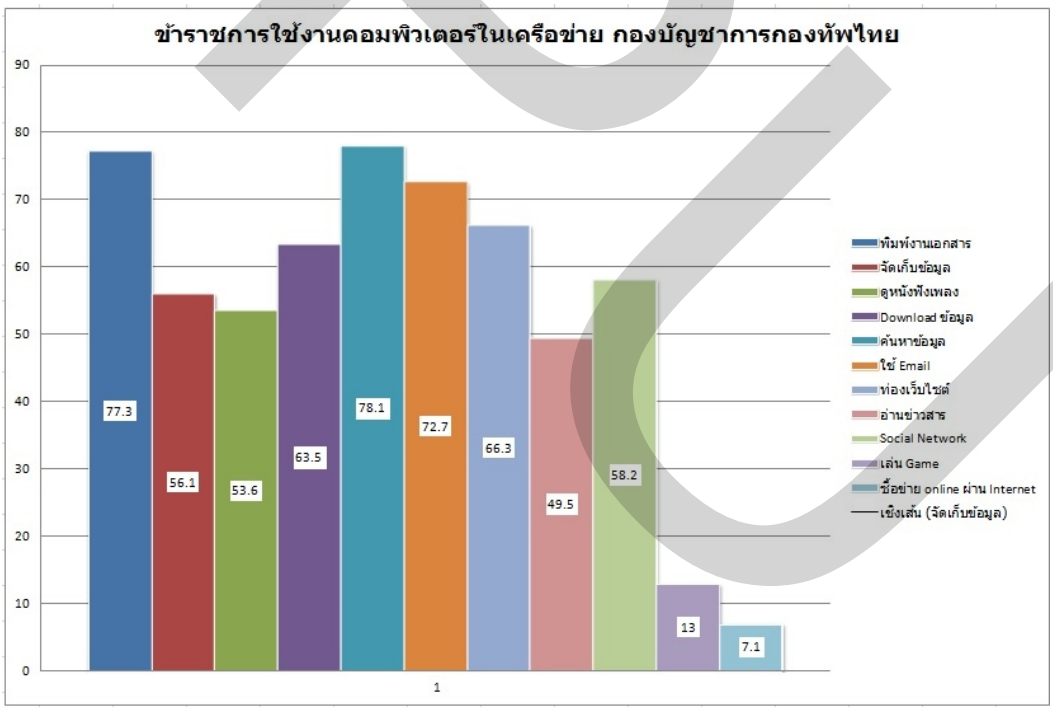
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	เคยนำเชื่อมต่อ	133	33.9	33.9	33.9
	ไม่เคยเชื่อมต่อ	259	66.1	66.1	100.0
	Total	392	100.0	100.0	

ผลจากตารางที่ 4.8 แสดงให้เห็นว่าจำนวนกลุ่มตัวอย่างของข้าราชการกองบัญชาการกองทัพไทยทั้งสิ้น 392 คน มีผู้ที่เคยใช้อุปกรณ์สื่อสารชนิดอื่นมาเชื่อมต่อในเครือข่ายของ กองบัญชาการกองทัพไทย จำนวนทั้งสิ้น 133 คน คิดเป็นร้อยละ 33.9 และอีก 259 คน ไม่เคยนำอุปกรณ์สื่อสารชนิดอื่นมาเชื่อมต่อในเครือข่าย คิดเป็นร้อยละ 66.1

ภาพที่ 4.8 ผลการศึกษาข้อมูลพฤติกรรมการเชื่อมต่อภายในองค์กร



ภาพที่ 4.9 ผลการศึกษาข้อมูลพฤติกรรมการใช้งานเครื่องคอมพิวเตอร์ภายในองค์กร



ผลจากภาพที่ 4.9 แสดงให้เห็นว่าจำนวนกลุ่มตัวอย่างของข้าราชการกองบัญชาการกองทัพไทยทั้งสิ้น 392 คน มีผู้ที่ใช้งานคอมพิวเตอร์ในเครือข่ายของ กองบัญชาการกองทัพไทย

1) ในการพิมพ์งานด้านเอกสาร มีจำนวน 303 คน คิดเป็นร้อยละ 77.3

2) ในการจัดเก็บข้อมูล มีจำนวน 220 คน คิดเป็นร้อยละ 56.1

3) ในการดูหนังฟังเพลง มีจำนวน 210 คน คิดเป็นร้อยละ 53.6

4) ในการDownload ข้อมูล มีจำนวน 249 คน คิดเป็นร้อยละ 63.5

5) ในการค้นหาข้อมูล มีจำนวน 306 คน คิดเป็นร้อยละ 78.1

6) ในการใช้ Email ติดต่อสื่อสาร มีจำนวน 285 คน คิดเป็นร้อยละ 72.1

7) ในการท่องเว็บไซต์ มีจำนวน 260 คน คิดเป็นร้อยละ 66.3

8) ในการอ่านข่าวสารข้อมูล มีจำนวน 194 คน คิดเป็นร้อยละ 49.5

9) ในการเล่น Social Network มีจำนวน 228 คน คิดเป็นร้อยละ 58.2

10) ในการเล่นGame มีจำนวน 51 คน คิดเป็นร้อยละ 13.0

11) ในการซื้อขาย online ผ่าน เครือข่าย มีจำนวน 28 คน คิดเป็นร้อยละ 7.1

ตอนที่ 3 แสดงข้อมูลของการทดสอบความรู้ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ของข้าราชการกองบัญชาการกองทัพไทย ว่าโดยภาพรวมโดยเฉลี่ยแล้ว ข้าราชการกองบัญชาการกองทัพไทย มีความรู้มากน้อยเพียงใดในเรื่อง ต่าง ๆ จำแนกแบ่งออกเป็น 3 กลุ่มใหญ่

1) ความรู้ด้านที่เกี่ยวกับข้อมูลการรักษาข้อมูล

2) ความรู้ด้านที่เกี่ยวกับ ภัยคุกคาม ระบบการป้องกันภัยคุกคาม

3) ความรู้ด้านที่เกี่ยวกับ นโยบาย ข้อกฎหมาย กฎระเบียบข้อบังคับต่าง ๆ

โดยที่แต่ละแบบทดสอบความรู้ จะแบ่งเป็น กลุ่มละ 5 คำถาม เป็นเกณฑ์การวัดความรู้เฉพาะเรื่อง ที่ผู้ตอบแบบสอบถามจากกลุ่มตัวอย่าง ได้ผ่านการทดสอบ เพื่อวัดความรู้ในแต่ละด้านของข้าราชการกองบัญชาการกองทัพไทย จากข้อมูลผลการศึกษาพบว่า ลักษณะทางด้านความรู้ในแต่ละด้าน ถ้าผลที่ได้เกิดขึ้นในจำนวน 5 ข้อ ของคำถาม โดยเฉลี่ยแล้ว จากจำนวนข้อที่ถูกต้อง

ถ้าตอบได้ 1 ข้อ ให้ผลออกมาเป็นอยู่ในเกณฑ์ที่ น้อยที่สุด

ถ้าตอบได้ 2 ข้อ ให้ผลออกมาเป็นอยู่ในเกณฑ์ที่ น้อย

ถ้าตอบได้ 3 ข้อ ให้ผลออกมาเป็นอยู่ในเกณฑ์ที่ ปานกลาง

ถ้าตอบได้ 4 ข้อ ให้ผลออกมาเป็นอยู่ในเกณฑ์ที่ มาก

ถ้าตอบได้ 5 ข้อ ให้ผลออกมาเป็นอยู่ในเกณฑ์ที่ มากที่สุด

รายละเอียดมีดังต่อไปนี้ตามตาราง

ตารางที่ 4.10 ผลการทดสอบความรู้ด้านที่เกี่ยวกับข้อมูลการรักษาข้อมูล

ข้อ1 ข้อมูล

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ผิด	113	28.8	28.8	28.8
	ถูก	279	71.2	71.2	100.0
	Total	392	100.0	100.0	

ข้อ2 ข้อมูล

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ผิด	169	43.1	43.1	43.1
	ถูก	223	56.9	56.9	100.0
	Total	392	100.0	100.0	

ข้อ3 ข้อมูล

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ผิด	133	33.9	33.9	33.9
	ถูก	259	66.1	66.1	100.0
	Total	392	100.0	100.0	

ข้อ4 ข้อมูล

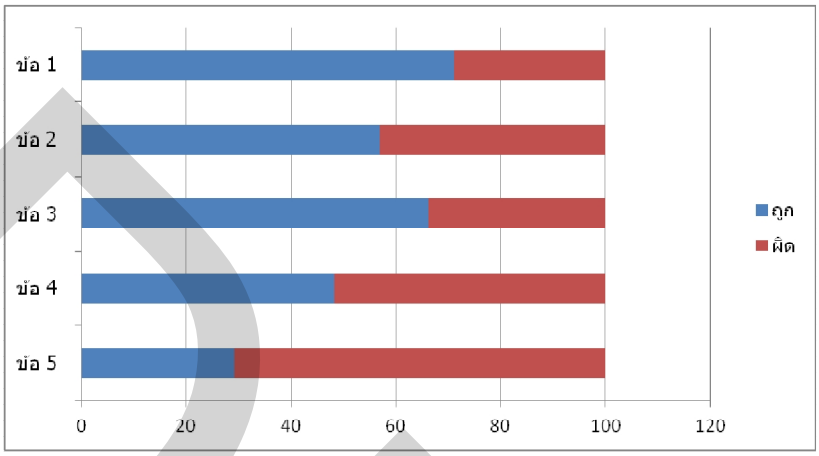
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ผิด	203	51.8	51.8	51.8
	ถูก	189	48.2	48.2	100.0
	Total	392	100.0	100.0	

ข้อ5 ข้อมูล

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ผิด	278	70.9	70.9	70.9
	ถูก	114	29.1	29.1	100.0
	Total	392	100.0	100.0	

ผลจากตารางที่ 4.10 แสดงให้เห็นว่าจำนวนกลุ่มตัวอย่างของข้าราชการกองบัญชาการกองทัพไทยทั้งสิ้น 392 คน ส่วนมากตอบข้อที่ถูกต้อง ผ่านการทดสอบด้านความรู้ด้านที่เกี่ยวกับข้อมูลการรักษาข้อมูล ที่เกินจำนวน ร้อยละ 50.0 ขึ้นไป มีจำนวนทั้งสิ้น 3 ข้อ จากรายงานผลในแต่ละข้อ ข้อ 1 ร้อยละ 71.2 ข้อ 2 ร้อยละ 56.9 ข้อ 3 ร้อยละ 66.1 ข้อ 4 ร้อยละ 48.2 ข้อ 5 ร้อยละ 29.1 แสดงว่าข้าราชการกองบัญชาการกองทัพไทย จากกลุ่มตัวอย่างที่นำมาทดสอบผ่านเกณฑ์ มีความรู้ความเข้าใจในด้านที่เกี่ยวกับข้อมูลการรักษาข้อมูล อยู่ในเกณฑ์ที่ปานกลาง

ภาพที่ 4.10 ผลการทดสอบความรู้ด้านที่เกี่ยวกับข้อมูลการรักษาข้อมูล



ตารางที่ 4.11 ผลการทดสอบความรู้ด้านที่เกี่ยวกับ ภัยคุกคาม ระบบการป้องกันภัยคุกคาม

ข้อ1 Virus

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ผิด	288	73.5	73.5	73.5
	ถูก	104	26.5	26.5	100.0
	Total	392	100.0	100.0	

ข้อ2 Virus

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ผิด	55	14.0	14.0	14.0
	ถูก	337	86.0	86.0	100.0
	Total	392	100.0	100.0	

ข้อ3 Virus

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ผิด	165	42.1	42.1	42.1
	ถูก	227	57.9	57.9	100.0
	Total	392	100.0	100.0	

ข้อ4 Virus

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ผิด	135	34.4	34.4	34.4
	ถูก	257	65.6	65.6	100.0
	Total	392	100.0	100.0	

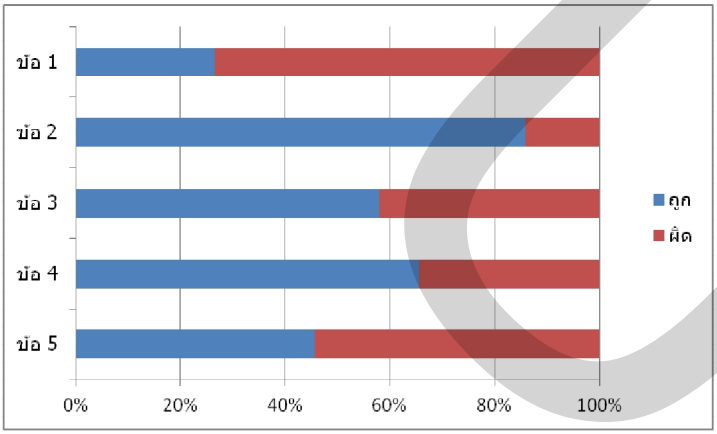
ตารางที่ 4.11 (ต่อ)

ข้อ5 Virus

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ผิด	213	54.3	54.3	54.3
	ถูก	179	45.7	45.7	100.0
	Total	392	100.0	100.0	

ผลจากตารางที่ 4.11 แสดงให้เห็นว่าจำนวนกลุ่มตัวอย่างของข้าราชการกองบัญชาการกองทัพไทยทั้งสิ้น 392 คน ส่วนมากตอบข้อที่ถูกต้อง ผ่านการทดสอบด้านความรู้ด้านที่เกี่ยวกับ ภัยคุกคาม ระบบการป้องกันภัยคุกคาม ที่เกินจำนวน ร้อยละ 50.0 ขึ้นไป มีจำนวนทั้งสิ้น 3 ข้อ จากรายงานผลในแต่ละข้อ ข้อ 1 ร้อยละ 26.5 ข้อ 2 ร้อยละ 86.0 ข้อ 3 ร้อยละ 57.9 ข้อ 4 ร้อยละ 65.6 ข้อ 5 ร้อยละ 45.7 แสดงว่าข้าราชการกองบัญชาการกองทัพไทย จากกลุ่มตัวอย่างที่นำมาทดสอบผ่านเกณฑ์ มีความรู้ความเข้าใจในด้านที่เกี่ยวกับ ภัยคุกคาม ระบบการป้องกันภัยคุกคาม อยู่ในเกณฑ์ที่ปานกลาง

ภาพที่ 4.11 ผลการทดสอบความรู้ด้านที่เกี่ยวกับ ภัยคุกคาม ระบบการป้องกันภัยคุกคาม



ตารางที่ 4.12 ผลการทดสอบความรู้ด้านที่เกี่ยวกับ นโยบาย ข้อกฎหมาย กฎระเบียบข้อบังคับต่าง ๆ

ข้อ1 กฎหมายนโยบาย

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ผิด	274	69.9	69.9	69.9
	ถูก	118	30.1	30.1	100.0
	Total	392	100.0	100.0	

ข้อ2 กฎหมายนโยบาย

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ผิด	202	51.5	51.5	51.5
	ถูก	190	48.5	48.5	100.0
	Total	392	100.0	100.0	

ข้อ3 กฎหมายนโยบาย

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ผิด	217	55.4	55.4	55.4
	ถูก	175	44.6	44.6	100.0
	Total	392	100.0	100.0	

ข้อ4 กฎหมายนโยบาย

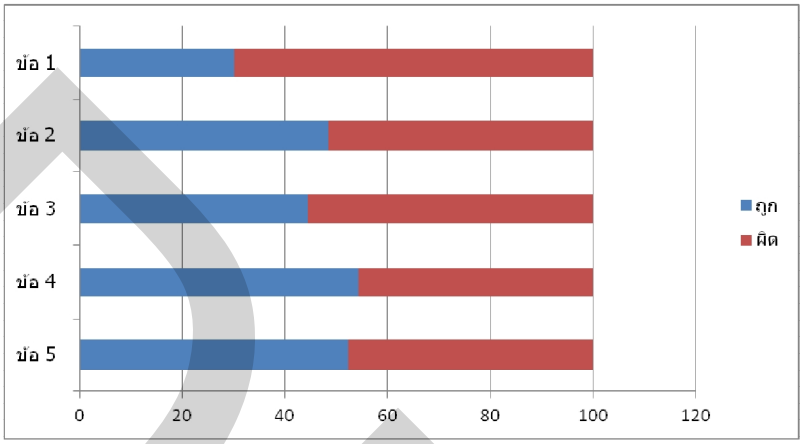
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ผิด	179	45.7	45.7	45.7
	ถูก	213	54.3	54.3	100.0
	Total	392	100.0	100.0	

ข้อ5 กฎหมายนโยบาย

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ผิด	187	47.7	47.7	47.7
	ถูก	205	52.3	52.3	100.0
	Total	392	100.0	100.0	

ผลจากตารางที่ 4.12 แสดงให้เห็นว่าจำนวนกลุ่มตัวอย่างของข้าราชการกองบัญชาการกองทัพไทยทั้งสิ้น 392 คน ส่วนมากตอบข้อที่ถูกต้อง ผ่านการทดสอบด้านความรู้ด้านที่เกี่ยวกับ นโยบาย ข้อกฎหมาย กฎระเบียบข้อบังคับต่าง ๆ ที่เกินจำนวน ร้อยละ 50.0 ขึ้นไป มีจำนวนทั้งสิ้น 2 ข้อ จากรายงานผลในแต่ละข้อ ข้อ 1 ร้อยละ 30.1 ข้อ 2 ร้อยละ 48.5 ข้อ 3 ร้อยละ 44.6 ข้อ 4 ร้อยละ 54.3 ข้อ 5 ร้อยละ 52.3 แสดงว่าข้าราชการกองบัญชาการกองทัพไทย จากกลุ่มตัวอย่างที่นำมาทดสอบผ่านเกณฑ์ มีความรู้ด้านที่เกี่ยวกับ นโยบาย ข้อกฎหมาย กฎระเบียบข้อบังคับต่าง ๆ อยู่ในเกณฑ์ที่น้อย

ภาพที่ 4.12 ผลการทดสอบความรู้ด้านที่เกี่ยวกับ นโยบาย ข้อกฎหมาย กฎระเบียบข้อบังคับต่าง ๆ



ตารางที่ 4.13 ผลการทดสอบความรู้เปรียบเทียบผลวิเคราะห์ระหว่างทดสอบความรู้ตามตำแหน่งหน้าที่

4.13.1 ด้านข้อมูล

ข้อ1 ข้อมูล * ระดับหน้าที่ทำงาน Crosstabulation

			ระดับหน้าที่ทำงาน			
			ระดับข้าราชการชั้นสัญญาบัตร	ระดับข้าราชการชั้นประทวน	ระดับข้าราชการลูกจ้างพนักงานราชการ	Total
ข้อ1 ข้อมูล	ผิด	Count	8	82	23	113
		% within ระดับหน้าที่ทำงาน	6.5%	38.9%	39.7%	28.8%
	ถูก	Count	115	129	35	279
		% within ระดับหน้าที่ทำงาน	93.5%	61.1%	60.3%	71.2%
Total		Count	123	211	58	392
		% within ระดับหน้าที่ทำงาน	100.0%	100.0%	100.0%	100.0%

ข้อ2 ข้อมูล * ระดับหน้าที่ทำงาน Crosstabulation

			ระดับหน้าที่ทำงาน			
			ระดับข้าราชการชั้นสัญญาบัตร	ระดับข้าราชการชั้นประทวน	ระดับข้าราชการลูกจ้างพนักงานราชการ	Total
ข้อ2 ข้อมูล	ผิด	Count	28	107	34	169
		% within ระดับหน้าที่ทำงาน	22.8%	50.7%	58.6%	43.1%
	ถูก	Count	95	104	24	223
		% within ระดับหน้าที่ทำงาน	77.2%	49.3%	41.4%	56.9%
Total		Count	123	211	58	392
		% within ระดับหน้าที่ทำงาน	100.0%	100.0%	100.0%	100.0%

ตารางที่ 4.13 (ต่อ)

ข้อ3 ข้อมูล * ระดับหน้าที่ทำงาน Crosstabulation

			ระดับหน้าที่ทำงาน			
			ระดับข้าราชการชั้นสัญญาบัตร	ระดับข้าราชการชั้นประทวน	ระดับข้าราชการลูกจ้างพนักงานราชการ	Total
ข้อ3 ข้อมูล	ผิด	Count	30	83	20	133
		% within ระดับหน้าที่ทำงาน	24.4%	39.3%	34.5%	33.9%
	ถูก	Count	93	128	38	259
		% within ระดับหน้าที่ทำงาน	75.6%	60.7%	65.5%	66.1%
Total		Count	123	211	58	392
		% within ระดับหน้าที่ทำงาน	100.0%	100.0%	100.0%	100.0%

ข้อ4 ข้อมูล * ระดับหน้าที่ทำงาน Crosstabulation

			ระดับหน้าที่ทำงาน			
			ระดับข้าราชการชั้นสัญญาบัตร	ระดับข้าราชการชั้นประทวน	ระดับข้าราชการลูกจ้างพนักงานราชการ	Total
ข้อ4 ข้อมูล	ผิด	Count	65	105	33	203
		% within ระดับหน้าที่ทำงาน	52.8%	49.8%	56.9%	51.8%
	ถูก	Count	58	106	25	189
		% within ระดับหน้าที่ทำงาน	47.2%	50.2%	43.1%	48.2%
Total		Count	123	211	58	392
		% within ระดับหน้าที่ทำงาน	100.0%	100.0%	100.0%	100.0%

ข้อ5 ข้อมูล * ระดับหน้าที่ทำงาน Crosstabulation

			ระดับหน้าที่ทำงาน			
			ระดับข้าราชการชั้นสัญญาบัตร	ระดับข้าราชการชั้นประทวน	ระดับข้าราชการลูกจ้างพนักงานราชการ	Total
ข้อ5 ข้อมูล	ผิด	Count	59	167	52	278
		% within ระดับหน้าที่ทำงาน	48.0%	79.1%	89.7%	70.9%
	ถูก	Count	64	44	6	114
		% within ระดับหน้าที่ทำงาน	52.0%	20.9%	10.3%	29.1%
Total		Count	123	211	58	392
		% within ระดับหน้าที่ทำงาน	100.0%	100.0%	100.0%	100.0%

ตารางที่ 4.13 (ต่อ)

4.13.2 ด้านเกี่ยวกับ ภัยคุกคาม ระบบการป้องกันภัยคุกคาม

ข้อ1 Virus * ระดับหน้าที่ทำงาน Crosstabulation

			ระดับหน้าที่ทำงาน			
			ระดับข้าราชการชั้นสัญญาบัตร	ระดับข้าราชการชั้นประทวน	ระดับข้าราชการลูกจ้างพนักงานราชการ	Total
ข้อ1 Virus	ผิด	Count	68	166	54	288
		% within ระดับหน้าที่ทำงาน	55.3%	78.7%	93.1%	73.5%
	ถูก	Count	55	45	4	104
		% within ระดับหน้าที่ทำงาน	44.7%	21.3%	6.9%	26.5%
Total		Count	123	211	58	392
		% within ระดับหน้าที่ทำงาน	100.0%	100.0%	100.0%	100.0%

ข้อ2 Virus * ระดับหน้าที่ทำงาน Crosstabulation

			ระดับหน้าที่ทำงาน			
			ระดับข้าราชการชั้นสัญญาบัตร	ระดับข้าราชการชั้นประทวน	ระดับข้าราชการลูกจ้างพนักงานราชการ	Total
ข้อ2 Virus	ผิด	Count	5	42	8	55
		% within ระดับหน้าที่ทำงาน	4.1%	19.9%	13.8%	14.0%
	ถูก	Count	118	169	50	337
		% within ระดับหน้าที่ทำงาน	95.9%	80.1%	86.2%	86.0%
Total		Count	123	211	58	392
		% within ระดับหน้าที่ทำงาน	100.0%	100.0%	100.0%	100.0%

ข้อ3 Virus * ระดับหน้าที่ทำงาน Crosstabulation

			ระดับหน้าที่ทำงาน			
			ระดับข้าราชการชั้นสัญญาบัตร	ระดับข้าราชการชั้นประทวน	ระดับข้าราชการลูกจ้างพนักงานราชการ	Total
ข้อ3 Virus	ผิด	Count	50	93	22	165
		% within ระดับหน้าที่ทำงาน	40.7%	44.1%	37.9%	42.1%
	ถูก	Count	73	118	36	227
		% within ระดับหน้าที่ทำงาน	59.3%	55.9%	62.1%	57.9%
Total		Count	123	211	58	392
		% within ระดับหน้าที่ทำงาน	100.0%	100.0%	100.0%	100.0%

ข้อ4 Virus * ระดับหน้าที่ทำงาน Crosstabulation

			ระดับหน้าที่ทำงาน			
			ระดับข้าราชการชั้นสัญญาบัตร	ระดับข้าราชการชั้นประทวน	ระดับข้าราชการลูกจ้างพนักงานราชการ	Total
ข้อ4 Virus	ผิด	Count	21	88	26	135
		% within ระดับหน้าที่ทำงาน	17.1%	41.7%	44.8%	34.4%
	ถูก	Count	102	123	32	257
		% within ระดับหน้าที่ทำงาน	82.9%	58.3%	55.2%	65.6%
Total		Count	123	211	58	392
		% within ระดับหน้าที่ทำงาน	100.0%	100.0%	100.0%	100.0%

ตารางที่ 4.13 (ต่อ)

ข้อ5 Virus * ระดับหน้าที่ทำงาน Crosstabulation

			ระดับหน้าที่ทำงาน			Total
			ระดับข้าราชการชั้นสัญญาบัตร	ระดับข้าราชการชั้นประทวน	ระดับข้าราชการลูกจ้างพนักงานราชการ	
ข้อ5 Virus	ผิด	Count	53	135	25	213
		% within ระดับหน้าที่ทำงาน	43.1%	64.0%	43.1%	54.3%
	ถูก	Count	70	76	33	179
		% within ระดับหน้าที่ทำงาน	56.9%	36.0%	56.9%	45.7%
Total		Count	123	211	58	392
		% within ระดับหน้าที่ทำงาน	100.0%	100.0%	100.0%	100.0%

4.13.3 ด้านนโยบาย ข้อกฎหมาย กฎระเบียบข้อบังคับต่าง ๆ

ข้อ1 กฎหมายนโยบาย * ระดับหน้าที่ทำงาน Crosstabulation

			ระดับหน้าที่ทำงาน			Total
			ระดับข้าราชการชั้นสัญญาบัตร	ระดับข้าราชการชั้นประทวน	ระดับข้าราชการลูกจ้างพนักงานราชการ	
ข้อ1 กฎหมายนโยบาย	ผิด	Count	63	172	39	274
		% within ระดับหน้าที่ทำงาน	51.2%	81.5%	67.2%	69.9%
	ถูก	Count	60	39	19	118
		% within ระดับหน้าที่ทำงาน	48.8%	18.5%	32.8%	30.1%
Total		Count	123	211	58	392
		% within ระดับหน้าที่ทำงาน	100.0%	100.0%	100.0%	100.0%

ข้อ2 กฎหมายนโยบาย * ระดับหน้าที่ทำงาน Crosstabulation

			ระดับหน้าที่ทำงาน			Total
			ระดับข้าราชการชั้นสัญญาบัตร	ระดับข้าราชการชั้นประทวน	ระดับข้าราชการลูกจ้างพนักงานราชการ	
ข้อ2 กฎหมายนโยบาย	ผิด	Count	50	116	36	202
		% within ระดับหน้าที่ทำงาน	40.7%	55.0%	62.1%	51.5%
	ถูก	Count	73	95	22	190
		% within ระดับหน้าที่ทำงาน	59.3%	45.0%	37.9%	48.5%
Total		Count	123	211	58	392
		% within ระดับหน้าที่ทำงาน	100.0%	100.0%	100.0%	100.0%

ข้อ3 กฎหมายนโยบาย * ระดับหน้าที่ทำงาน Crosstabulation

			ระดับหน้าที่ทำงาน			Total
			ระดับข้าราชการชั้นสัญญาบัตร	ระดับข้าราชการชั้นประทวน	ระดับข้าราชการลูกจ้างพนักงานราชการ	
ข้อ3 กฎหมายนโยบาย	ผิด	Count	67	108	42	217
		% within ระดับหน้าที่ทำงาน	54.5%	51.2%	72.4%	55.4%
	ถูก	Count	56	103	16	175
		% within ระดับหน้าที่ทำงาน	45.5%	48.8%	27.6%	44.6%
Total		Count	123	211	58	392
		% within ระดับหน้าที่ทำงาน	100.0%	100.0%	100.0%	100.0%

ตารางที่ 4.13 (ต่อ)

ข้อ4 กฎหมายนโยบาย * ระดับหน้าที่ทำงาน Crosstabulation

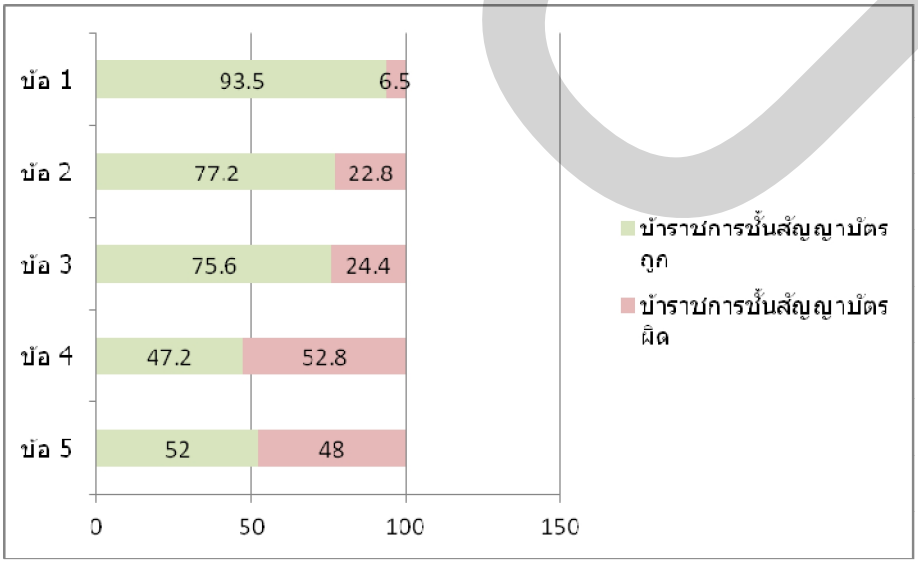
			ระดับหน้าที่ทำงาน			
			ระดับข้าราชการชั้นสัญญาบัตร	ระดับข้าราชการชั้นประทวน	ระดับข้าราชการลูกจ้างพนักงานราชการ	Total
ข้อ4 กฎหมายนโยบาย	ผิด	Count	32	132	15	179
		% within ระดับหน้าที่ทำงาน	26.0%	62.6%	25.9%	45.7%
	ถูก	Count	91	79	43	213
		% within ระดับหน้าที่ทำงาน	74.0%	37.4%	74.1%	54.3%
Total		Count	123	211	58	392
		% within ระดับหน้าที่ทำงาน	100.0%	100.0%	100.0%	100.0%

ข้อ5 กฎหมายนโยบาย * ระดับหน้าที่ทำงาน Crosstabulation

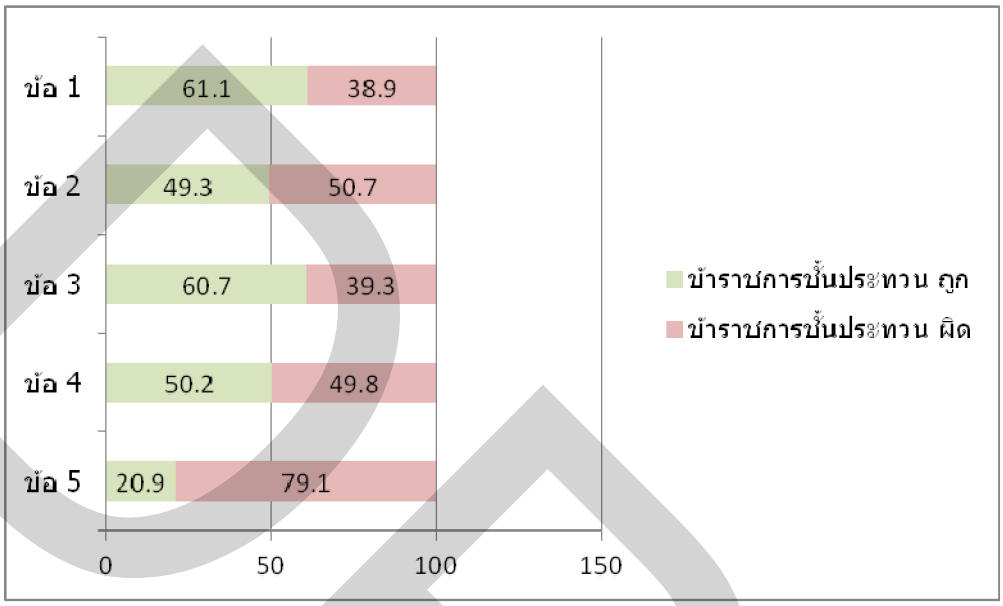
			ระดับหน้าที่ทำงาน			
			ระดับข้าราชการชั้นสัญญาบัตร	ระดับข้าราชการชั้นประทวน	ระดับข้าราชการลูกจ้างพนักงานราชการ	Total
ข้อ5 กฎหมายนโยบาย	ผิด	Count	49	118	20	187
		% within ระดับหน้าที่ทำงาน	39.8%	55.9%	34.5%	47.7%
	ถูก	Count	74	93	38	205
		% within ระดับหน้าที่ทำงาน	60.2%	44.1%	65.5%	52.3%
Total		Count	123	211	58	392
		% within ระดับหน้าที่ทำงาน	100.0%	100.0%	100.0%	100.0%

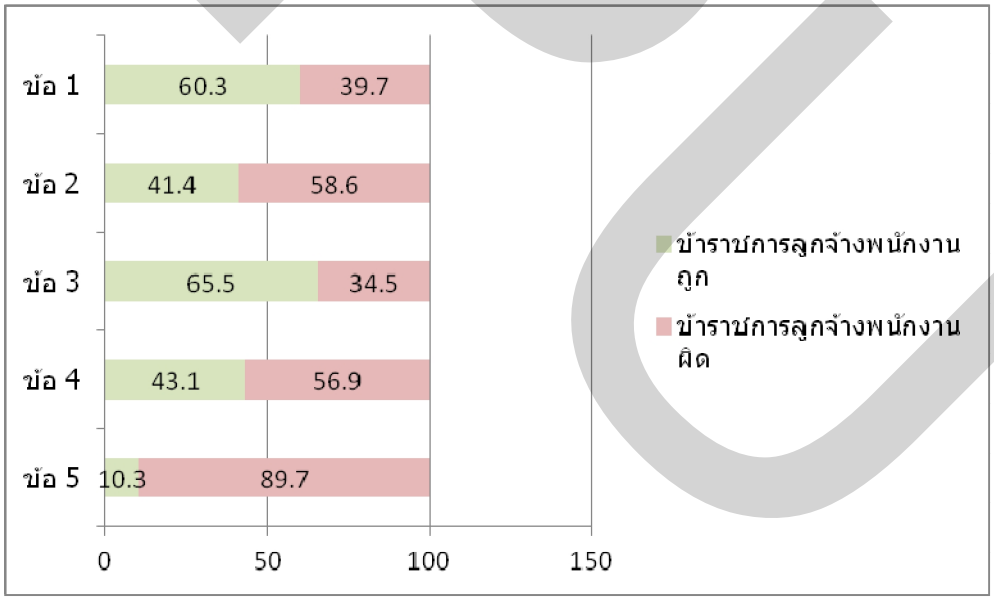
ภาพที่ 4.13 ผลการทดสอบความรู้เปรียบเทียบผลวิเคราะห์ระหว่างทดสอบความรู้ตามตำแหน่งหน้าที่

4.13.1 ด้านข้อมูล



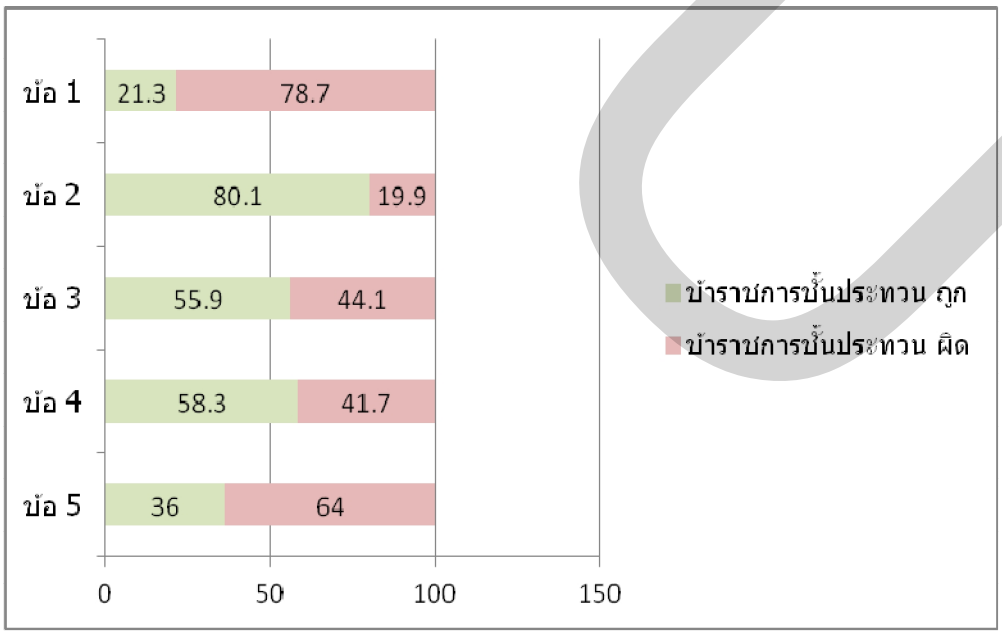
ภาพที่ 4.13 (ต่อ)


ข้อ 1
61.1
38.9
ข้อ 2
49.3
50.7
ข้อ 3
60.7
39.3
ข้อ 4
50.2
49.8
ข้อ 5
20.9
79.1
0
50
100
150
ข้าราชการชั้นประทวน ถูก
ข้าราชการชั้นประทวน ผิด

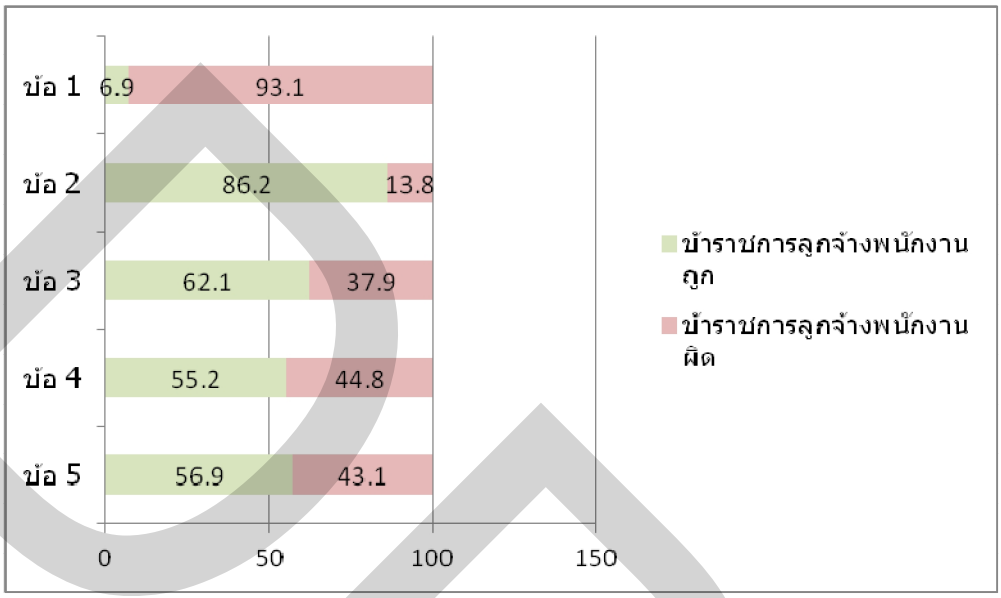

ข้อ 1
60.3
39.7
ข้อ 2
41.4
58.6
ข้อ 3
65.5
34.5
ข้อ 4
43.1
56.9
ข้อ 5
10.3
89.7
0
50
100
150
ข้าราชการลูกจ้างพนักงาน ถูก
ข้าราชการลูกจ้างพนักงาน ผิด

ภาพที่ 4.13 (ต่อ)

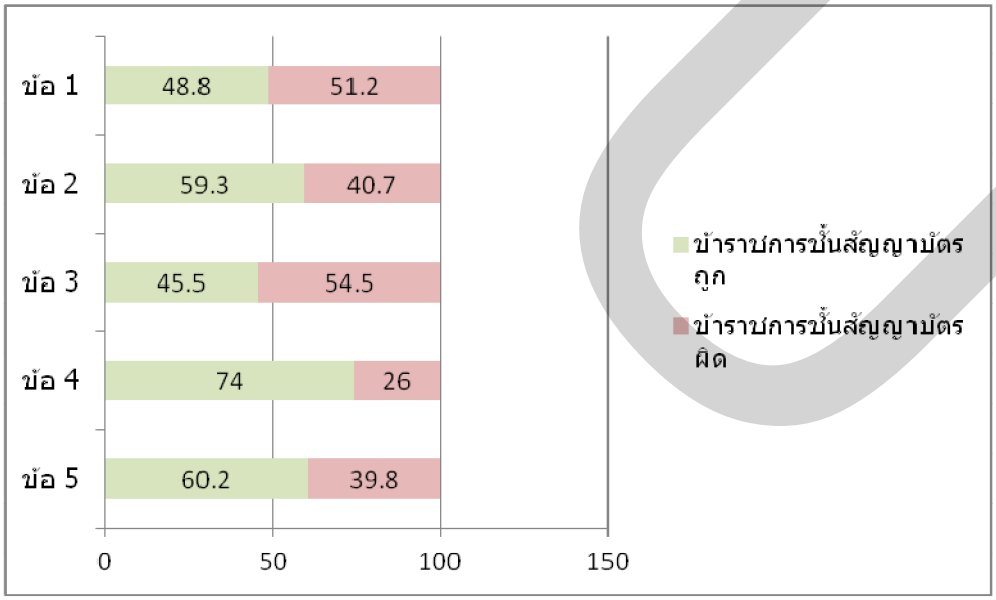
4.13.2 ด้านเกี่ยวกับ ภัยคุกคาม ระบบการป้องกันภัยคุกคาม



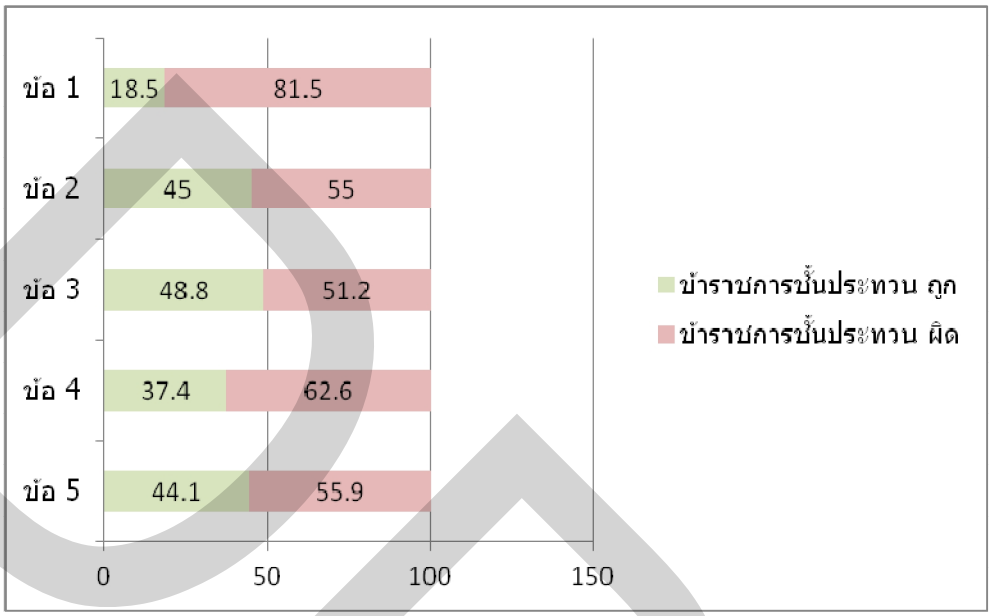
ภาพที่ 4.13 (ต่อ)

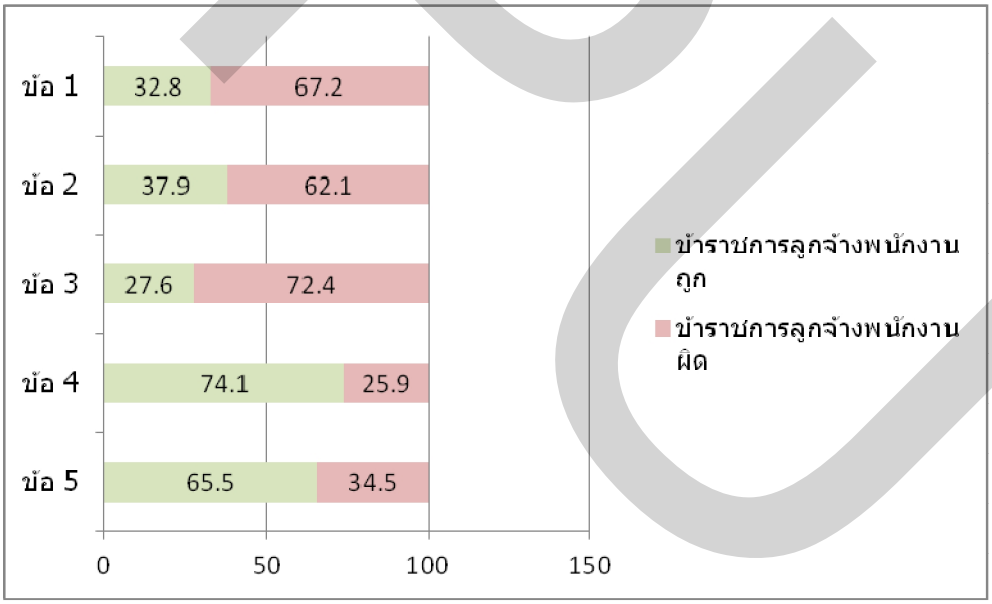


4.13.3 ด้านนโยบาย ข้อกฎหมาย กฎระเบียบข้อบังคับต่าง ๆ



ภาพที่ 4.13 (ต่อ)


ข้อ 1
ข้อ 2
ข้อ 3
ข้อ 4
ข้อ 5
18.5
81.5
45
55
48.8
51.2
37.4
62.6
44.1
55.9
0
50
100
150
ข้าราชการชั้นประทวน ถูก
ข้าราชการชั้นประทวน ผิด


ข้อ 1
ข้อ 2
ข้อ 3
ข้อ 4
ข้อ 5
32.8
67.2
37.9
62.1
27.6
72.4
74.1
25.9
65.5
34.5
0
50
100
150
ข้าราชการลูกจ้างพนักงาน ถูก
ข้าราชการลูกจ้างพนักงาน ผิด

ตารางที่ 4.14 ผลการทดสอบความรู้เปรียบเทียบผลวิเคราะห์ระหว่างทดสอบความรู้ของ ผู้เข้ารับการฝึกอบรมกับผู้ที่ไม่เคยผ่านการฝึกอบรม

4.14.1 ด้านข้อมูล

ข้อ1 ข้อมูล * การฝึกอบรม Crosstabulation

			การฝึกอบรม		
			เคยผ่านหลักสูตร	ไม่เคยผ่านหลักสูตร	Total
ข้อ1 ข้อมูล	ผิด	Count	17	96	113
		% within การฝึกอบรม	10.6%	41.6%	28.8%
	ถูก	Count	144	135	279
		% within การฝึกอบรม	89.4%	58.4%	71.2%
Total		Count	161	231	392
		% within การฝึกอบรม	100.0%	100.0%	100.0%

ข้อ2 ข้อมูล * การฝึกอบรม Crosstabulation

			การฝึกอบรม		
			เคยผ่านหลักสูตร	ไม่เคยผ่านหลักสูตร	Total
ข้อ2 ข้อมูล	ผิด	Count	40	129	169
		% within การฝึกอบรม	24.8%	55.8%	43.1%
	ถูก	Count	121	102	223
		% within การฝึกอบรม	75.2%	44.2%	56.9%
Total		Count	161	231	392
		% within การฝึกอบรม	100.0%	100.0%	100.0%

ข้อ3 ข้อมูล * การฝึกอบรม Crosstabulation

			การฝึกอบรม		
			เคยผ่านหลักสูตร	ไม่เคยผ่านหลักสูตร	Total
ข้อ3 ข้อมูล	ผิด	Count	58	75	133
		% within การฝึกอบรม	36.0%	32.5%	33.9%
	ถูก	Count	103	156	259
		% within การฝึกอบรม	64.0%	67.5%	66.1%
Total		Count	161	231	392
		% within การฝึกอบรม	100.0%	100.0%	100.0%

ตารางที่ 4.14 (ต่อ)

ข้อ4 ข้อมูล * การฝึกอบรม Crosstabulation

			การฝึกอบรม		
			เคยผ่านหลักสูตร	ไม่เคยผ่านหลักสูตร	Total
ข้อ4 ข้อมูล	ผิด	Count	71	132	203
		% within การฝึกอบรม	44.1%	57.1%	51.8%
	ถูก	Count	90	99	189
		% within การฝึกอบรม	55.9%	42.9%	48.2%
Total		Count	161	231	392
		% within การฝึกอบรม	100.0%	100.0%	100.0%

ข้อ5 ข้อมูล * การฝึกอบรม Crosstabulation

			การฝึกอบรม		
			เคยผ่านหลักสูตร	ไม่เคยผ่านหลักสูตร	Total
ข้อ5 ข้อมูล	ผิด	Count	106	172	278
		% within การฝึกอบรม	65.8%	74.5%	70.9%
	ถูก	Count	55	59	114
		% within การฝึกอบรม	34.2%	25.5%	29.1%
Total		Count	161	231	392
		% within การฝึกอบรม	100.0%	100.0%	100.0%

4.14.2 ด้านเกี่ยวกับ ภัยคุกคาม ระบบการป้องกันภัยคุกคาม

ข้อ1 Virus * การฝึกอบรม Crosstabulation

			การฝึกอบรม		
			เคยผ่านหลักสูตร	ไม่เคยผ่านหลักสูตร	Total
ข้อ1 Virus	ผิด	Count	102	186	288
		% within การฝึกอบรม	63.4%	80.5%	73.5%
	ถูก	Count	59	45	104
		% within การฝึกอบรม	36.6%	19.5%	26.5%
Total		Count	161	231	392
		% within การฝึกอบรม	100.0%	100.0%	100.0%

ตารางที่ 4.14 (ต่อ)

ข้อ2 Virus * การฝึกอบรม Crosstabulation

			การฝึกอบรม		
			เคยผ่านหลักสูตร	ไม่เคยผ่านหลักสูตร	Total
ข้อ2 Virus	ผิด	Count	7	48	55
		% within การฝึกอบรม	4.3%	20.8%	14.0%
	ถูก	Count	154	183	337
		% within การฝึกอบรม	95.7%	79.2%	86.0%
Total		Count	161	231	392
		% within การฝึกอบรม	100.0%	100.0%	100.0%

ข้อ3 Virus * การฝึกอบรม Crosstabulation

			การฝึกอบรม		
			เคยผ่านหลักสูตร	ไม่เคยผ่านหลักสูตร	Total
ข้อ3 Virus	ผิด	Count	36	129	165
		% within การฝึกอบรม	22.4%	55.8%	42.1%
	ถูก	Count	125	102	227
		% within การฝึกอบรม	77.6%	44.2%	57.9%
Total		Count	161	231	392
		% within การฝึกอบรม	100.0%	100.0%	100.0%

ข้อ4 Virus * การฝึกอบรม Crosstabulation

			การฝึกอบรม		
			เคยผ่านหลักสูตร	ไม่เคยผ่านหลักสูตร	Total
ข้อ4 Virus	ผิด	Count	35	100	135
		% within การฝึกอบรม	21.7%	43.3%	34.4%
	ถูก	Count	126	131	257
		% within การฝึกอบรม	78.3%	56.7%	65.6%
Total		Count	161	231	392
		% within การฝึกอบรม	100.0%	100.0%	100.0%

ข้อ5 Virus * การฝึกอบรม Crosstabulation

			การฝึกอบรม		
			เคยผ่านหลักสูตร	ไม่เคยผ่านหลักสูตร	Total
ข้อ5 Virus	ผิด	Count	81	132	213
		% within การฝึกอบรม	50.3%	57.1%	54.3%
	ถูก	Count	80	99	179
		% within การฝึกอบรม	49.7%	42.9%	45.7%
Total		Count	161	231	392
		% within การฝึกอบรม	100.0%	100.0%	100.0%

ตารางที่ 4.14 (ต่อ)

4.14.3 ด้านนโยบาย ข้อกฎหมาย กฎระเบียบข้อบังคับต่าง ๆ

ข้อ1 กฎหมายนโยบาย * การฝึกอบรม Crosstabulation

			การฝึกอบรม		
			เคยผ่านหลักสูตร	ไม่เคยผ่านหลักสูตร	Total
ข้อ1 กฎหมายนโยบาย	ผิด	Count	85	189	274
		% within การฝึกอบรม	52.8%	81.8%	69.9%
	ถูก	Count	76	42	118
		% within การฝึกอบรม	47.2%	18.2%	30.1%
Total		Count	161	231	392
		% within การฝึกอบรม	100.0%	100.0%	100.0%

ข้อ2 กฎหมายนโยบาย * การฝึกอบรม Crosstabulation

			การฝึกอบรม		
			เคยผ่านหลักสูตร	ไม่เคยผ่านหลักสูตร	Total
ข้อ2 กฎหมายนโยบาย	ผิด	Count	65	137	202
		% within การฝึกอบรม	40.4%	59.3%	51.5%
	ถูก	Count	96	94	190
		% within การฝึกอบรม	59.6%	40.7%	48.5%
Total		Count	161	231	392
		% within การฝึกอบรม	100.0%	100.0%	100.0%

ข้อ3 กฎหมายนโยบาย * การฝึกอบรม Crosstabulation

			การฝึกอบรม		
			เคยผ่านหลักสูตร	ไม่เคยผ่านหลักสูตร	Total
ข้อ3 กฎหมายนโยบาย	ผิด	Count	89	128	217
		% within การฝึกอบรม	55.3%	55.4%	55.4%
	ถูก	Count	72	103	175
		% within การฝึกอบรม	44.7%	44.6%	44.6%
Total		Count	161	231	392
		% within การฝึกอบรม	100.0%	100.0%	100.0%

ตารางที่ 4.14 (ต่อ)

ข้อ4 กฎหมายนโยบาย * การฝึกอบรม Crosstabulation

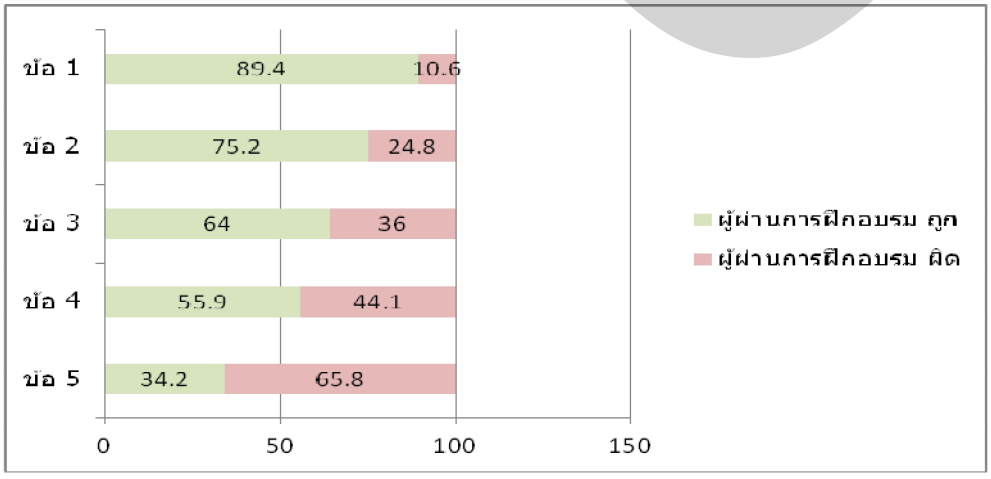
			การฝึกอบรม		
			เคยผ่านหลักสูตร	ไม่เคยผ่านหลักสูตร	Total
ข้อ4 กฎหมายนโยบาย	ผิด	Count	56	123	179
		% within การฝึกอบรม	34.8%	53.2%	45.7%
	ถูก	Count	105	108	213
		% within การฝึกอบรม	65.2%	46.8%	54.3%
Total		Count	161	231	392
		% within การฝึกอบรม	100.0%	100.0%	100.0%

ข้อ5 กฎหมายนโยบาย * การฝึกอบรม Crosstabulation

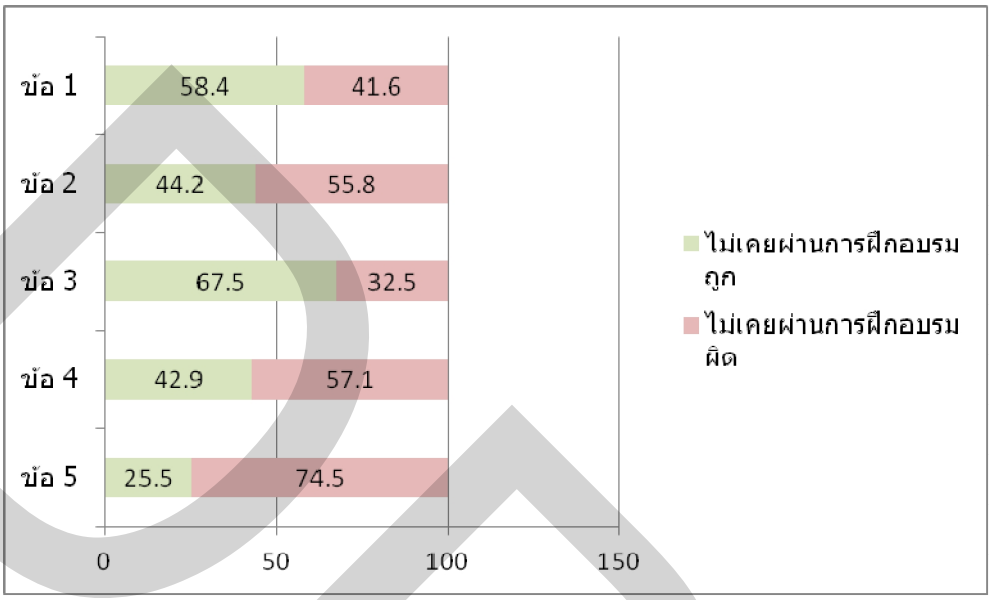
			การฝึกอบรม		
			เคยผ่านหลักสูตร	ไม่เคยผ่านหลักสูตร	Total
ข้อ5 กฎหมายนโยบาย	ผิด	Count	52	135	187
		% within การฝึกอบรม	32.3%	58.4%	47.7%
	ถูก	Count	109	96	205
		% within การฝึกอบรม	67.7%	41.6%	52.3%
Total		Count	161	231	392
		% within การฝึกอบรม	100.0%	100.0%	100.0%

ภาพที่ 4.14 ผลการทดสอบความรู้เปรียบเทียบผลวิเคราะห์ระหว่างทดสอบความรู้ของ ผู้เข้ารับการฝึกอบรมกับผู้ที่ไม่เคยผ่านการฝึกอบรม

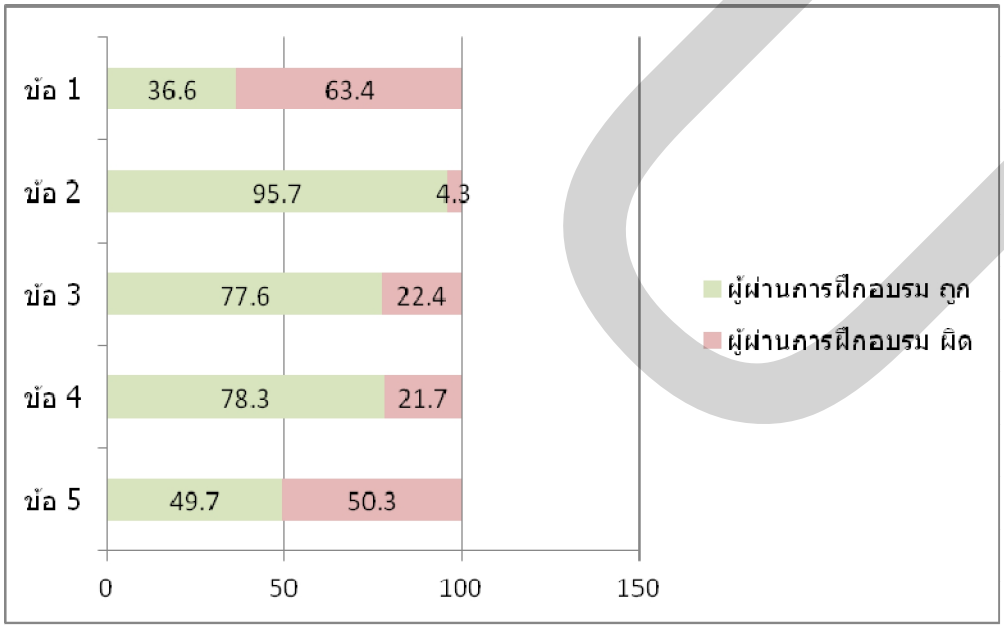
4.14.1 ด้านข้อมูล



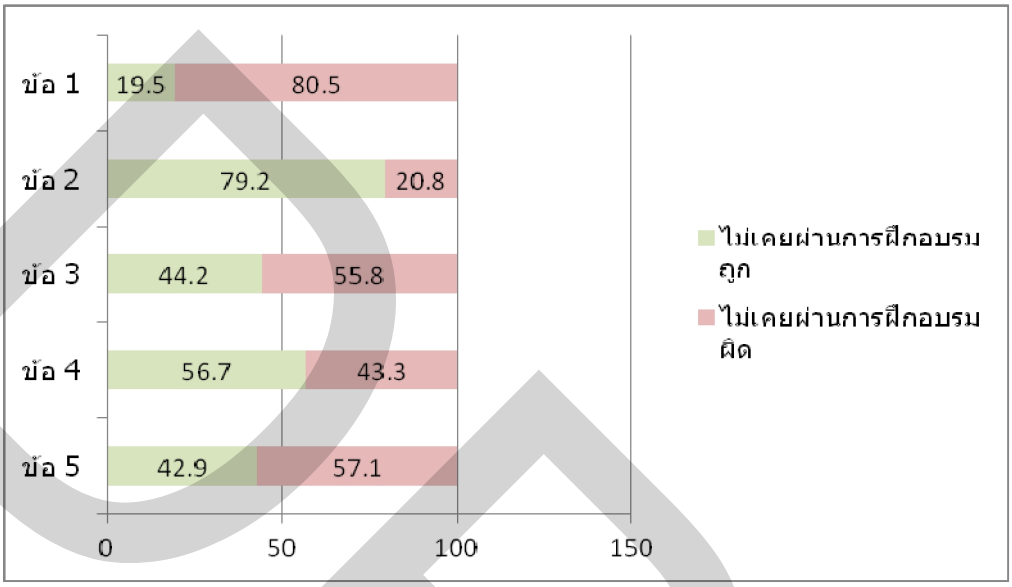
ภาพที่ 4.14 (ต่อ)



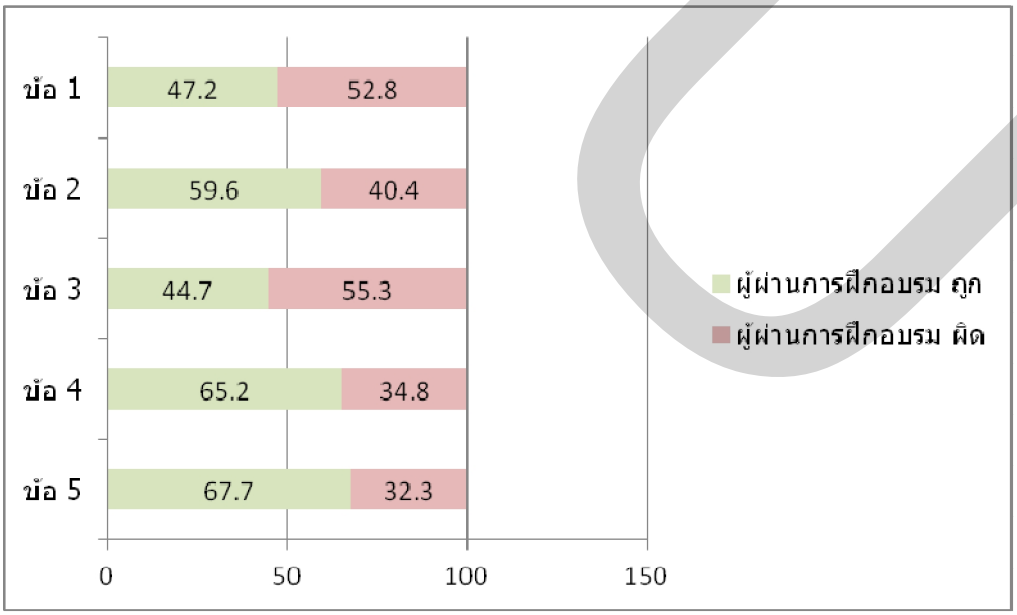
4.14.2 ด้านเกี่ยวกับ ภัยคุกคาม ระบบการป้องกันภัยคุกคาม



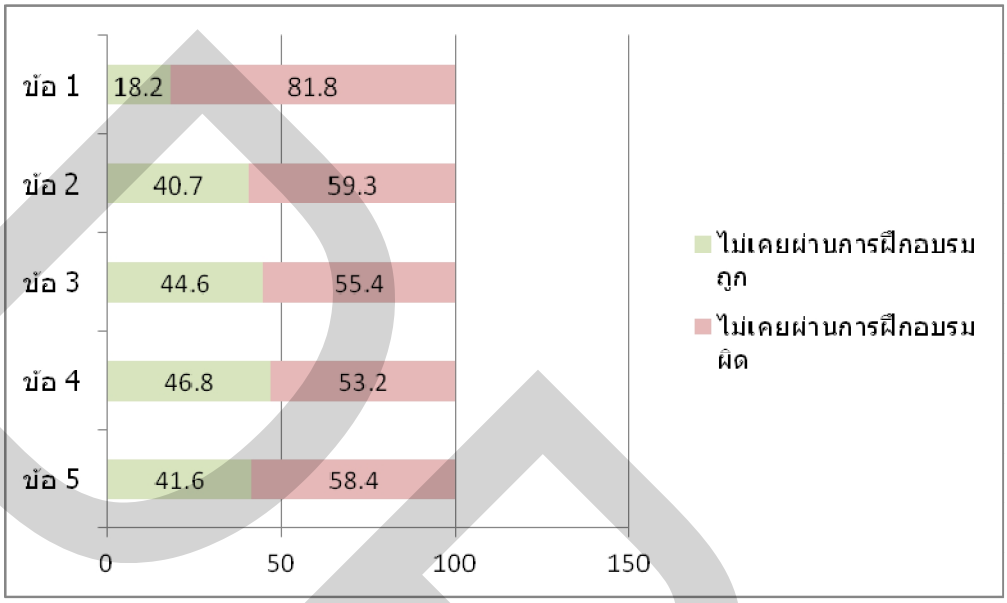
ภาพที่ 4.14 (ต่อ)



4.14.3 ด้านนโยบาย ข้อกฎหมาย กฎระเบียบข้อบังคับต่าง ๆ



ภาพที่ 4.14 (ต่อ)



ตอนที่ 4 แสดงข้อมูลของการทดสอบพฤติกรรมความเสี่ยงต่อการรักษาความมั่นคงปลอดภัยสารสนเทศ ของข้าราชการกองบัญชาการกองทัพไทย ว่าโดยภาพรวมโดยเฉลี่ยแล้ว ข้าราชการ กองบัญชาการกองทัพไทย มีความรู้ความเข้าใจแล้ว จากผลของแบบทดสอบ ความรู้ในตอนที่ 3 ที่ผ่านมา แล้วยังมีพฤติกรรมต่อความเสี่ยงด้านภัยคุกคามต่าง ๆ ในแต่ละด้านเพียงใด ในเรื่อง ต่าง ๆ ที่จำแนกแบ่งออกเป็น 3 กลุ่มใหญ่ มีจำนวนทั้งสิ้น 10 ข้อ

1) พฤติกรรมความเสี่ยงด้านที่เกี่ยวกับข้อมูลการรักษาข้อมูล จำนวน 5 ข้อ จากจำนวน 5 ข้อนี้ ถ้าผลการทดสอบออกมา เป็น 3 ข้อ ขึ้นไป ให้ถือว่า โดยเฉลี่ยแล้ว มีพฤติกรรมความเสี่ยงในด้านนี้

2) พฤติกรรมความเสี่ยงด้านที่เกี่ยวกับ ภัยคุกคาม ระบบการป้องกันภัยคุกคาม จำนวน 4 ข้อ จากจำนวน 4 ข้อนี้ ถ้าผลการทดสอบออกมา เป็น 3 ข้อขึ้นไป ให้ถือว่า โดยเฉลี่ยแล้ว มีพฤติกรรมความเสี่ยงในด้านนี้

3) พฤติกรรมความเสี่ยงด้านที่เกี่ยวกับ นโยบาย ข้อกฎหมาย กฎระเบียบข้อบังคับต่าง ๆ จำนวน 1 ข้อ จากจำนวน 1 ข้อนี้ ถ้า ผลการทดสอบออกมา ระดับร้อยละของ ความเสี่ยง มีมากเกินร้อยละ 50 ขึ้นไป ให้ถือว่า โดยเฉลี่ยแล้ว มีพฤติกรรมความเสี่ยงในด้านนี้

ตารางที่ 4.15 ผลการทดสอบพฤติกรรมความเสี่ยงในด้านที่เกี่ยวกับข้อมูลการรักษาข้อมูล

ข้อ1 ข้อมูล

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ไม่เสี่ยง	156	39.8	39.8	39.8
	เสี่ยง	236	60.2	60.2	100.0
	Total	392	100.0	100.0	

ข้อ2 ข้อมูล

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ไม่เสี่ยง	121	30.9	30.9	30.9
	เสี่ยง	271	69.1	69.1	100.0
	Total	392	100.0	100.0	

ข้อ3 ข้อมูล

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ไม่เสี่ยง	128	32.7	32.7	32.7
	เสี่ยง	264	67.3	67.3	100.0
	Total	392	100.0	100.0	

ข้อ4 ข้อมูล

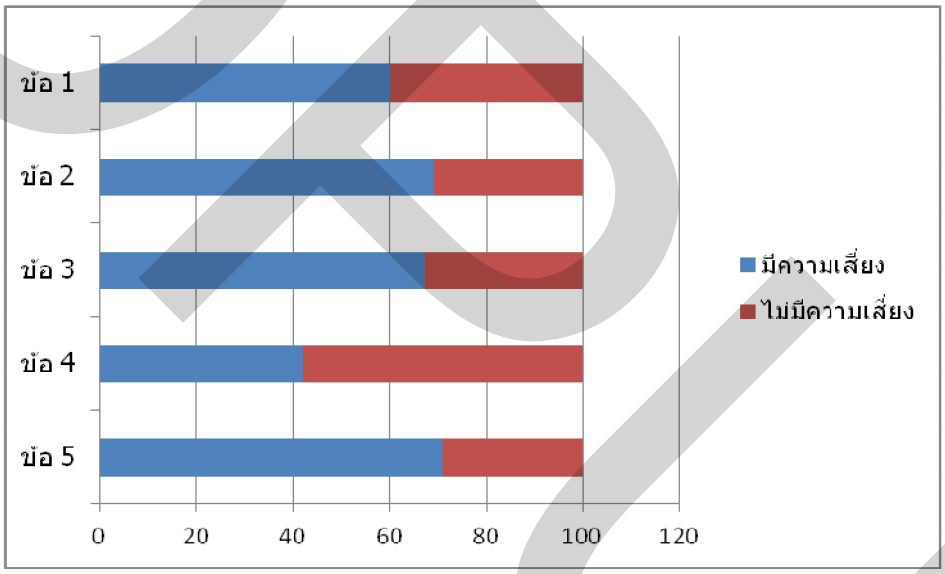
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ไม่เสี่ยง	226	57.7	57.7	57.7
	เสี่ยง	166	42.3	42.3	100.0
	Total	392	100.0	100.0	

ข้อ5 ข้อมูล

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ไม่เสี่ยง	114	29.1	29.1	29.1
	เสี่ยง	278	70.9	70.9	100.0
	Total	392	100.0	100.0	

ผลจากตารางที่ 4.15 แสดงให้เห็นว่าจำนวนกลุ่มตัวอย่างของข้าราชการกองบัญชาการกองทัพไทย ทั้งสิ้น 392 คน จากผลการทดสอบพฤติกรรมความเสี่ยงในด้านที่เกี่ยวกับข้อมูลการรักษาข้อมูล ที่เกินจำนวน ร้อยละ 50.0 ขึ้นไป ในแต่ละข้อ มีจำนวนทั้งสิ้น 4 ข้อ จากรายงานผลในแต่ละข้อดังนี้ ข้อ 1 เสี่ยง ร้อยละ 60.2 ข้อ 2 เสี่ยง ร้อยละ 69.1 ข้อ 3 เสี่ยง ร้อยละ 67.3 ข้อ 4 เสี่ยง ร้อยละ 42.3 ข้อ 5 เสี่ยง ร้อยละ 70.9 แสดงว่าข้าราชการกองบัญชาการกองทัพไทย จากกลุ่มตัวอย่างที่นำมาทดสอบพฤติกรรมความเสี่ยงด้านที่เกี่ยวข้องกับข้อมูลการรักษาข้อมูล อยู่ในเกณฑ์ที่เสี่ยงในด้านนี้

ภาพที่ 4.15 ผลการทดสอบพฤติกรรมความเสี่ยงในด้านที่เกี่ยวกับข้อมูลการรักษาข้อมูล



ตารางที่ 4.16 ผลการทดสอบพฤติกรรมความเสี่ยงในด้านที่เกี่ยวกับ ภัยคุกคาม ระบบการป้องกันภัยคุกคาม

ข้อ1 Virus

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ไม่เสี่ยง	60	15.3	15.3	15.3
	เสี่ยง	332	84.7	84.7	100.0
	Total	392	100.0	100.0	

ตารางที่ 4.16 (ต่อ)

ข้อ2 Virus

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ไม่เสี่ยง	133	33.9	33.9	33.9
	เสี่ยง	259	66.1	66.1	100.0
	Total	392	100.0	100.0	

ข้อ3 Virus

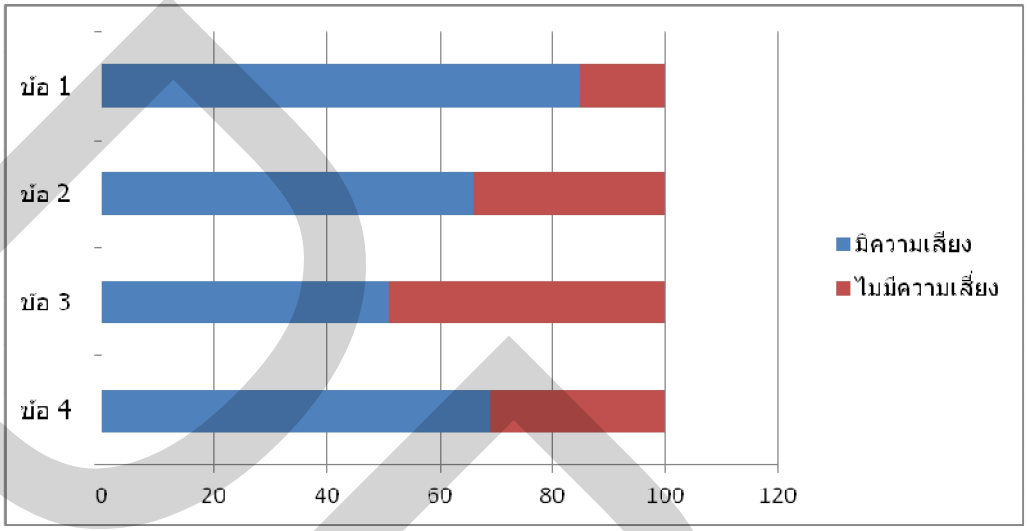
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ไม่เสี่ยง	192	49.0	49.0	49.0
	เสี่ยง	200	51.0	51.0	100.0
	Total	392	100.0	100.0	

ข้อ4 Virus

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ไม่เสี่ยง	122	31.1	31.1	31.1
	เสี่ยง	270	68.9	68.9	100.0
	Total	392	100.0	100.0	

ผลจากตารางที่ 4.16 แสดงให้เห็นว่าจำนวนกลุ่มตัวอย่างของข้าราชการกองบัญชาการกองทัพไทย ทั้งสิ้น 392 คน จากผลการทดสอบพฤติกรรมความเสี่ยงในด้านที่เกี่ยวกับ ภัยคุกคามระบบการป้องกันภัยคุกคาม ที่เกินจำนวน ร้อยละ 50.0 ขึ้นไป ในแต่ละข้อ มีจำนวนทั้งสิ้น 4 ข้อ จากรายงานผลในแต่ละข้อดังนี้ ข้อ 1 เสี่ยง ร้อยละ 84.7 ข้อ 2 เสี่ยง ร้อยละ 66.1 ข้อ 3 เสี่ยง ร้อยละ 51.0 ข้อ 4 เสี่ยง ร้อยละ 68.9 แสดงว่าข้าราชการกองบัญชาการกองทัพไทย จากกลุ่มตัวอย่างที่นำมาทดสอบพฤติกรรมความเสี่ยงในด้านที่เกี่ยวกับ ภัยคุกคาม ระบบการป้องกันภัยคุกคาม อยู่ในเกณฑ์ที่เสี่ยงในด้านนี้

ภาพที่ 4.16 ผลการทดสอบพฤติกรรมความเสี่ยงในด้านที่เกี่ยวกับ ภัยคุกคาม ระบบการป้องกันภัยคุกคาม



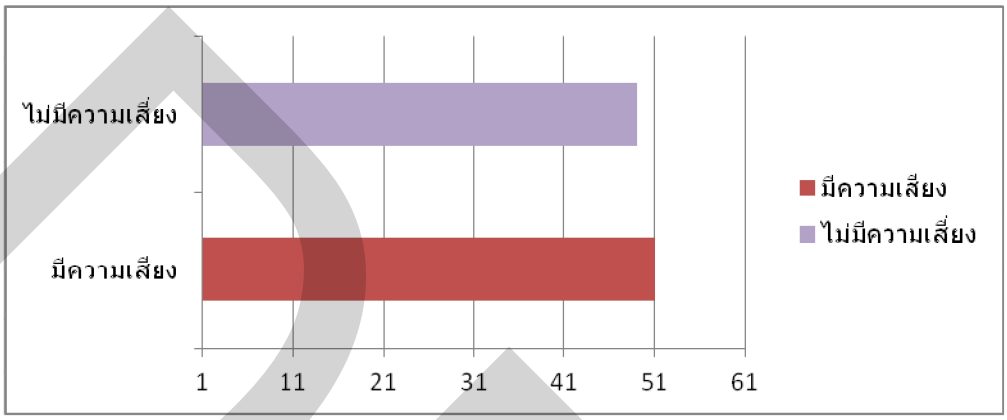
ตารางที่ 4.17 ผลการทดสอบพฤติกรรมความเสี่ยงด้านที่เกี่ยวกับ นโยบาย ข้อกฎหมาย กฎระเบียบข้อบังคับต่าง ๆ

ข้อกฎหมายนโยบาย

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ไม่เสี่ยง	192	49.0	49.0	49.0
	เสี่ยง	200	51.0	51.0	100.0
	Total	392	100.0	100.0	

ผลจากตารางที่ 4.17 แสดงให้เห็นว่าจำนวนกลุ่มตัวอย่างของข้าราชการกองบัญชาการกองทัพไทยทั้งสิ้น 392 คน จากผลการทดสอบพฤติกรรมความเสี่ยงในด้านที่เกี่ยวกับ นโยบาย ข้อกฎหมาย กฎระเบียบข้อบังคับต่าง ๆ มีความเสี่ยง ร้อยละ 51.0 แสดงว่าข้าราชการกองบัญชาการกองทัพไทย จากกลุ่มตัวอย่างที่นำมาทดสอบพฤติกรรมความเสี่ยงในด้านที่เกี่ยวกับ ภัยคุกคาม ระบบการป้องกันภัยคุกคาม อยู่ในเกณฑ์ที่เสี่ยงในด้านนี้

ภาพที่ 4.17 ผลการทดสอบพฤติกรรมความเสี่ยงด้านที่เกี่ยวกับ นโยบาย ข้อกฎหมาย กฎระเบียบ ข้อบังคับต่าง ๆ



ตารางที่ 4.18 ผลการทดสอบพฤติกรรมความเสี่ยงเปรียบเทียบผลวิเคราะห์ระหว่างพฤติกรรมความเสี่ยงตามตำแหน่งหน้าที่

4.18.1 ด้านข้อมูล

ข้อ1 ข้อมูล * ระดับหน้าที่ทำงาน Crosstabulation

			ระดับหน้าที่ทำงาน			
			ระดับข้าราชการชั้นสัญญาบัตร	ระดับข้าราชการชั้นประทวน	ระดับข้าราชการลูกจ้างพนักงานราชการ	Total
ข้อ1 ข้อมูล	ไม่เสี่ยง	Count	59	80	17	156
		% within ระดับหน้าที่ทำงาน	48.0%	37.9%	29.3%	39.8%
	เสี่ยง	Count	64	131	41	236
		% within ระดับหน้าที่ทำงาน	52.0%	62.1%	70.7%	60.2%
Total		Count	123	211	58	392
		% within ระดับหน้าที่ทำงาน	100.0%	100.0%	100.0%	100.0%

ข้อ2 ข้อมูล * ระดับหน้าที่ทำงาน Crosstabulation

			ระดับหน้าที่ทำงาน			
			ระดับข้าราชการชั้นสัญญาบัตร	ระดับข้าราชการชั้นประทวน	ระดับข้าราชการลูกจ้างพนักงานราชการ	Total
ข้อ2 ข้อมูล	ไม่เสี่ยง	Count	40	74	7	121
		% within ระดับหน้าที่ทำงาน	32.5%	35.1%	12.1%	30.9%
	เสี่ยง	Count	83	137	51	271
		% within ระดับหน้าที่ทำงาน	67.5%	64.9%	87.9%	69.1%
Total		Count	123	211	58	392
		% within ระดับหน้าที่ทำงาน	100.0%	100.0%	100.0%	100.0%

ตารางที่ 4.18 (ต่อ)

ข้อ3 ข้อมูล * ระดับหน้าที่ทำงาน Crosstabulation

			ระดับหน้าที่ทำงาน			
			ระดับข้าราชการชั้นสัญญาบัตร	ระดับข้าราชการชั้นประทวน	ระดับข้าราชการลูกจ้างพนักงานราชการ	Total
ข้อ3 ข้อมูล	ไม่เสี่ยง	Count	20	97	11	128
		% within ระดับหน้าที่ทำงาน	16.3%	46.0%	19.0%	32.7%
	เสี่ยง	Count	103	114	47	264
		% within ระดับหน้าที่ทำงาน	83.7%	54.0%	81.0%	67.3%
Total		Count	123	211	58	392
		% within ระดับหน้าที่ทำงาน	100.0%	100.0%	100.0%	100.0%

ข้อ4 ข้อมูล * ระดับหน้าที่ทำงาน Crosstabulation

			ระดับหน้าที่ทำงาน			
			ระดับข้าราชการชั้นสัญญาบัตร	ระดับข้าราชการชั้นประทวน	ระดับข้าราชการลูกจ้างพนักงานราชการ	Total
ข้อ4 ข้อมูล	ไม่เสี่ยง	Count	78	121	27	226
		% within ระดับหน้าที่ทำงาน	63.4%	57.3%	46.6%	57.7%
	เสี่ยง	Count	45	90	31	166
		% within ระดับหน้าที่ทำงาน	36.6%	42.7%	53.4%	42.3%
Total		Count	123	211	58	392
		% within ระดับหน้าที่ทำงาน	100.0%	100.0%	100.0%	100.0%

ข้อ5 ข้อมูล * ระดับหน้าที่ทำงาน Crosstabulation

			ระดับหน้าที่ทำงาน			
			ระดับข้าราชการชั้นสัญญาบัตร	ระดับข้าราชการชั้นประทวน	ระดับข้าราชการลูกจ้างพนักงานราชการ	Total
ข้อ5 ข้อมูล	ไม่เสี่ยง	Count	41	59	14	114
		% within ระดับหน้าที่ทำงาน	33.3%	28.0%	24.1%	29.1%
	เสี่ยง	Count	82	152	44	278
		% within ระดับหน้าที่ทำงาน	66.7%	72.0%	75.9%	70.9%
Total		Count	123	211	58	392
		% within ระดับหน้าที่ทำงาน	100.0%	100.0%	100.0%	100.0%

ตารางที่ 4.18 (ต่อ)

4.18.2 ด้านเกี่ยวกับ ภัยคุกคาม ระบบการป้องกันภัยคุกคาม

ข้อ1 Virus * ระดับหน้าที่ทำงาน Crosstabulation

			ระดับหน้าที่ทำงาน			Total
			ระดับข้าราชการชั้นสัญญาบัตร	ระดับข้าราชการชั้นประทวน	ระดับข้าราชการลูกจ้างพนักงานราชการ	
ข้อ1 Virus	ไม่เสี่ยง	Count	15	37	8	60
		% within ระดับหน้าที่ทำงาน	12.2%	17.5%	13.8%	15.3%
	เสี่ยง	Count	108	174	50	332
		% within ระดับหน้าที่ทำงาน	87.8%	82.5%	86.2%	84.7%
Total		Count	123	211	58	392
		% within ระดับหน้าที่ทำงาน	100.0%	100.0%	100.0%	100.0%

ข้อ2 Virus * ระดับหน้าที่ทำงาน Crosstabulation

			ระดับหน้าที่ทำงาน			Total
			ระดับข้าราชการชั้นสัญญาบัตร	ระดับข้าราชการชั้นประทวน	ระดับข้าราชการลูกจ้างพนักงานราชการ	
ข้อ2 Virus	ไม่เสี่ยง	Count	32	89	12	133
		% within ระดับหน้าที่ทำงาน	26.0%	42.2%	20.7%	33.9%
	เสี่ยง	Count	91	122	46	259
		% within ระดับหน้าที่ทำงาน	74.0%	57.8%	79.3%	66.1%
Total		Count	123	211	58	392
		% within ระดับหน้าที่ทำงาน	100.0%	100.0%	100.0%	100.0%

ข้อ3 Virus * ระดับหน้าที่ทำงาน Crosstabulation

			ระดับหน้าที่ทำงาน			Total
			ระดับข้าราชการชั้นสัญญาบัตร	ระดับข้าราชการชั้นประทวน	ระดับข้าราชการลูกจ้างพนักงานราชการ	
ข้อ3 Virus	ไม่เสี่ยง	Count	69	101	22	192
		% within ระดับหน้าที่ทำงาน	56.1%	47.9%	37.9%	49.0%
	เสี่ยง	Count	54	110	36	200
		% within ระดับหน้าที่ทำงาน	43.9%	52.1%	62.1%	51.0%
Total		Count	123	211	58	392
		% within ระดับหน้าที่ทำงาน	100.0%	100.0%	100.0%	100.0%

ตารางที่ 4.18 (ต่อ)

ข้อ4 Virus * ระดับหน้าที่ทำงาน Crosstabulation

			ระดับหน้าที่ทำงาน			Total
			ระดับข้าราชการชั้นสัญญาบัตร	ระดับข้าราชการชั้นประทวน	ระดับข้าราชการลูกจ้างพนักงานราชการ	
ข้อ4 Virus	ไม่เสี่ยง	Count	41	74	7	122
		% within ระดับหน้าที่ทำงาน	33.3%	35.1%	12.1%	31.1%
	เสี่ยง	Count	82	137	51	270
		% within ระดับหน้าที่ทำงาน	66.7%	64.9%	87.9%	68.9%
Total		Count	123	211	58	392
		% within ระดับหน้าที่ทำงาน	100.0%	100.0%	100.0%	100.0%

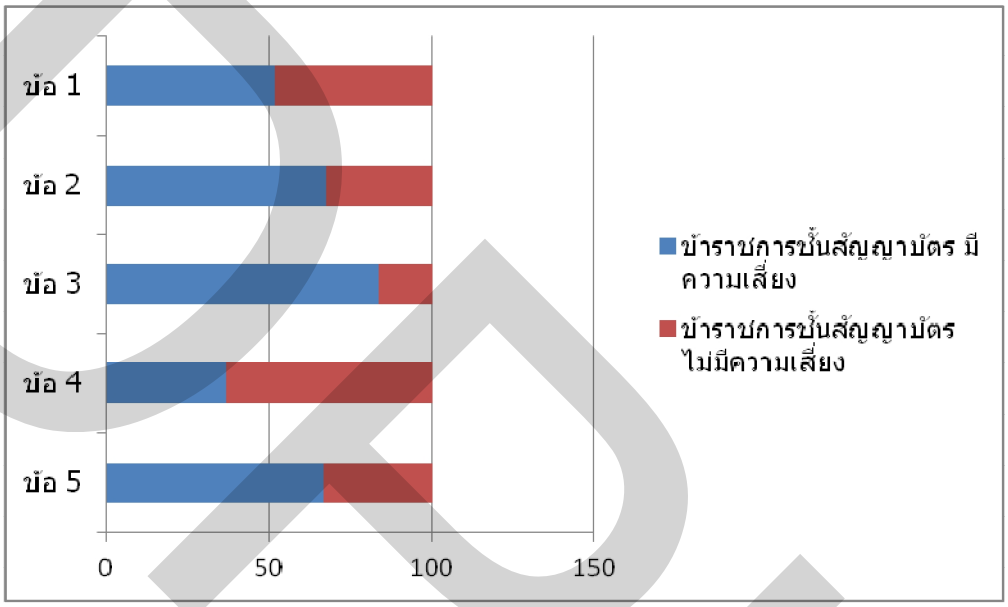
4.18.3 ด้านนโยบาย ข้อกฎหมาย กฎระเบียบข้อบังคับต่าง ๆ

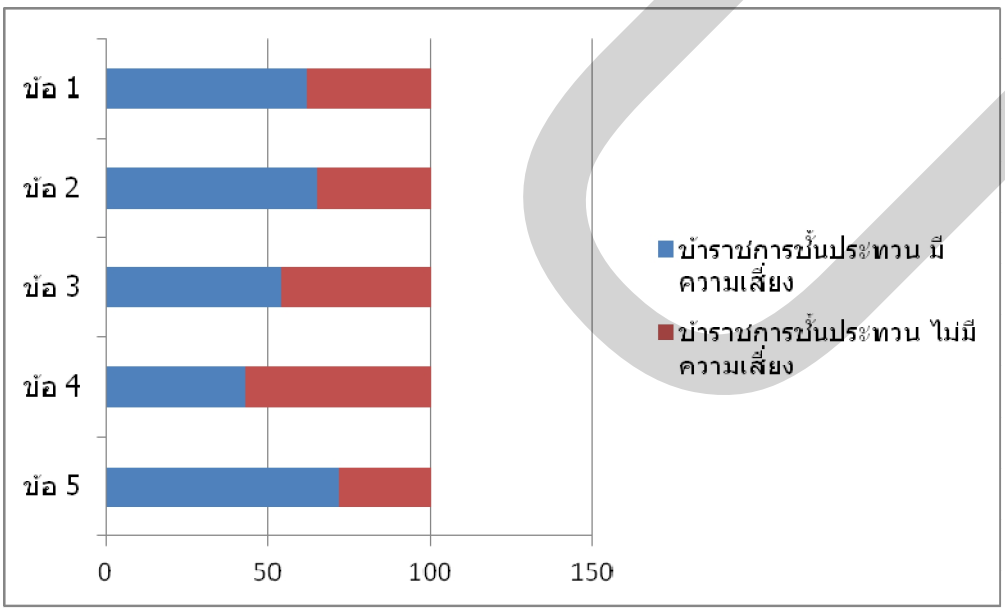
ข้อกฎหมายนโยบาย * ระดับหน้าที่ทำงาน Crosstabulation

			ระดับหน้าที่ทำงาน			Total
			ระดับข้าราชการชั้นสัญญาบัตร	ระดับข้าราชการชั้นประทวน	ระดับข้าราชการลูกจ้างพนักงานราชการ	
ข้อกฎหมายนโยบาย	ไม่เสี่ยง	Count	56	116	20	192
		% within ระดับหน้าที่ทำงาน	45.5%	55.0%	34.5%	49.0%
	เสี่ยง	Count	67	95	38	200
		% within ระดับหน้าที่ทำงาน	54.5%	45.0%	65.5%	51.0%
Total		Count	123	211	58	392
		% within ระดับหน้าที่ทำงาน	100.0%	100.0%	100.0%	100.0%

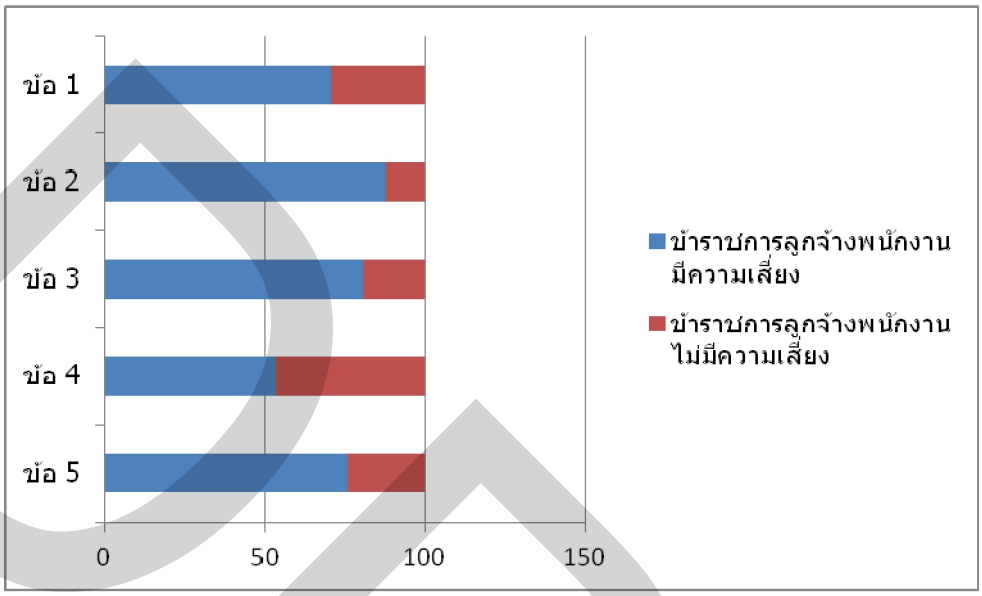
ภาพที่ 4.18 ผลการทดสอบพฤติกรรมความเสี่ยงเปรียบเทียบผลวิเคราะห์ระหว่างพฤติกรรมความเสี่ยงตามตำแหน่งหน้าที่

4.18.1 ด้านข้อมูล

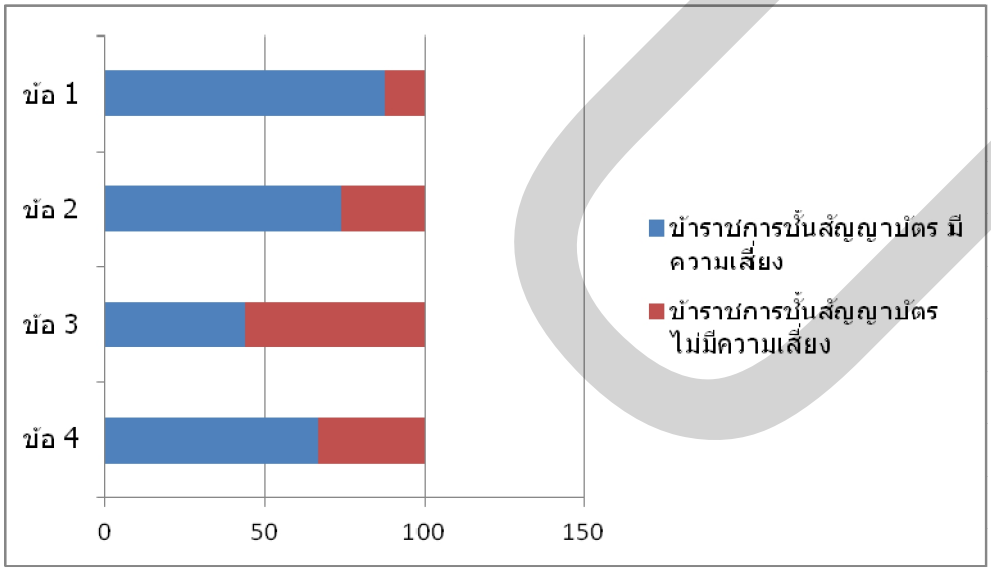




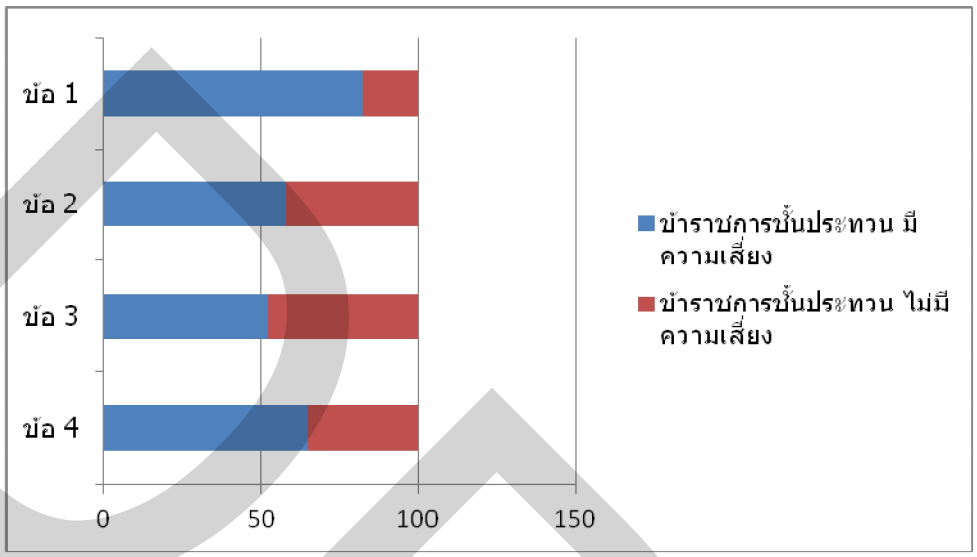
ภาพที่ 4.18 (ต่อ)

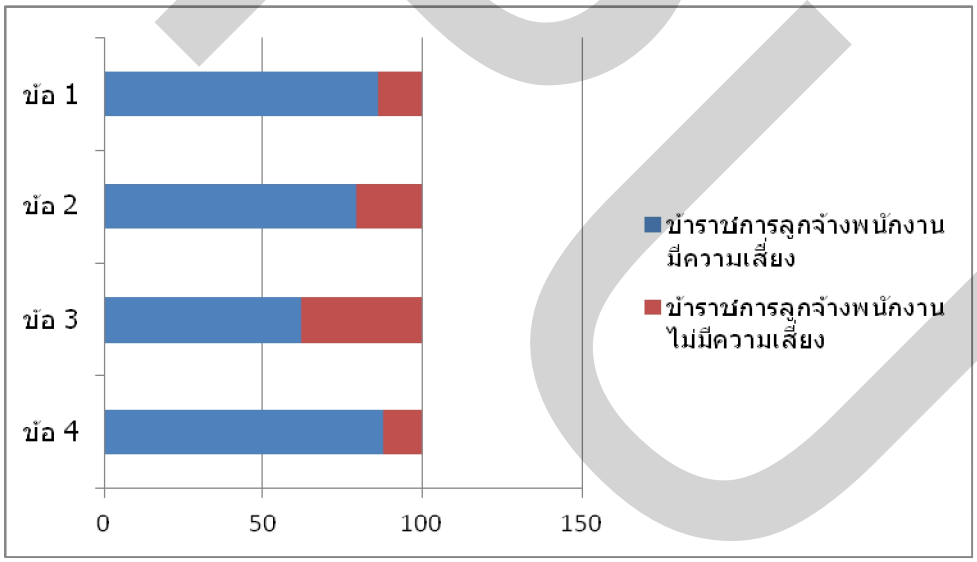


4.18.2 ด้านเกี่ยวกับ ภัยคุกคาม ระบบการป้องกันภัยคุกคาม



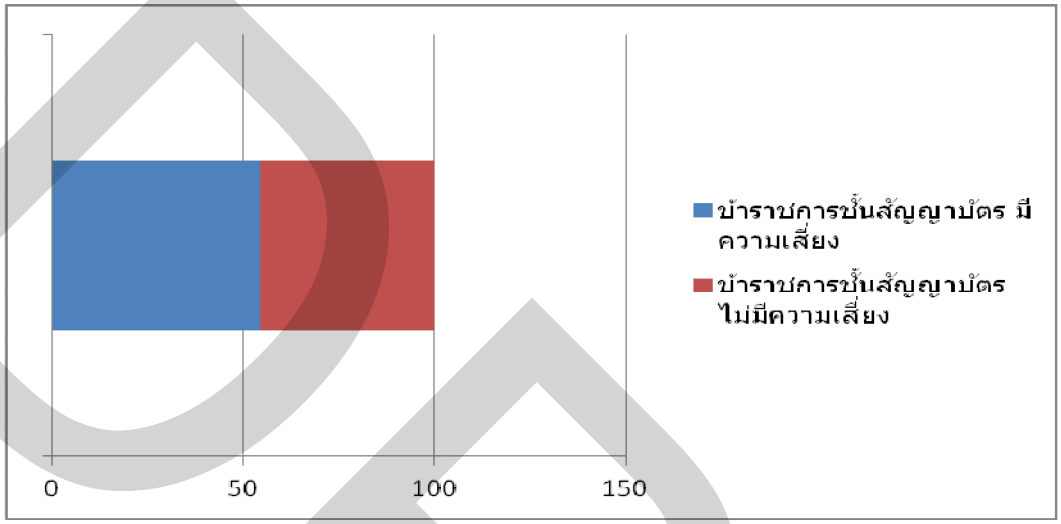
ภาพที่ 4.18 (ต่อ)

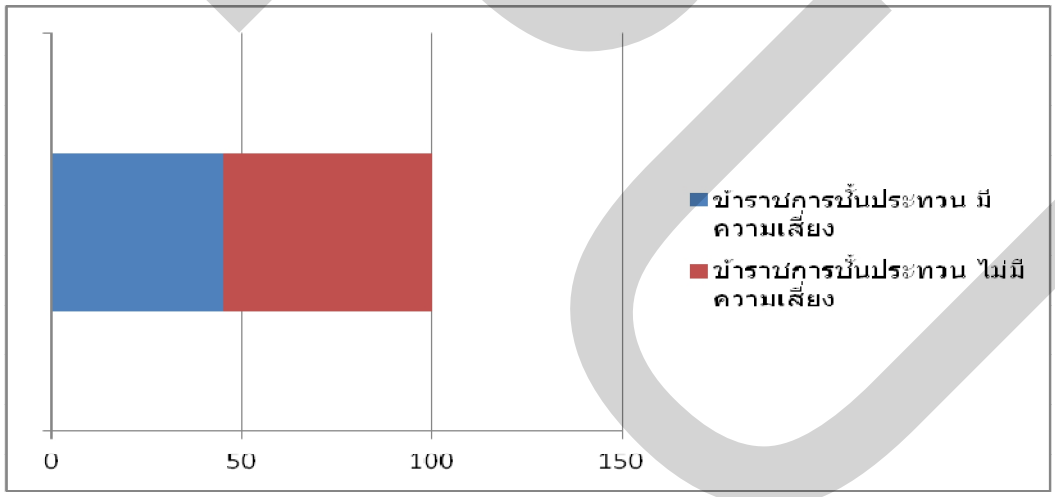

ข้อ 1
ข้อ 2
ข้อ 3
ข้อ 4
0
50
100
150
ข้าราชการชั้นประทวน มีความเสี่ยง
ข้าราชการชั้นประทวน ไม่มีความเสี่ยง


ข้อ 1
ข้อ 2
ข้อ 3
ข้อ 4
0
50
100
150
ข้าราชการลูกจ้างพนักงาน มีความเสี่ยง
ข้าราชการลูกจ้างพนักงาน ไม่มีความเสี่ยง

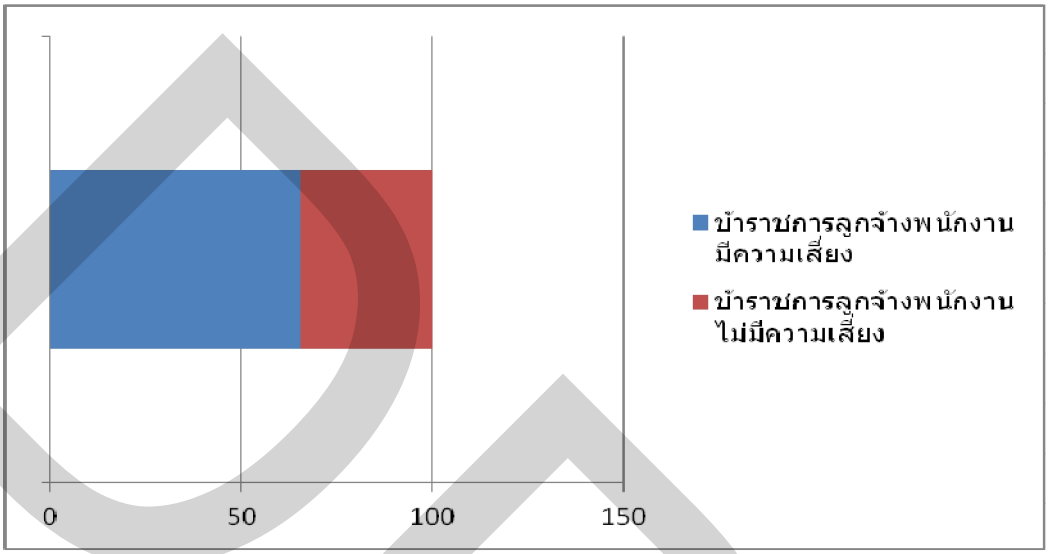
ภาพที่ 4.18 (ต่อ)

4.18.3 ด้านนโยบาย ข้อกฎหมาย กฎระเบียบข้อบังคับต่าง ๆ





ภาพที่ 4.18 (ต่อ)



ตารางที่ 4.19 ผลการทดสอบพฤติกรรมความเสี่ยงเทียบผลวิเคราะห์ระหว่างทดสอบพฤติกรรมความเสี่ยงของ ผู้เข้ารับการฝึกอบรมกับผู้ที่ไม่เคยผ่านการฝึกอบรม

4.19.1 ด้านข้อมูล

ข้อ1 ข้อมูล * การฝึกอบรม Crosstabulation

			การฝึกอบรม		
			เคยผ่านหลักสูตร	ไม่เคยผ่านหลักสูตร	Total
ข้อ1 ข้อมูล	ไม่เสี่ยง	Count	66	90	156
		% within การฝึกอบรม	41.0%	39.0%	39.8%
	เสี่ยง	Count	95	141	236
		% within การฝึกอบรม	59.0%	61.0%	60.2%
Total		Count	161	231	392
		% within การฝึกอบรม	100.0%	100.0%	100.0%

ตารางที่ 4.19 (ต่อ)

ข้อ2 ข้อมูล * การฝึกอบรม Crosstabulation

			การฝึกอบรม		
			เคยผ่านหลักสูตร	ไม่เคยผ่านหลักสูตร	Total
ข้อ2 ข้อมูล	ไม่เสี่ยง	Count	59	62	121
		% within การฝึกอบรม	36.6%	26.8%	30.9%
	เสี่ยง	Count	102	169	271
		% within การฝึกอบรม	63.4%	73.2%	69.1%
Total		Count	161	231	392
		% within การฝึกอบรม	100.0%	100.0%	100.0%

ข้อ3 ข้อมูล * การฝึกอบรม Crosstabulation

			การฝึกอบรม		
			เคยผ่านหลักสูตร	ไม่เคยผ่านหลักสูตร	Total
ข้อ3 ข้อมูล	ไม่เสี่ยง	Count	42	86	128
		% within การฝึกอบรม	26.1%	37.2%	32.7%
	เสี่ยง	Count	119	145	264
		% within การฝึกอบรม	73.9%	62.8%	67.3%
Total		Count	161	231	392
		% within การฝึกอบรม	100.0%	100.0%	100.0%

ข้อ4 ข้อมูล * การฝึกอบรม Crosstabulation

			การฝึกอบรม		
			เคยผ่านหลักสูตร	ไม่เคยผ่านหลักสูตร	Total
ข้อ4 ข้อมูล	ไม่เสี่ยง	Count	95	131	226
		% within การฝึกอบรม	59.0%	56.7%	57.7%
	เสี่ยง	Count	66	100	166
		% within การฝึกอบรม	41.0%	43.3%	42.3%
Total		Count	161	231	392
		% within การฝึกอบรม	100.0%	100.0%	100.0%

ข้อ5 ข้อมูล * การฝึกอบรม Crosstabulation

			การฝึกอบรม		
			เคยผ่านหลักสูตร	ไม่เคยผ่านหลักสูตร	Total
ข้อ5 ข้อมูล	ไม่เสี่ยง	Count	51	63	114
		% within การฝึกอบรม	31.7%	27.3%	29.1%
	เสี่ยง	Count	110	168	278
		% within การฝึกอบรม	68.3%	72.7%	70.9%
Total		Count	161	231	392
		% within การฝึกอบรม	100.0%	100.0%	100.0%

ตารางที่ 4.19 (ต่อ)

4.19.2 ด้านเกี่ยวกับ ภัยคุกคาม ระบบการป้องกันภัยคุกคาม

ข้อ1 Virus * การฝึกอบรม Crosstabulation

			การฝึกอบรม		Total
			เคยผ่านหลักสูตร	ไม่เคยผ่านหลักสูตร	
ข้อ1 Virus	ไม่เสี่ยง	Count	10	50	60
		% within การฝึกอบรม	6.2%	21.6%	15.3%
	เสี่ยง	Count	151	181	332
		% within การฝึกอบรม	93.8%	78.4%	84.7%
Total		Count	161	231	392
		% within การฝึกอบรม	100.0%	100.0%	100.0%

ข้อ2 Virus * การฝึกอบรม Crosstabulation

			การฝึกอบรม		Total
			เคยผ่านหลักสูตร	ไม่เคยผ่านหลักสูตร	
ข้อ2 Virus	ไม่เสี่ยง	Count	53	80	133
		% within การฝึกอบรม	32.9%	34.6%	33.9%
	เสี่ยง	Count	108	151	259
		% within การฝึกอบรม	67.1%	65.4%	66.1%
Total		Count	161	231	392
		% within การฝึกอบรม	100.0%	100.0%	100.0%

ข้อ3 Virus * การฝึกอบรม Crosstabulation

			การฝึกอบรม		Total
			เคยผ่านหลักสูตร	ไม่เคยผ่านหลักสูตร	
ข้อ3 Virus	ไม่เสี่ยง	Count	105	87	192
		% within การฝึกอบรม	65.2%	37.7%	49.0%
	เสี่ยง	Count	56	144	200
		% within การฝึกอบรม	34.8%	62.3%	51.0%
Total		Count	161	231	392
		% within การฝึกอบรม	100.0%	100.0%	100.0%

ข้อ4 Virus * การฝึกอบรม Crosstabulation

			การฝึกอบรม		Total
			เคยผ่านหลักสูตร	ไม่เคยผ่านหลักสูตร	
ข้อ4 Virus	ไม่เสี่ยง	Count	43	79	122
		% within การฝึกอบรม	26.7%	34.2%	31.1%
	เสี่ยง	Count	118	152	270
		% within การฝึกอบรม	73.3%	65.8%	68.9%
Total		Count	161	231	392
		% within การฝึกอบรม	100.0%	100.0%	100.0%

ตารางที่ 4.19 (ต่อ)

4.19.3 ด้านนโยบาย ข้อกฎหมาย กฎระเบียบข้อบังคับต่าง ๆ

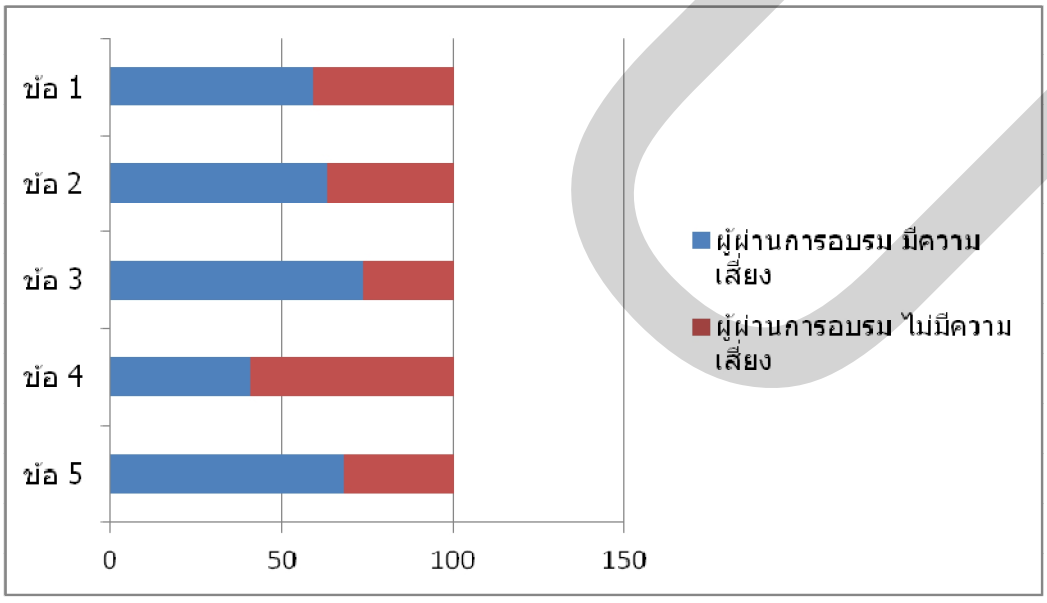
ข้อกฎหมายนโยบาย * การฝึกอบรม Crosstabulation

			การฝึกอบรม		
			เคยผ่านหลักสูตร	ไม่เคยผ่านหลักสูตร	Total
ข้อกฎหมายนโยบาย	ไม่เสี่ยง	Count	104	88	192
		% within การฝึกอบรม	64.6%	38.1%	49.0%
	เสี่ยง	Count	57	143	200
		% within การฝึกอบรม	35.4%	61.9%	51.0%
Total		Count	161	231	392
		% within การฝึกอบรม	100.0%	100.0%	100.0%

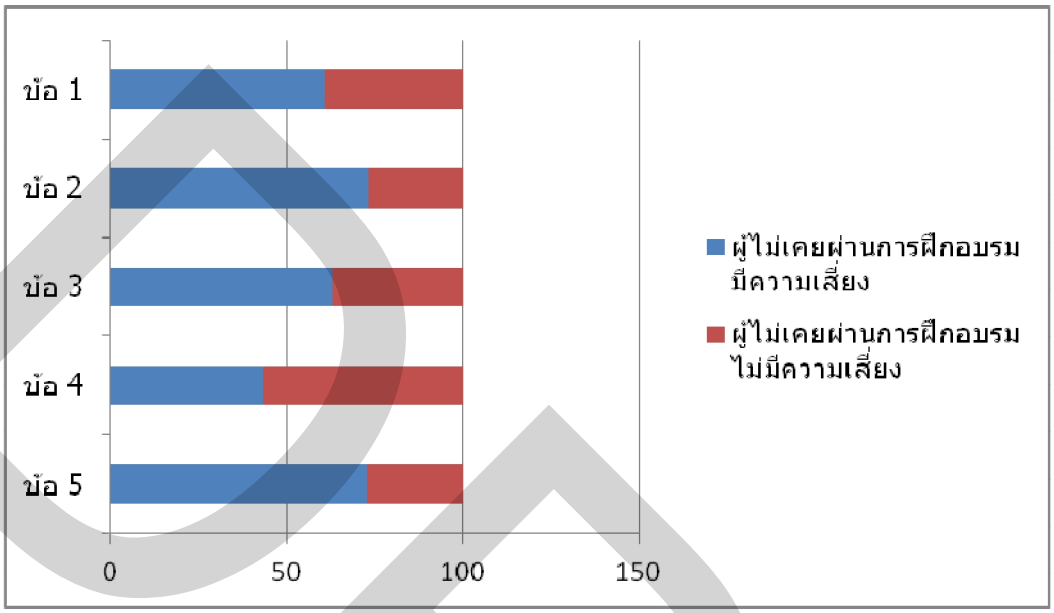
ภาพที่ 4.19 ผลการทดสอบพฤติกรรมความเสี่ยงเทียบผลวิเคราะห์ระหว่างทดสอบพฤติกรรมความเสี่ยงของ ผู้เข้ารับการฝึกอบรมกับผู้ที่ไม่เคยผ่านการฝึกอบรม

4.19.1 ด้านข้อมูล

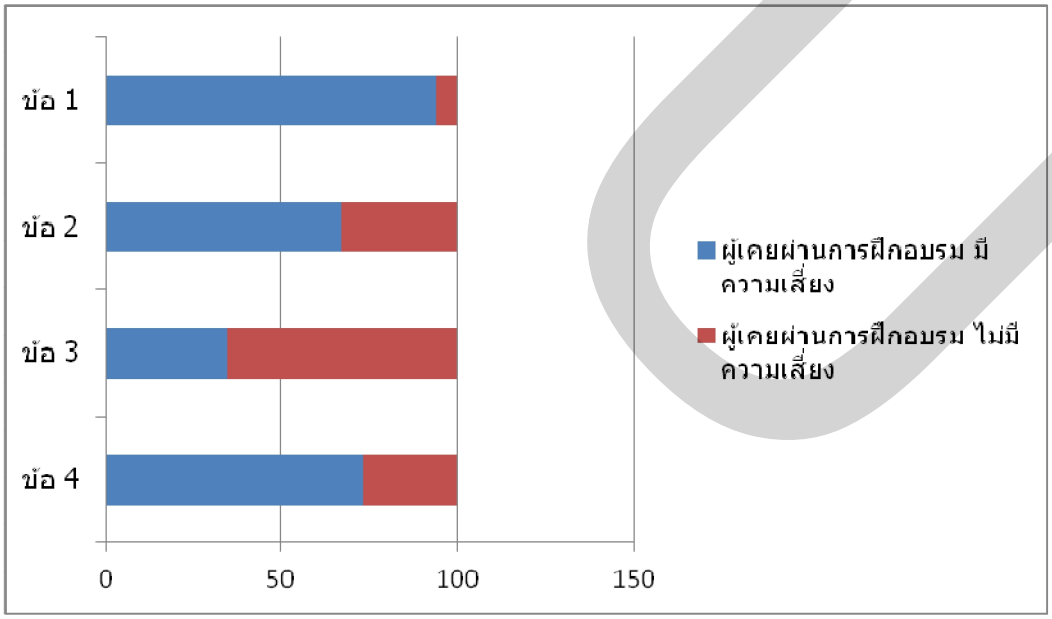
.



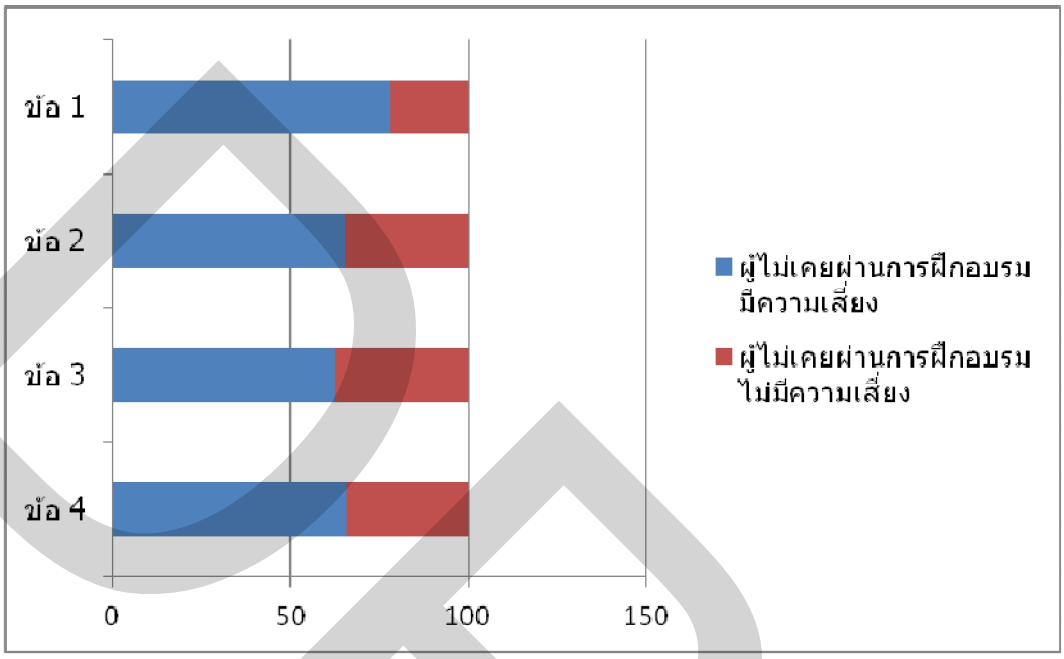
ภาพที่ 4.19 (ต่อ)



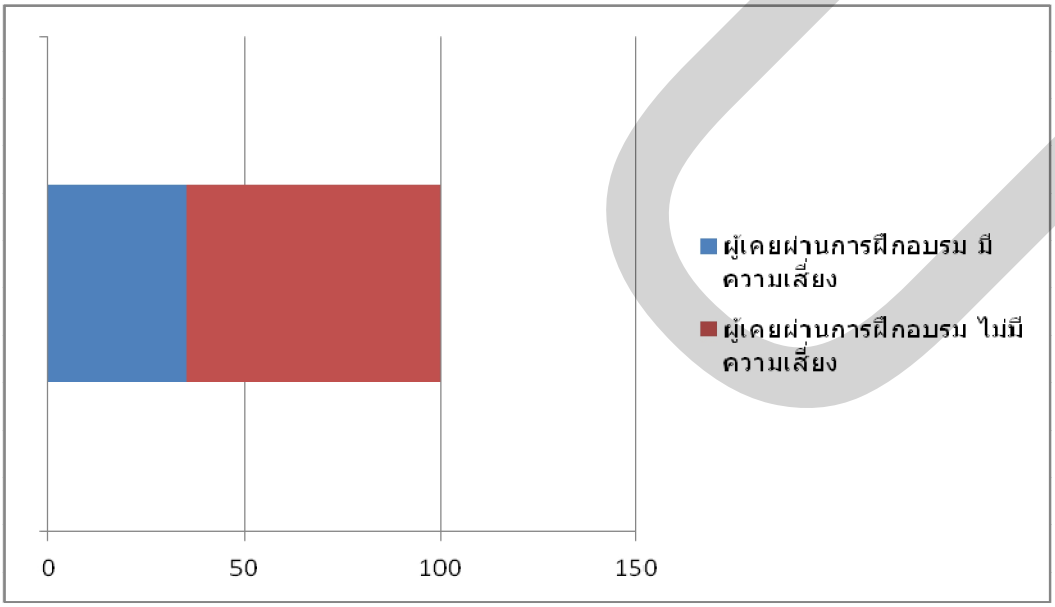
4.19.2 ด้านเกี่ยวกับ ภัยคุกคาม ระบบการป้องกันภัยคุกคาม



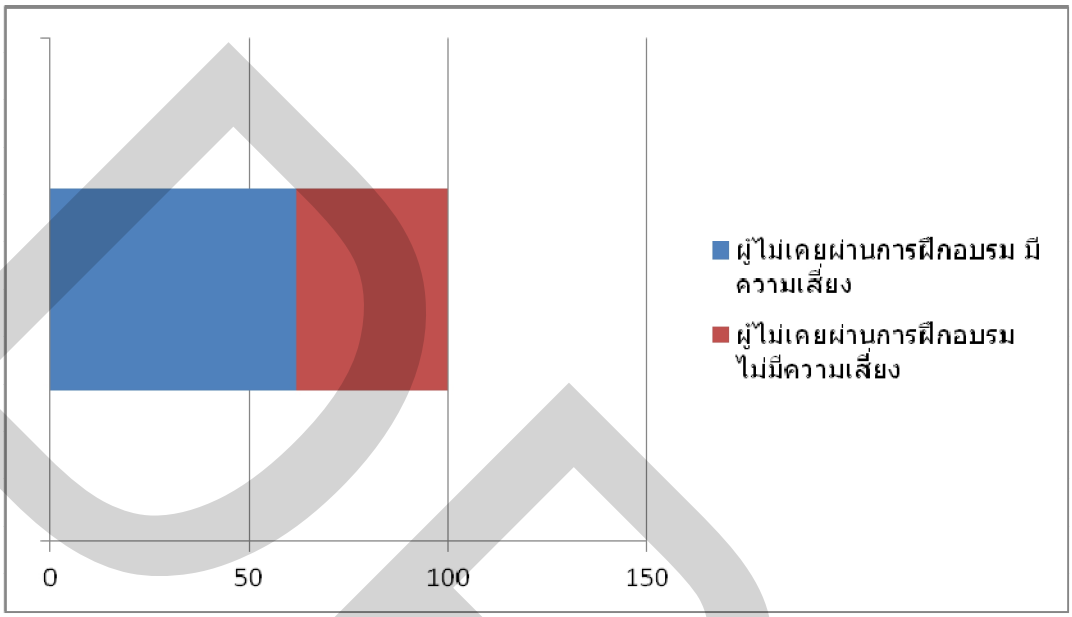
ภาพที่ 4.19 (ต่อ)



4.19.3 ด้านนโยบาย ข้อกฎหมาย กฎระเบียบข้อบังคับต่าง ๆ



ภาพที่ 4.19 (ต่อ)


ผู้ไม่เคยผ่านการฝึกอบรม มีความเสี่ยง
ผู้ไม่เคยผ่านการฝึกอบรม ไม่มีความเสี่ยง
0
50
100
150

บทที่ 5
สรุปการศึกษาวิเคราะห์และข้อเสนอแนะ

การศึกษาครั้งนี้ มีวัตถุประสงค์เพื่อศึกษาถึงข้าราชการใน กองบัญชาการกองทัพไทย ว่ามีความรู้ ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศของข้อมูล ในยุคปัจจุบัน เป็นอย่างไร และมีวิธีการดูแลรักษาป้องกันเบื้องต้นของข้าราชการเป็นอย่างไร เพื่อที่จะได้นำผลการศึกษาในครั้งนี้ไปใช้ในการวิเคราะห์ข้อมูลและอุดช่องโหว่ในด้านการรักษาความมั่นคงปลอดภัย ของ กองบัญชาการกองทัพไทย ต่อไป และจัดให้มีการฝึกอบรมหลักสูตรการรักษาความปลอดภัยสารสนเทศ ของ กองบัญชาการกองทัพไทย เน้นในด้านที่เป็นจุดอ่อน ของข้าราชการ เป็นพิเศษ จากจำนวนแบบสอบถามของกลุ่มตัวอย่าง 392 คน โดยการวิเคราะห์ค่าเฉลี่ย และเปรียบเทียบระหว่างค่าตัวแปรสองตัวแปร โดยสามารถสรุปผลการศึกษาและข้อเสนอแนะได้ดังนี้

5.1 สรุปผลการศึกษา

5.1.1 ส่วนที่ 1 ข้อมูลลักษณะทั่วไปของข้าราชการ กองบัญชาการกองทัพไทย ลักษณะทางด้านปัจจัยส่วนบุคคล

จากผลการวิเคราะห์พบว่าข้าราชการส่วนใหญ่เป็นเพศชาย ถึงร้อยละ 56.9 วิเคราะห์ได้ว่าเป็นเพราะว่าอัตราการบรรจุ โดยรับการบรรจุข้าราชการมาจาก นักเรียนโรงเรียนทหาร การบรรจุเฉพาะตำแหน่งบุคคลที่ผ่านกองหนุนมาแล้ว ส่วนข้าราชการหญิง รับมาจากการบรรจุบุคคลพลเรือน อายุ โดยเฉลี่ยอยู่ที่ 21 ปี - 30 ปี คิดเป็นร้อยละ 35.5 วิเคราะห์ได้ว่าเป็นเพราะช่วงอายุนี้อยู่ในช่วงที่บรรจุเข้ารับราชการ เพื่อเป็นการทดแทนกำลังพลในแต่ละปี ข้าราชการส่วนมากจึงมีอายุอยู่ในเกณฑ์ช่วงนี้ การศึกษาโดยภาพรวมอยู่ในระดับ ปริญญาตรี คิดเป็นร้อยละ 36.7 วิเคราะห์ได้ว่าเป็นเพราะว่าการเข้ารับราชการ การบรรจุนายทหารสัญญาบัตร ซึ่งรับผู้ที่จบตามวุฒิขั้นต่ำ ปริญญาตรี และ นายทหารประทวนที่จะทำการสอบทำหน้าที่นายทหารสัญญาบัตรต้องมีคุณสมบัติ ด้วยการเรียนรู้เพิ่มเติมในคุณวุฒิปริญญาตรี จึงมีสิทธิ์สอบบรรจุ ในอัตราดังกล่าว จึงทำให้ข้าราชการบางท่านได้ศึกษาเพิ่มเติมจนจบคุณวุฒิปริญญาตรี เพื่อใช้ในการเตรียมตัวสอบปรับคุณวุฒิเป็นข้าราชการชั้นสัญญาบัตรระดับหน้าที่การงาน ผลออกมาพบว่าเป็นข้าราชการชั้นสัญญาบัตร จำนวน 132 นาย คิดเป็นร้อยละ 31.4 เป็นข้าราชการชั้นประทวน จำนวน 211 นาย คิดเป็นร้อยละ 53.8 เป็นข้าราชการลูกจ้างพนักงาน จำนวน 58 นาย คิดเป็นร้อยละ 14.8 วิเคราะห์ว่า

การบรรจุข้าราชการชั้นสัญญาบัตร จะบรรจุเฉพาะข้าราชการที่มีคุณสมบัติสูงเป็นนักเรียนหรือรับผู้ที่จบคุณวุฒิปริญญาตรีขึ้นไป ในอัตราการบรรจุจะน้อยกว่า ส่วนข้าราชการชั้นประทวนเป็นอัตราที่บรรจุ จากนักเรียน หรือบุคคลพลเรือน และมีการบรรจุเพื่อทดแทนจำนวนมาก เพื่อเป็นกำลังหลักในการปฏิบัติงาน ลูกจ้างพนักงาน การบรรจุจะเป็นแบบสัญญาจ้าง หมดอายุต้องต่อสัญญา หรือว่าเลิกจ้าง การจัดหาเพื่อทดแทนตำแหน่งที่ไม่สามารถบรรจุลงได้ในอัตราข้าราชการชั้นประทวน จึงทำให้มีการเปิดอัตราชั่วคราวเป็นอัตราจ้างที่น้อยกว่าปกติ ข้าราชการที่เคยเข้ารับการอบรมผ่านหลักสูตร คิดเป็น ร้อยละ 41.1 ข้าราชการที่ไม่เคยเข้ารับการอบรม คิดเป็นร้อยละ 58.9 วิเคราะห์ได้ว่า การเปิดหลักสูตร มีเพียงปีละครั้ง ตามห้วงปีงบประมาณผู้เข้ารับการฝึกอบรมส่วนมากจะเป็นเจ้าหน้าที่ ที่เกี่ยวข้อง หรือข้าราชการที่หน่วยส่งตัวมา เพื่อเป็นตัวแทนในการเข้ารับ การฝึกอบรม ยังคงมีกำลังพล ส่วนใหญ่ ที่บรรจุเข้ารับราชการใหม่ และข้าราชการลูกจ้างพนักงาน อีกจำนวนมากที่ยังไม่เคยได้ผ่านการเข้ารับการฝึกอบรมหลักสูตรการรักษาความมั่นคงปลอดภัย ของ กองบัญชาการกองทัพไทย

5.1.2 ส่วนที่ 2 ตามพฤติกรรมการใช้คอมพิวเตอร์ภายในเครือข่าย กองบัญชาการกองทัพไทย

จากผลการวิเคราะห์พบว่าคอมพิวเตอร์ส่วนใหญ่ เป็นเครื่องคอมพิวเตอร์ของสำนักงาน ร้อยละ 81.4 คอมพิวเตอร์ส่วนตัว เป็นร้อยละ 18.6 วิเคราะห์ว่า ด้วยการจัดหาเครื่องคอมพิวเตอร์ใช้ภายในสำนักงาน จะมีงบประมาณในการจัดซื้อจัดจ้าง ตามแต่ปีงบประมาณ ส่วนคอมพิวเตอร์ที่ไม่เพียงพอ ก็จะนำเครื่องส่วนตัวมาใช้ภายในเครือข่ายของทางราชการ เพื่อสะดวกแก่การปฏิบัติงานและจัดประชุมวางแผนงาน การใช้งานร่วมกันของเครื่องคอมพิวเตอร์สำนักงาน อัตราร้อยละ 65.3 และไม่มีการใช้งานร่วมกันส่วนมากจะเป็นคอมพิวเตอร์ส่วนตัว อัตราร้อยละ 34.7 วิเคราะห์ได้ว่าการใช้งานคอมพิวเตอร์สำนักงาน ต้องมีการทำงานร่วมกัน มีการแก้งาน หรือเจ้าหน้าที่ ที่ใช้งานด้านการพิมพ์ร่วมกันส่วนอัตราที่ไม่เคยมีผู้มาใช้งานร่วมกัน อาจเป็นเพราะว่า การใช้งานส่วนบุคคลเฉพาะตำแหน่ง หรือคอมพิวเตอร์ส่วนตัว จึงมีอัตราร้อยละ 34.7 การเชื่อมต่ออุปกรณ์ชนิดอื่นเข้ากับเครือข่ายใน กองบัญชาการกองทัพไทย อัตราร้อยละ 33.9 ผู้ที่เคยนำอุปกรณ์ชนิดอื่นมาเชื่อมต่อในระบบเครือข่าย อัตราร้อยละ 66.1 เป็นอัตราผู้ที่ไม่เคยนำอุปกรณ์ชนิดอื่นเข้ามาเชื่อมต่อภายในระบบเครือข่ายของ กองบัญชาการกองทัพไทย วิเคราะห์ได้ว่า ข้าราชการส่วนใหญ่ใช้คอมพิวเตอร์สำนักงานอยู่แล้ว จึงไม่ได้นำอุปกรณ์ชนิดอื่นมาเชื่อมต่อภายในระบบเครือข่าย ส่วนปัจจัยผู้ที่เคยใช้อุปกรณ์มาเชื่อมต่อ จะเป็นเจ้าหน้าที่เฉพาะหรือข้าราชการชั้นผู้ใหญ่ ที่มีการนำเอามือถือ สมาร์ทโฟน หรือ แท็บเล็ต นำมาเชื่อมต่อ ในระหว่างการประชุมหรือหาข้อมูลเร่งด่วน

5.1.3 ส่วนที่ 3 ผลการวัดความรู้ในแต่ละด้านเกี่ยวกับเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ

ผลการวิเคราะห์พบว่าคำถามในแต่ละข้อดังนี้ คำถามเกี่ยวกับด้านข้อมูล คำถามข้อ 1 ถามว่าการเข้ารหัสเพื่อป้องกันผู้อื่นเข้าถึง มีผู้ที่ตอบถูก ร้อยละ 71.2 วิเคราะห์ว่า ข้าราชการส่วนใหญ่ มีความรู้เรื่องการตั้งค่ารหัส จากทางหน้าเว็บไซต์ กองบัญชาการกองทัพไทย จากสื่อประชาสัมพันธ์ของหน่วยงาน จึงทำให้ข้าราชการมีความรู้ในเรื่องการเข้ารหัสเพื่อการป้องกัน คำถามข้อ 2 ถามว่ามาตรฐานการรักษาความปลอดภัยข้อมูล คืออะไร มีผู้ที่ตอบถูก ร้อยละ 56.9 วิเคราะห์ว่า ข้าราชการมีความรู้เรื่องมาตรฐานจากการฝึกอบรม หรือและการค้นหาข้อมูลเพิ่มเติม จากสื่อเว็บไซต์เพื่อทำให้เกิดความรู้ในข้อคำถาม คำถามข้อ 3 ถามว่าการจัดเก็บข้อมูลงานเอกสารต่าง ๆ เป็นอย่างไรมีผู้ตอบถูก ร้อยละ 66.1 วิเคราะห์ว่า ข้าราชการส่วนใหญ่จะแยกเก็บเอกสารเป็นหมวดหมู่ง่ายต่อการค้นหาเมื่อผู้บังคับบัญชาเรียกหาข้อมูล ส่วนอีก ร้อยละ 33.9 จะจัดเก็บไว้ตามหน้า Desktop เพื่อง่ายต่อการหางาน และแก้ไขงานในเบื้องต้น การกระทำทั้งสองอย่าง เป็นการสะดวกแก่การค้นหา ของผู้ที่จะกลับมาแก้ไขพิมพ์งานต่อจากผู้ที่ใช้งานก่อนหน้านี้ เมื่อเจ้าหน้าที่พิมพ์งานไม่อยู่ คำถามข้อ 4 ถามว่าการส่งเครื่องคอมพิวเตอร์เพื่อเข้าซ่อมควรปฏิบัติอย่างไรเกี่ยวกับข้อมูลภายในเครื่องคอมพิวเตอร์ มีผู้ตอบถูก ร้อยละ 48.2 พบว่าส่วนใหญ่กำลังพลยังขาดความเข้าใจในเรื่องการ backup ข้อมูลออกก่อนทำการส่งซ่อม เลือกคำตอบที่ว่าส่งซ่อมกับเจ้าหน้าที่หรือช่างซ่อมผู้ชำนาญโดยตรง เพราะว่าข้าราชการยังขาดความรู้ด้านเทคนิคการบำรุงรักษา และการ backup เก็บข้อมูลอยู่เสมอ เพื่อการรักษาความปลอดภัยด้านข้อมูล การประชาสัมพันธ์ยังไม่ทั่วถึง จึงทำให้ผู้ใช้งานทั่วไป เมื่อคอมพิวเตอร์เสีย จึงหาทางแก้ไขเพื่อให้ใช้งานต่อได้เพียงอย่างเดียว คำถามข้อ 5 ถามว่าการตั้งแชร์ข้อมูลผ่านระบบเครือข่าย มีผู้ตอบถูก ร้อยละ 29.1 วิเคราะห์ว่าข้าราชการส่วนใหญ่จะไม่เข้าใจเรื่องการตั้งค่ารหัสในการแชร์ข้อมูล ใช้ร่วมกันไม่รู้วิธีตั้งรหัส จึงทำให้ตั้งค่าแบบอ่านได้และเขียนทับได้ หรือตั้งค่าแบบอ่านได้เพียงอย่างเดียวโดยที่ข้อมูลก็อาจถูกบุคคลอื่นเข้ามาค้นหาภายในเครือข่ายได้ง่าย จึงไม่ปลอดภัยต่อข้อมูลภายในเครือข่าย เพราะว่าข้าราชการบางท่านยังขาดการเรียนรู้ และความเข้าใจของการแชร์ไฟล์ที่ถูกต้อง คำถามเกี่ยวกับด้านภัยคุกคาม ระบบการป้องกันภัยคุกคาม คำถามข้อ 1 ถามว่าโปรแกรม Antivirus ที่เจ้าหน้าที่กำหนดให้ติดตั้งภายในเครือข่ายของ กองบัญชาการกองทัพไทย มีผู้ที่ตอบถูก ร้อยละ 26.5 ซึ่งน้อยมาก วิเคราะห์ได้ว่าข้าราชการส่วนใหญ่ยังไม่ทราบว่า ภายในเครือข่ายกองบัญชาการกองทัพไทย กำหนดให้มีการติดตั้ง Antivirus ชนิดใด ส่วนมากจะหามาติดตั้งเองตามที่สะดวกง่าย บางครั้งโปรแกรมที่เจ้าหน้าที่ติดตั้งก็ทำให้เครื่องโหลดหนักการทำงานช้าด้วยการ scan ตลอดเวลา คุณภาพเครื่องคอมพิวเตอร์ ที่มีอยู่ในเกณฑ์ล่าสมัย ผู้ใช้จึงได้ทำการเอาโปรแกรม Antivirus ออกแล้วลงโปรแกรมที่ทำงานเบากับเครื่อง เช่น Nod32 Antivirus

เป็นส่วนใหญ่ ทั้ง ๆ ที่กองบัญชาการกองทัพไทย กำหนดให้ใช้ Trend Micro Antivirus เพื่อง่ายต่อที่เจ้าหน้าที่จะทำการค้นหาหรือควบคุม ระบบรักษาความปลอดภัย ในการส่งข้อมูลตอบรับหรือ scan ค้นหา เพื่ออุดช่องโหว่ที่อาจแพร่กระจายได้ง่าย คำถามข้อ 2 ถามว่าการนำ Flash drive มา save งาน นำมาเสียบเข้าในระบบคอมพิวเตอร์ควรปฏิบัติอย่างไร มีผู้ที่ตอบถูก ร้อยละ 86 เข้าใจดีว่าต้องทำการตรวจสอบ scan virus ก่อนเปิดทุกครั้งเพื่อปกป้องเครื่องคอมพิวเตอร์ ของตนเอง ไม่ให้ติด virus ที่มาจาก Flash drive มีความรู้เรื่องการปกป้อง virus และเกรงว่าจะนำพามาติดที่เครื่องของตนเองได้ คำถามข้อ 3 ถามถึงความรู้เกี่ยวกับการทำงานของ Malware คืออะไร มีผู้ตอบถูก ร้อยละ 57.9 วิเคราะห์ได้ว่าข้าราชการใส่ใจที่จะค้นหาคำตอบจากสื่อต่าง ๆ ที่ตนเองไม่เคยรู้มาก่อน กับข้าราชการบางส่วนไม่เคยรู้เรื่องการทำงานนี้เลย ลักษณะ คำตอบจึงอยู่ในค่าระดับกลางๆ ค่าที่ได้ใกล้เคียงกัน คำถามข้อ 4 ความรู้เกี่ยวกับการทำงานของ Backdoor คืออะไร มีผู้ตอบถูก ร้อยละ 65.6 วิเคราะห์ได้ว่า ข้าราชการใส่ใจที่จะค้นหาคำตอบจากสื่อต่าง ๆ ที่ตนเองไม่เคยรู้มาก่อน กับข้าราชการบางส่วนไม่เคยรู้เรื่องการทำงานนี้เลย ลักษณะ คำตอบจึงอยู่ในค่าระดับกลาง ๆ ค่าที่ได้ใกล้เคียงกัน คำถามข้อ 5 ความรู้เกี่ยวกับการทำงานของ Spyware คืออะไร มีผู้ตอบถูก ร้อยละ 45.7 วิเคราะห์ได้ว่า ข้าราชการใส่ใจที่จะค้นหาคำตอบจากสื่อต่าง ๆ ที่ตนเอง ไม่เคยรู้มาก่อนกับข้าราชการบางส่วนไม่เคยรู้เรื่องการทำงานนี้เลย ลักษณะ คำตอบ จึงอยู่ในค่าระดับกลาง ๆ ค่าที่ได้ใกล้เคียงกัน จากคำถาม เกี่ยวกับการทำงาน และลักษณะของ Virus แต่ละชนิด เป็นการทดสอบผลออกมาอยู่ในค่าเกณฑ์ที่ใกล้เคียงกัน จากการค้นหาความหมายของคำตอบกับผู้ที่รู้อยู่แล้วกับผู้ที่ไม่เคยรู้เรื่องแบบนี้ และการคาดเดาลักษณะคำตอบ ตามความน่าจะเป็นของคำถามคำตอบ เพราะการทดสอบแบบสอบถามชนิดนี้ ไม่ได้ทำการทดสอบเฉพาะที่ห้ามค้นหาข้อมูลที่ถูกต้อง ค่าที่ได้แตกต่างกันจึงอยู่กับผู้ที่ไม่ทราบคำตอบจริง ๆ คำถามเกี่ยวกับด้านนโยบาย ข้อกฎหมาย กฎระเบียบข้อบังคับต่าง ๆ คำถามข้อ 1 ถามว่าความรู้เกี่ยวกับ พรบ. คอมพิวเตอร์ มีกี่หมวด มีผู้ที่ตอบถูก ร้อยละ 30.1 วิเคราะห์ได้ว่าข้าราชการยังขาดความรู้เรื่อง พรบ. คอมพิวเตอร์ ไม่เคยค้นคว้าหาข้อมูลมาก่อน จึงให้หลักความน่าจะเป็นในการตอบคำถาม อีกอย่างคำถามเป็นแบบลักษณะตัวเลขใกล้เคียงกัน ค่าร้อยละที่ได้จึงอยู่ในเกณฑ์ที่ผู้รู้เรื่องนี้หรือสนใจเรื่องนี้น้อยมาก คำถามข้อ 2 ถามถึงข้อ พรบ. การกระทำผิดในการเข้าถึง ซึ่งระบบที่มีผู้ป้องกันไว้แล้ว แต่พยายามที่จะกระทำผิด มีผู้ที่ตอบถูก ร้อยละ 48.5 วิเคราะห์ว่าคำถามอยู่ในหลักกฎหมาย ข้าราชการขาดความเอาใจใส่ในเรื่องกฎหมาย ต้องค้นหาคำตอบที่ถูกต้อง ก็จะตอบคำถามข้อนี้ได้ คำถามเป็นลักษณะการท่องจำ จึงจะตอบคำถามได้ แต่ถ้าถามว่ารู้ไหมว่าทำแบบนี้แล้วผิด คำตอบน่าจะทำได้ดีกว่านี้ คำถามข้อ 3 ถามถึงข้อ พรบ. การกระทำผิดในการเข้าถึงซึ่งข้อมูลที่มีผู้ป้องกันไว้แล้ว แต่พยายามที่จะกระทำผิด มีผู้ที่ตอบถูก ร้อยละ 44.6 วิเคราะห์ว่าคำถามอยู่ในหลักกฎหมาย ข้าราชการขาดความเอาใจใส่ในเรื่องกฎหมาย ต้องค้นหา

คำตอบที่ถูกต้อง ก็จะตอบคำถามข้อนี้ได้ คำถามเป็นลักษณะการท่องจำ จึงจะตอบคำถามได้ แต่ถ้าถามว่ารู้ไหมว่าทำแบบนี้แล้วผิด คำตอบน่าจะทำได้ดีกว่านี้ คำถามข้อ 4 ถามถึงข้อ พรบ. การกระทำผิดในการให้ข้อมูลเป็นเท็จเกิดการเสียหายต่อความมั่นคงประเทศ หรือการตื่นตระหนกของประชาชน มีผู้ที่ตอบถูก ร้อยละ 54.3 วิเคราะห์ว่าคำถามอยู่ในหลักกฎหมาย ข้าราชการขาดความเอาใจใส่ในเรื่องกฎหมาย ต้องค้นหาคำตอบที่ถูกต้อง ก็จะตอบคำถามข้อนี้ได้ คำถามเป็นลักษณะการท่องจำ จึงจะตอบคำถามได้ แต่ถ้าถามว่ารู้ไหมว่าทำแบบนี้แล้วผิด คำตอบน่าจะทำได้ดีกว่านี้ คำถามข้อ 5 ถามว่าการออกใช้ ของ ระเบียบ กองบัญชาการทหารสูงสุด ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ ของ กองบัญชาการกองทัพไทย เมื่อใด มีผู้ที่ตอบถูก ร้อยละ 52.3 วิเคราะห์ว่าคำถามอยู่ใน หลักระเบียบนโยบายออกให้ข้าราชการปฏิบัติ เป็นคำถามเกี่ยวกับวันที่ออกคำระเบียบ ผู้ที่ตอบได้ ก็จะเป็นผู้ที่ใส่ใจค้นหาระเบียบนี้ขึ้นมา เพื่อตอบคำถามที่ถูกต้อง ผลการทดสอบจำนวน 5 ข้อดังกล่าว จึงเป็นเหตุ วิเคราะห์ในภาพรวมได้ว่า เรื่องการออกกฎหมายระเบียบ ต่าง ๆ ต้องอาศัย การอ่านหรือ ท่องจำเป็นพิเศษ ซึ่งข้าราชการไม่ได้นำไปใช้ในชีวิตประจำวัน จึงทำให้ผลออกมาอยู่ในระดับน้อยมาก ค่าคำตอบที่ได้จึงอยู่ในลักษณะใกล้เคียงกัน ค่าที่ได้แตกต่างกันจึงอยู่กับผู้ที่ไม่ทราบคำตอบจริง ๆ

5.1.3.1 การทดสอบความรู้ผลเปรียบเทียบ ระหว่าง ข้าราชการตำแหน่งหน้าที่แต่ละลำดับชั้นผลที่ได้คือ คำถามทางด้านข้อมูล ข้าราชการชั้นสัญญาบัตร มีจำนวนที่ผ่านเกณฑ์ทั้งสิ้น 4 ข้อ ข้าราชการชั้นประทวน มีจำนวนที่ผ่านเกณฑ์ทั้งสิ้น 3 ข้อ ข้าราชการลูกจ้างพนักงานราชการ มีจำนวนที่ผ่านเกณฑ์ทั้งสิ้น 2 ข้อ วิเคราะห์ว่า ข้าราชการแตกต่างตามชั้นยศตำแหน่งอย่างเห็นได้ชัด เป็นเพราะว่าการรับรู้ศึกษาจะให้ความสำคัญต่อระดับข้าราชการชั้นสัญญาบัตรก่อน ส่วนข้าราชการชั้นประทวนเป็นเพียงเจ้าหน้าที่ ที่อยู่ในความรับผิดชอบ หรือต้องค้นหาความรู้ด้วยตัวเอง หรือใช้ความรู้ในการเพื่อทดสอบในการสอบเลื่อนฐานะนายทหารชั้นสัญญาบัตร ข้าราชการลูกจ้างพนักงาน ซึ่งบรรจุจากคุณวุฒิ ปวช. ปวส. จึงมีความรอบรู้น้อยกว่า ผู้ที่บรรจุอยู่อายุราชการมากกว่าด้วยประสบการณ์ คำถามด้านป้องกันภัยคุกคาม ข้าราชการชั้นสัญญาบัตร มีจำนวนที่ผ่านเกณฑ์ทั้งสิ้น 4 ข้อ ข้าราชการชั้นประทวน มีจำนวนที่ผ่านเกณฑ์ทั้งสิ้น 3 ข้อ ข้าราชการลูกจ้างพนักงานราชการ มีจำนวนที่ผ่านเกณฑ์ทั้งสิ้น 2 ข้อ วิเคราะห์ว่า ข้าราชการแตกต่างตามชั้นยศตำแหน่งอย่างเห็นได้ชัด เป็นเพราะว่าการรับรู้ศึกษาจะให้ความสำคัญต่อระดับข้าราชการชั้นสัญญาบัตรก่อน ส่วนข้าราชการชั้นประทวนเป็นเพียงเจ้าหน้าที่ที่อยู่ในความรับผิดชอบ หรือต้องค้นหาความรู้ด้วยตัวเอง หรือใช้ความรู้ในการเพื่อทดสอบในการสอบเลื่อนฐานะนายทหาร ข้าราชการลูกจ้างพนักงาน ซึ่งบรรจุจากคุณวุฒิ ปวช. ปวส. จึงมีความรอบรู้น้อยกว่า ผู้ที่บรรจุอยู่อายุราชการมากกว่าด้วยประสบการณ์ ด้านกฎหมายกฎระเบียบข้อบังคับ ข้าราชการชั้นสัญญาบัตร มีจำนวนที่

ผ่านเกณฑ์ทั้งสิ้น 4 ข้อ ข้าราชการชั้นประทวน มีจำนวนที่ผ่านเกณฑ์ทั้งสิ้น 3 ข้อ ข้าราชการลูกจ้าง พนักงานราชการ มีจำนวนที่ผ่านเกณฑ์ทั้งสิ้น 4 ข้อ วิเคราะห์ว่า จากที่เห็น ข้าราชการสัญญาบัตร กับข้าราชการลูกจ้าง จะทำคะแนนได้ดีในข้อนี้อาจเป็นเพราะว่าค้นหาความรู้ในการที่จะตอบแบบสอบถาม เพราะเป็น สิ่งที่เขาไม่ทราบ ในระหว่างที่ข้าราชการชั้นประทวน จะตอบคำถามมาจากประสบการณ์การทำงานคาดเดา ความน่าจะเป็น

5.1.3.2 การทดสอบความรู้ผลเปรียบเทียบ ระหว่าง ผู้ที่เข้ารับการฝึกอบรม และผู้ที่ไม่เคยเข้ารับการฝึกอบรม ผลที่ได้คือ คำถามทางด้านข้อมูล ผู้ผ่านการฝึกอบรม มีจำนวนที่ผ่านเกณฑ์ทั้งสิ้น 4ข้อ ผู้ไม่เคยผ่านการฝึกอบรม มีจำนวนที่ผ่านเกณฑ์ทั้งสิ้น 2 ข้อ วิเคราะห์ว่า จากที่เห็น ข้าราชการที่ผ่านการฝึกอบรมมาแล้วจะทำการทดสอบได้ดีกว่า จึงทำให้ผลออกมาอยู่ในเกณฑ์ที่ดีกว่าผู้ที่ยังไม่ได้รับการฝึกอบรม เพราะว่า ไม่มีประสบการณ์และความรู้เท่า ในการทดสอบ จึงทำให้ผลออกมาอยู่ในเกณฑ์ที่น้อย เพราะว่าไม่เคยรับรู้ข้อมูลมาก่อน คำถามด้านป้องกันภัยคุกคาม ผู้ผ่านการฝึกอบรม มีจำนวนที่ผ่านเกณฑ์ทั้งสิ้น 3ข้อ ผู้ไม่เคยผ่านการฝึกอบรม มีจำนวนที่ผ่านเกณฑ์ทั้งสิ้น 2 ข้อ วิเคราะห์ว่า จากที่เห็น ข้าราชการที่ผ่านการฝึกอบรมมาแล้วจะทำการทดสอบได้ดีกว่า ผู้ที่ยังไม่ได้รับการฝึกอบรม เพราะว่า ไม่มีประสบการณ์และความรู้เท่าในการทดสอบจึงทำให้ผลออกมาอยู่ในเกณฑ์ที่น้อย เพราะว่าตัวเองไม่มีความรู้ทางด้านนี้ คำถามทางด้านกฎหมายกฎระเบียบข้อบังคับ ผู้ผ่านการฝึกอบรม มีจำนวนที่ผ่านเกณฑ์ทั้งสิ้น 3 ข้อ ผู้ไม่เคยผ่านการฝึกอบรม ไม่มีจำนวนที่ผ่านเกณฑ์เลย วิเคราะห์ได้ว่า จากที่เห็น ข้าราชการที่ผ่านการฝึกอบรมมาแล้วจะทำการทดสอบได้ดีกว่า จึงทำให้ผลออกมาอยู่ในเกณฑ์ที่ปานกลาง ผู้ที่ยังไม่ได้รับการฝึกอบรม และไม่มีประสบการณ์ความรู้ในการทดสอบนี้เลย จึงทำให้ผลออกมาอยู่ในเกณฑ์ไม่ผ่านทำได้น้อยมาก ไม่มีความเข้าใจในเรื่องนี้เลย

5.1.4 ส่วนที่ 4 ผลการวัดพฤติกรรมความเสี่ยงในแต่ละด้านเกี่ยวกับเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ

ผลการวิเคราะห์พบว่าคำถามการทดสอบพฤติกรรมความเสี่ยงในภาพรวมผลที่ได้คือ คำถามทางด้านข้อมูล มีจำนวนที่มีความเสี่ยงต่อภัยคุกคามทั้งสิ้น 4 ข้อ จาก 5 คำถาม คำถามด้านป้องกันภัยคุกคาม มีความเสี่ยงต่อภัยคุกคามทั้งสิ้น 4 ข้อ จาก 4 คำถาม และคำถามทางด้านกฎหมาย ระเบียบ และนโยบาย มีความเสี่ยงต่อภัยคุกคาม ร้อยละ 51 จาก 1 คำถาม รวมทั้งสิ้น 10 คำถาม ผลการวิเคราะห์จากคำถามทดสอบพฤติกรรมความเสี่ยงต่อภัยคุกคามในแต่ละข้อ คำถามเกี่ยวกับด้านข้อมูล จำนวน 5 ข้อ คำถามข้อ 1 ถามถึงการเข้าถึงการจดจำรหัสของตัวเอง มีผู้อยู่ในกลุ่มเสี่ยง ร้อยละ 60.2 วิเคราะห์ว่า ข้าราชการส่วนใหญ่ เคยบันทึกรหัสผ่าน เพื่อเข้าถึงข้อมูลไว้ใกล้บริเวณโต๊ะที่ทำงาน เพื่อสะดวกแก่การจดจำเข้าถึงได้ง่ายของตัวเอง กลัวที่จะลืมรหัส

แต่ยังไม่นึกถึงการป้องกันทางด้านความปลอดภัยของข้อมูล คำถามข้อ 2 ถามถึงเรื่องการ backup ไฟล์ข้อมูล หรือไม่ มีผู้อยู่ในกลุ่มเสี่ยง ร้อยละ 69.1 วิเคราะห์ว่า ข้าราชการส่วนใหญ่ ไม่เคย backup ข้อมูลของตัวเองหรือข้อมูลราชการไว้เลย เพราะคิดว่าข้อมูลคงไม่หายไปไหนพอคอมพิวเตอร์เสีย ก็แค่ว่าทำงานไม่ได้ งานอยู่ในเครื่องจึงต้องทำใหม่อีกครั้ง และไม่รู้ว่าข้อมูลไหนสำคัญเป็นความลับที่จะต้องให้ความสำคัญเป็นพิเศษ ถ้าเกิดรั่วไหลออกไป ถ้าผู้บังคับบัญชาไม่ได้สั่งการปกป้องมาโดยเฉพาะ คำถามข้อ 3 ถามถึงการส่งซ่อม โดยการ backup ข้อมูลออกก่อน เพื่อให้ข้อมูลของเราไม่รั่วไหลออกไป มีผู้อยู่ในกลุ่มเสี่ยง ร้อยละ 67.3 เป็นคำถามใกล้เคียงกับข้อที่แล้ว แต่เป็นคำถามที่ว่า ส่งต่อไปให้เจ้าหน้าที่ซ่อม เราสามารถ backup ข้อมูลออกก่อน เพื่อไม่ให้ตกไปถึงผู้อื่น วิเคราะห์ได้ว่า ข้าราชการยังขาดการเรียนรู้ถึงวิธีการแก้ไขเบื้องต้น และไม่ได้ทำการ backup ข้อมูลไว้เลย จึงเป็นเหตุให้อยู่ในกลุ่มเสี่ยงต่อข้อมูลรั่วไหลไปถึงบุคคลที่ไม่มีหน้าที่การเกี่ยวข้องกับงานในหน้าที่ เพราะว่าการประชาสัมพันธ์ในเรื่องนี้ ยังไม่มี คำถามข้อ 4 ถามถึงการแชร์ไฟล์ข้อมูลสำคัญโดยการเข้ารหัสหรือไม่ มีผู้อยู่ในกลุ่มเสี่ยง ร้อยละ 42.3 วิเคราะห์ว่า ข้าราชการยังตระหนักถึงผลเสีย ในการแชร์ข้อมูลสำคัญ จึงมีเกณฑ์ ที่อยู่ในกลุ่มเสี่ยงน้อย เพื่อปกป้องข้อมูลของตัวเองอยู่ และส่วนมากก็จะใช้แต่ Flash drive ในการนำพาข้อมูลไปอีกเครื่องเสียมากกว่า คำถามข้อ 5 ถามถึงการแชร์ไฟล์แบบ full อ่านได้เขียนได้ มีผู้อยู่ในกลุ่มเสี่ยง ร้อยละ 70.9 วิเคราะห์ว่า ข้าราชการยังขาดความเข้าใจที่ถูกต้องถึงลักษณะการแชร์ข้อมูลแบบอ่านได้เขียนได้ ผลเสียเป็นแบบไหนอย่างไร คิดว่าคงอยากให้มีการแชร์ข้อมูลเพียงให้ได้ทั้งหมด เลยไม่มีความเข้าใจในเรื่องนี้ที่ถูกต้อง เพราะขาดการประชาสัมพันธ์ที่ดี คำถามเกี่ยวกับด้านภัยคุกคาม ระบบการป้องกันภัยคุกคาม จำนวน 4 ข้อ เป็นคำถามข้อ 6 ถามถึงการใช้ free email ทั่วไป ภายในเครือข่าย กองบัญชาการกองทัพไทยมีผู้อยู่ในกลุ่มเสี่ยง 84.7 วิเคราะห์ว่า ข้าราชการส่วนใหญ่ ใช้ free mail ของตนเอง ภายในระบบเครือข่าย โดยที่ กองบัญชาการกองทัพไทย ก็ออกเผยแพร่ข้อมูลให้ใช้ email ภายใน กองบัญชาการกองทัพไทย @rtarf.mi.th แต่การสมัครขั้นตอนยังไม่เป็นที่แพร่หลาย อาจเป็นเพราะว่า ด้านการประชาสัมพันธ์ยังไม่ดีพอจึงทำให้ข้าราชการไม่ทราบถึงความแตกต่างระหว่างการใช้ free mail กับ email ที่ทางราชการกำหนด คำถามข้อ 7 ถามถึงการ Download โปรแกรม ฟรีแวร์ จากเว็บไซต์มาติดตั้งในคอมพิวเตอร์เครือข่าย ซึ่งอาจมีความเสี่ยงต่อภัยคุกคามที่แอบแฝงมากับโปรแกรมได้ มีผู้อยู่ในกลุ่มเสี่ยง ร้อยละ 66.1 วิเคราะห์ว่า ข้าราชการอีกจำนวนมากที่ใช้โปรแกรม ฟรีแวร์ จากเว็บไซต์ เพื่อสะดวกมาติดตั้งใช้ง่าย การควบคุมเรื่องโปรแกรม ฟรีแวร์ ทำได้ยาก นอกจากข้าราชการจะตระหนักถึงภัยคุกคามที่แอบแฝงมา ส่วนผู้ที่ไม่เคยใช้ ค่าอัตราร้อยละ 33.9 เป็นข้าราชการที่รู้ถึงภัยเสี่ยงหรือไม่ก็เป็นข้าราชการที่จัดการเกี่ยวกับคอมพิวเตอร์ด้านการลงโปรแกรม เพื่อใช้เองไม่เป็น เป็นเพียงแค่ผู้ใช้งานอย่างเดียว คำถามข้อ 8 ถามถึงการศึกษาหาความรู้

เพิ่มเติมของตนเองเกี่ยวกับภัยคุกคาม มีผู้ที่อยู่ในกลุ่มเสี่ยง ร้อยละ 51 วิเคราะห์ว่า ข้าราชการร้อยละ 51 ไม่เคยผ่านการศึกษา ค้นหา ความรู้ด้วยตนเอง เกี่ยวกับ นโยบายการป้องกัน virus ที่อาจแอบแฝงมาในคอมพิวเตอร์ อาจเป็นเพราะว่ากำลังพลส่วนใหญ่จะใช้เวลาในการทำงานเฉพาะเรื่องในหน้าที่ส่วนมากจะขาดการดูแลรักษาหรือหาความรู้เพิ่มเติมมาเพื่อป้องกันภัยต่อคอมพิวเตอร์ของตนเองเป็นเพียงแค่ผู้ใช้งานอย่างเดียว คำถามข้อ 9 ถามถึงการนำ usb flash drive ไปใช้กับคอมพิวเตอร์ที่ไม่มีระบบป้องกัน antivirus มีผู้ที่อยู่ในกลุ่มเสี่ยง ร้อยละ 68.9 วิเคราะห์ได้ว่าข้าราชการส่วนใหญ่รู้ตระหนักถึงภัยคุกคามที่อาจแอบแฝงมากับ usb flash drive แต่ด้วยภารกิจเร่งด่วน เพื่อให้ทันต่อผู้บังคับบัญชา เลยต้องใช้งานดังกล่าว แล้วค่อยนำกลับมา scan กับเครื่องที่มีระบบป้องกันที่ดี อีกครั้ง คำถามเกี่ยวกับด้านนโยบาย ข้อกฎหมาย กฎระเบียบข้อบังคับต่าง ๆ จำนวน 1 ข้อ เป็นคำถามข้อ 10 ถามถึงการศึกษาเกี่ยวกับวิธีป้องกันภัยคุกคาม กฎหมาย นโยบายต่าง ๆ ว่าข้าราชการได้ทำการศึกษาหาความรู้ในเรื่องนี้บ้างหรือไม่ มีผู้อยู่ในกลุ่มเสี่ยง ร้อยละ 51 วิเคราะห์ว่าส่วนมากจะเป็นผู้ที่ไม่เคยผ่านการฝึกอบรม และไม่เคยเข้าใจถึงภัยคุกคามผลเสียของภัยคุกคาม เป็นเพียงแค่ผู้ใช้งานทั่วไป ทำงานเฉพาะหน้าที่ จึงไม่ใส่ใจที่จะทำการศึกษาหาความรู้ในเรื่องดังกล่าว

5.1.4.1 การทดสอบพฤติกรรมความเสี่ยงเปรียบเทียบ ระหว่าง ข้าราชการตำแหน่งหน้าที่แต่ละลำดับชั้น ผลวิเคราะห์ทางด้านข้อมูล ข้าราชการชั้นสัญญาบัตร มีความเสี่ยงจากการทดสอบทั้งสิ้น 4 ข้อ ข้าราชการชั้นประทวน มีความเสี่ยงจากการทดสอบทั้งสิ้น 4 ข้อ ข้าราชการลูกจ้างพนักงานราชการ มีความเสี่ยงจากการทดสอบทั้งสิ้น 5 ข้อ วิเคราะห์ว่า จากที่เห็น ข้าราชการทุกระดับชั้น ยังคงมีความเสี่ยงในด้านข้อมูลอยู่ในระดับสูง ดังเหตุผลที่กล่าวมาว่าเรื่องของหน้าที่งานเร่งด่วน ต้องให้ทันต่อผู้บังคับบัญชา มอบหมาย ด้านป้องกันภัยคุกคาม ข้าราชการชั้นสัญญาบัตร มีความเสี่ยงจากการทดสอบทั้งสิ้น 3 ข้อ ข้าราชการชั้นประทวน มีความเสี่ยงจากการทดสอบทั้งสิ้น 4 ข้อ ข้าราชการลูกจ้างพนักงานราชการ มีความเสี่ยงจากการทดสอบทั้งสิ้น 4 ข้อ วิเคราะห์ว่า จากที่เห็น ข้าราชการทุกระดับชั้น ยังคงมีความเสี่ยงในด้านภัยคุกคามอยู่ในระดับสูง ดังเหตุผลที่กล่าวมาด้วย ว่าเรื่องของหน้าที่และงานเร่งด่วน ต้องทันต่อผู้บังคับบัญชามอบหมายด้านกฎหมายกฎระเบียบข้อบังคับ ข้าราชการชั้นสัญญาบัตร มีความเสี่ยงจากการทดสอบทั้งสิ้น ร้อยละ 54.5 ข้าราชการชั้นประทวน มีความเสี่ยงจากการทดสอบทั้งสิ้น ร้อยละ 45 ข้าราชการลูกจ้างพนักงานราชการ มีความเสี่ยงจากการทดสอบทั้งสิ้น ร้อยละ 65.5 วิเคราะห์ว่า จากที่เห็นข้าราชการชั้นสัญญาบัตร กับลูกจ้างพนักงาน ยังคงมีความเสี่ยงในด้านกฎหมาย อยู่ในระดับสูงเพราะความไม่มีประสบการณ์ไม่รู้และเข้าใจที่ถูกต้อง ในระหว่างที่ข้าราชการประทวนใช้ความรู้และประสบการณ์การทำงานผลความเสี่ยงในข้อนี้เลยน้อยกว่า

5.1.4.2 การทดสอบพฤติกรรมความเสี่ยงเปรียบเทียบ ระหว่าง ผู้ที่เข้ารับการฝึกอบรม และผู้ที่ไม่เคยเข้ารับการฝึกอบรม ผลวิเคราะห์ที่ได้คือ ทางด้านข้อมูล ผู้ผ่านการฝึกอบรม มีความเสี่ยงอยู่ในเกณฑ์ทั้งสิ้น 4 ข้อ ผู้ไม่เคยผ่านการฝึกอบรม มีความเสี่ยงอยู่ในเกณฑ์ทั้งสิ้น 4ข้อ วิเคราะห์ว่า ด้วยเหตุผลที่ว่างานเร่งด่วนตามสายงานผู้บังคับบัญชาสั่งมาจึงทำให้ยังมีความเสี่ยงในด้านข้อมูลที่สูงอยู่ทั้ง ๆ ที่มีความรู้ในด้านนี้ คำถามด้านป้องกันภัยคุกคาม ผู้ผ่านการฝึกอบรม มีความเสี่ยงอยู่ในเกณฑ์ทั้งสิ้น 3ข้อ ผู้ไม่เคยผ่านการฝึกอบรม มีความเสี่ยงอยู่ในเกณฑ์ทั้งสิ้น 4ข้อ วิเคราะห์ว่า จากด้วยเหตุผลที่ว่า งานเร่งด่วน ตามสายงานผู้บังคับบัญชาสั่งมา จึงทำให้ยังมีความเสี่ยงในด้านข้อมูลที่สูงอยู่ แต่ก็ยังน้อยกว่าผู้ที่ไม่เคยผ่านการฝึกอบรม คำถามด้านกฎหมายกฎระเบียบข้อบังคับ ผู้ผ่านการฝึกอบรม มีความเสี่ยงอยู่ในเกณฑ์ทั้งสิ้น ร้อยละ 35.4 ผู้ไม่เคยผ่านการฝึกอบรม มีความเสี่ยงอยู่ในเกณฑ์ทั้งสิ้น ร้อยละ 61.9 วิเคราะห์ว่า เห็นได้ชัดว่า การเข้ารับการฝึกอบรม จะมีอัตราในการเสี่ยงเรื่องนี้อยู่น้อยมาก เพราะข้าราชการได้ผ่านการฝึกอบรม ด้าน กฎหมาย ระเบียบ ข้อบังคับมาแล้ว จึงทำให้เกิด มีความรู้ในเรื่องนี้อยู่บ้าง ผิดจากบุคคลที่ไม่ได้เข้ารับการอบรม จะไม่มีโอกาสที่จะได้รับรู้เรื่องดังกล่าว ถ้าไม่สนใจเพราะบุคคล ก็จะไม่ค้นหา ความรู้ หรือรอบรู้ได้ ถ้าไม่มีการฝึกอบรม ชี้แนะ ให้เห็นถึงภัยคุกคามต่าง ๆ

5.1.5 ส่วนที่ 5 ข้อเสนอแนะต่าง ๆ ที่ผู้ตอบแบบสอบถามได้ให้ข้อเสนอแนะไว้

ผลการวิเคราะห์พบว่า ส่วนใหญ่ไม่ตอบแบบสอบถามในข้อนี้ มีเพียงข้าราชการบ้างคนเท่านั้นที่ให้ข้อมูลในส่วนนี้ ส่วนมากจะเป็นว่าให้เปิดการอบรมออกกฎระเบียบมาใช้ ให้กำลังพลทราบ ส่วนที่ไม่ตอบคำถามในส่วนนี้วิเคราะห์ว่า ไม่มีเวลาให้ในการตอบแบบสอบถาม เร่งรีบที่จะตอบแบบสอบถาม ไม่รู้ว่าจะเสนอแนะอะไรดีก็จะว่างไว้

5.2 ข้อเสนอแนะ

เนื่องจากผลการวิเคราะห์ที่ผ่านมาส่วนใหญ่ข้าราชการ ใน กองบัญชาการกองทัพไทย เป็นเพียงผู้ใช้งานอย่างเดียว ขาดความรู้เรื่องการดูแลรักษาคอมพิวเตอร์และขาดการเอาใจใส่ต่อภัยคุกคาม อีกเป็นจำนวนมาก ด้วยการทำงานเฉพาะหน้าที่ตำแหน่งการทำงาน จึงมุ่งเน้นงานให้ผลสัมฤทธิ์ตามคำสั่งผู้บังคับบัญชา คอมพิวเตอร์เป็นของสำนักงาน มีผู้ใช้งานร่วมกัน จึงไม่คิดที่จะใส่ใจดูแลดีพอเหมือนกับคอมพิวเตอร์ส่วนตัว การระวังป้องกันภัย จึงทำได้น้อย นอกเสียจาก จะเป็นงานลับเฉพาะที่ไม่ต้องการให้ผู้อื่นล่วงรู้ ก็จะจัดการกับข้อมูลได้เป็นอย่างดี ข้าราชการ ใน กองบัญชาการกองทัพไทย อีกจำนวนมาก ที่ยังขาดการเข้ารับการฝึกอบรม หลักสูตรการรักษาความมั่นคงปลอดภัยสารสนเทศ ของ กองบัญชาการกองทัพไทย เนื่องจากเหตุเรื่องงบประมาณ การฝึกอบรม มีเพียงปีละครั้ง และจำกัดด้วยอัตราการเข้ารับการฝึกอบรม จึงทำ

ให้ผู้ที่เข้ารับการฝึกอบรมส่วนใหญ่ เป็นข้าราชการสัญญาบัตร และเจ้าหน้าที่ที่เกี่ยวข้อง เป็นผู้แทนของหน่วยเข้ารับการฝึกอบรมเท่านั้น ข้าราชการที่เป็นเพียงผู้ใช้งานคอมพิวเตอร์ในเครือข่ายเพียงอย่างเดียว จึงไม่มีความรู้และตระหนักในเรื่องภัยคุกคามดังกล่าว นอกเสียจากข้าราชการที่มีความรู้ความสนใจด้านคอมพิวเตอร์ จากการค้นคว้าหาความรู้เพิ่มเติมจากที่เรียน หรือจากข้อมูลข่าวสารทั่วไป

ข้อควรเน้นในการจัดการฝึกอบรม เรื่องการสอนเข้ารหัสเพื่อการรักษาความปลอดภัย เรื่องการ Backup ข้อมูล ขั้นตอนทำอย่างไร ผลดีผลเสียของการไม่ Backup ข้อมูล เป็นอย่างไร เรื่องการแชร์ข้อมูลกันผ่านในระบบเครือข่าย การตั้งค่าการแชร์ที่ถูกต้อง ผลเสียของการแชร์ข้อมูลผ่านระบบเครือข่าย เรื่องการให้ความรู้โปรแกรม Antivirus ที่ กองบัญชาการกองทัพไทย จัดให้มีวิธีการใช้งานอย่างไร ลักษณะของการทำงานโปรแกรม Antivirus เพื่อให้เกิดความมั่นใจกับผู้ใช้จะได้ไม่ใช้โปรแกรม Antivirus ชนิดอื่น ที่ทางราชการกำหนด ให้ความรู้เกี่ยวกับ ชนิดของภัยคุกคามที่แอบแฝงเข้ามา การตรวจค้นพบ บ่อยที่สุด สาเหตุเกิดจากอะไร เรื่องกฎหมาย พรบ. คอมพิวเตอร์เบื้องต้น ควรเน้นความง่าย ต่อการจดจำของผู้เข้าร่วมฝึกอบรมรวมทั้ง กฎระเบียบนโยบายต่าง ๆ เป็นพิเศษ

จึงเห็นควรให้ทุกหน่วยจัดข้าราชการเจ้าหน้าที่ที่เกี่ยวข้อง เป็นตัวแทน เข้ารับการฝึกอบรม หลักสูตร การรักษาความมั่นคงปลอดภัยสารสนเทศ ของ กองบัญชาการกองทัพไทย ให้มีระดับความรู้ความสามารถที่จะปกป้องภัยอันตรายจากภัยคุกคามที่จะเกิดขึ้นได้กับข้อมูลของทางราชการ และสามารถถ่ายทอดได้ นำความรู้ที่ได้ไปจัดการฝึกอบรมยังหน่วยงานของตนเอง เพื่อให้เพื่อนข้าราชการได้รับรู้ถึงอันตรายต่าง ๆ จากภัยคุกคาม ที่อาจเกิดขึ้นในระบบเครือข่าย ภายในกองบัญชาการกองทัพไทย ได้ หลักจากผ่านการฝึกอบรมมาแล้วจัดให้มีการฝึกอบรมภายในหน่วยงานของตนเอง แล้วรายงานผลการจัดฝึกอบรมภายในหน่วย กลับมายัง กรมการสื่อสารทหาร ซึ่งเป็นหน่วยงานรับผิดชอบดูแล เรื่องการจัดการฝึกอบรม หลักสูตร การรักษาความมั่นคงปลอดภัยสารสนเทศ ของ กองบัญชาการกองทัพไทย เพื่อที่จะได้รายงานผลการจัดการฝึกอบรม นำเรียนผู้บัญชาการทหารสูงสุด รับทราบข้อมูลต่อไป และเห็นควรสอดแทรกลงไปในหลักสูตรต่าง ๆ ที่ทางราชการจัดให้มีการฝึกอบรมเกี่ยวกับการรักษาความมั่นคงปลอดภัยต่าง ๆ และงานในด้านสารบรรณ

บรรณานุกรม

บรรณานุกรม

ภาษาไทย

ธานินทร์ ศิลป์จารุ. (2555). *การวิจัยและวิเคราะห์ข้อมูลทางสถิติด้วย SPSS และ AMOS* (พิมพ์ครั้งที่ 13). กรุงเทพฯ : บิสซิเนสอาร์แอนด์ดี.

นวรัตน์ พัฒโนทัย. (2555). *ความรู้ความเข้าใจในความปลอดภัยของข้อมูล ส่วนบุคคลทางระบบคอมพิวเตอร์ กรณีศึกษาในเขต กรุงเทพมหานคร* (สารนิพนธ์ปริญญามหาบัณฑิต). กรุงเทพฯ : มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี.

ปิยะนาถ คล่องดี. (2556). *การวิเคราะห์ความคุ้มทุนและประโยชน์ที่ชุมชมได้รับในการจัดตั้งศูนย์การเรียนรู้ ICT ชุมชน กรณีศึกษา ศูนย์การเรียนรู้ ICT ชุมชน ตำบลบางเพรียง อำเภอบางบ่อ จังหวัดสมุทรปราการ* (สารนิพนธ์ปริญญามหาบัณฑิต). กรุงเทพ ฯ : มหาวิทยาลัยธุรกิจบัณฑิตย์.

วรรณษา บุนนาค. (2554). *การใช้ประโยชน์และความพึงพอใจต่อระบบอินทราเน็ตเพื่อการสื่อสารภายในองค์กร กรณีศึกษา ข้าราชการโรงพยาบาลพระมงกุฎเกล้า* (สารนิพนธ์ปริญญามหาบัณฑิต). กรุงเทพ ฯ : มหาวิทยาลัยธุรกิจบัณฑิตย์.

ศิริพงศ์ ศรีสุขกาญจน์. (2553). *ความรู้ ทัศนคติต่อพฤติกรรมด้านความปลอดภัยของพนักงานอู่ทหารเรือ พระจุลจอมเกล้า กรมอู่ทหารเรือ กรณีศึกษา ในสายงานฝ่ายผลิต* (วิทยานิพนธ์ปริญญามหาบัณฑิต). กรุงเทพ ฯ : มหาวิทยาลัยธุรกิจบัณฑิตย์.

สุพรรษา เกษสีแก้ว. (2552). *พฤติกรรมการใช้สังคมออนไลน์เวลาจริงของนักศึกษาปริญญาตรี มหาวิทยาลัยธุรกิจบัณฑิตย์* (สารนิพนธ์ปริญญามหาบัณฑิต). กรุงเทพ ฯ : มหาวิทยาลัยธุรกิจบัณฑิตย์.

สารสนเทศจากสื่ออิเล็กทรอนิกส์

เศรษฐพงศ์ มะลิสุวรรณ. (2552). *ภัยคุกคามความมั่นคงระบบสารสนเทศ.*
สืบค้นวันที่ 4 กุมภาพันธ์ 2557,
จาก www.pi.ac.th/up_news/139c3cComputer_safty.pdf

ความมั่นคงปลอดภัยของสารสนเทศ ของคณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยฟาร์อิสเทอร์น.
สืบค้นวันที่ 7 กุมภาพันธ์ 2557, จาก http://sci.feu.ac.th/boonrit/security/

ภัยคุกคาม ช่องโหว่ และการโจมตี ของ มหาวิทยาลัยฟาร์อิสเทอร์น. สืบค้นวันที่ 7 กุมภาพันธ์ 2557,
จาก http://sci.feu.ac.th/boonrit/security/

ภาคผนวก

ภาคผนวก ก

แบบสอบถาม ความรู้ ความเข้าใจ การรักษาความมั่นคงปลอดภัยสารสนเทศ

แบบสอบถามความรู้ความเข้าใจการรักษาความมั่นคงปลอดภัยสารสนเทศ

กระผม จ.ส.อ.ศรวัสย์ สนธิ นักศึกษา มหาวิทยาลัยธุรกิจบัณฑิตย์ จึงใคร่ขอความร่วมมือ ตอบแบบสอบถาม เกี่ยวกับ ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของ กองบัญชาการกองทัพไทย เพื่อเป็นข้อมูลในการทำวิจัยสารนิพนธ์ ทั้งนี้ข้อมูลที่ได้จากการตอบแบบสอบถามในงานวิจัยนี้อาจเป็นประโยชน์แก่ผู้ศึกษาค้นคว้าต่อไปได้

<u>ส่วนที่ 1</u> ข้อมูลส่วนบุคคลทั่วไป

คำชี้แจง โปรดทำเครื่องหมาย ✓ ลงใน ❒ หรือเติมข้อความลงในช่องว่างตรงตามความเป็นจริง

1. เพศ

❒ 1. ชาย ❒ 2. หญิง

2. อายุ

❒ 1. ต่ำกว่า 20 ปี ❒ 2. ตั้งแต่ 21 ปี ถึง 30 ปี

❒ 3. ตั้งแต่ 31 ปี ถึง 40 ปี ❒ 4. ตั้งแต่ 41 ปี ถึง 50 ปี

❒ 5. ตั้งแต่ 51 ปี ขึ้นไป

3. ระดับการศึกษา

❒ 1. ระดับมัธยมศึกษาตอนต้น ❒ 2. ระดับมัธยมศึกษาตอนปลาย

❒ 3. ระดับประกาศนียบัตรวิชาชีพ ❒ 4. ระดับประกาศนียบัตรวิชาชีพชั้นสูง

❒ 5. ระดับปริญญาตรี ❒ 6. ระดับปริญญาโทขึ้นไป

4. ระดับหน้าที่ทำงาน

❒ 1. ระดับข้าราชการชั้นสัญญาบัตร ❒ 2. ระดับข้าราชการชั้นประทวน

❒ 3. ระดับข้าราชการลูกจ้างพนักงานราชการ

5. เคยได้รับการฝึกอบรม หลักสูตร การรักษาความมั่นคงปลอดภัยสารสนเทศ หรือไม่

❒ 1. เคยผ่านหลักสูตร ❒ 2. ไม่เคยผ่านหลักสูตร

<u>ส่วนที่ 2</u> พฤติกรรมการใช้ระบบอินทราเน็ตและอินเตอร์เน็ตภายในองค์กร

คำชี้แจง โปรดทำเครื่องหมาย ✓ ลงใน ❒ หรือเติมข้อความลงในช่องว่างตรงตามความเป็นจริง

1. ปัจจุบันท่านใช้คอมพิวเตอร์สำนักงานหรือของส่วนตัว

❒ สำนักงาน ❒ ส่วนตัว

2. คอมพิวเตอร์ของท่านมีคนอื่นใช้นอกจากท่านหรือไม่

❒ ใช้ ❒ ไม่ใช้

3. ท่านเคยนำอุปกรณ์สื่อสารชนิดอื่นๆ มาเชื่อมต่อในเครือข่าย กองบัญชาการกองทัพไทย หรือไม่ และเป็นอุปกรณ์ชนิดใด

❒ เคยนำเชื่อมต่อ อุปกรณ์ชนิด ..... ❒ ไม่เคยเชื่อมต่อ

4. ท่านใช้คอมพิวเตอร์ในการทำงานระบบอินทราเน็ตและอินเตอร์เน็ตใน กองบัญชาการกองทัพไทย ในเรื่องใดบ้าง (ตอบได้มากกว่า 1 ข้อ)

❒ 1. พิมพ์งานเอกสาร ❒ 2. จัดเก็บข้อมูล
❒ 3. ดูหนังฟังเพลง ❒ 4. Download ข้อมูล
❒ 5. ค้นหาข้อมูล ❒ 6. ใช้ Email
❒ 7. ท่องเว็บไซต์ ❒ 8. อ่านข่าวสาร
❒ 9. Social Network ❒ 10. เล่น Game
❒ 11. ซื้อขาย online ผ่านInternet ❒ 12. อื่นๆ ระบุ .....

<u>ส่วนที่ 3</u> แบบทดสอบความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ

คำชี้แจง โปรดทำเครื่องหมาย ✓ ลงใน ❒ หรือเติมข้อความลงในช่องว่างตรงตามความเป็นจริง

3.1 แบบทดสอบความรู้การรักษาความปลอดภัยสารสนเทศเกี่ยวกับข้อมูล

1) คอมพิวเตอร์ที่ดีควรเข้ารหัสเพื่อป้องกันผู้อื่นอย่างไร

❒ มั่นตั้งรหัสอย่างน้อย 8 ตัวอักษร ทั้งตัวหนังสือและตัวเลข
❒ ตั้งรหัสที่ง่ายต่อการจำของตัวเอง
❒ ตั้งรหัสและจดบันทึกเอาไว้

2) มาตรฐานเกี่ยวข้องกับการบริหารการ รักษาความปลอดภัยข้อมูล และเป็นแนวทางในการสร้าง ดูแล และปรับปรุงระบบบริหารการรักษาความปลอดภัยคือ ISO/IEC

❒ ISO/IEC 17025
❒ ISO/IEC 27001
❒ ISO/IEC 20000

3) ข้อมูลทางคอมพิวเตอร์ในปัจจุบันของท่านถูกจัดเก็บอย่างไร

❒ จัดเก็บเป็นระเบียบ แยกหมวดหมู่ ง่ายต่อการค้นหา
❒ ไม่ได้จัดเก็บเป็นระเบียบข้อมูลจัดวางไว้หน้า Desktop
❒ จัดเก็บไว้ในที่อื่น ๆ .....

4) เมื่อคอมพิวเตอร์ของท่านเสียมีการส่งซ่อมควรทำอย่างไร

❒ Backup Data และลบข้อมูลออกก่อนส่งซ่อม
❒ ส่งซ่อมกับเจ้าหน้าที่ซ่อมบำรุง
❒ ส่งซ่อมกับช่างผู้ชำนาญตามร้านเอง

5) ท่านตั้งแชร์ข้อมูลผ่ายระบบเครือข่ายอย่างไร

❒ แบบ Full อ่านและเขียนได้ ❒ แบบ อ่านได้อย่างเดียว
❒ แบบ อ่านได้อย่างเดียวและตั้งรหัสในการแชร์ข้อมูล

3.2 แบบทดสอบความรู้การรักษาความปลอดภัยสารสนเทศเกี่ยวกับการป้องกัน Virus และช่องโหว่ด้านต่าง ๆ

1) คอมพิวเตอร์ของท่านมี โปรแกรม Antivirus ที่เจ้าหน้าที่ติดตั้งของอะไร

- ❒ Nod32 Antivirus
- ❒ AVG Antivirus
- ❒ McAfee Antivirus
- ❒ AVIRA Antivirus
- ❒ อื่น ๆ ระบุ .....

2) เมื่อท่านนำ Flash drive ไป Save งานแล้วนำมาเปิดที่เครื่องของท่านควรปฏิบัติอย่างไร

- ❒ Scan Virus ก่อนเปิดทุกครั้ง
- ❒ เสียบแล้วเปิดทันที
- ❒ นำไปเสียบเครื่องอื่นก่อน เพื่อให้มั่นใจว่าไม่มี Virus
- ❒ ถามเจ้าของ Flash drive หรือ เครื่องคอมพิวเตอร์ที่นำไม่ Save งานว่ามีหรือไม่ เพื่อมั่นใจ ก่อนเปิดงานทันที

3) มัลแวร์ (Malware) คืออะไร

- ❒ โปรแกรมคอมพิวเตอร์ทุกชนิดที่มีจุดประสงค์ร้ายต่อคอมพิวเตอร์
- ❒ โปรแกรมคอมพิวเตอร์ประเภทหนึ่งที่ถูกออกแบบมาให้แพร่กระจาย
- ❒ โปรแกรมที่สามารถคัดลอกตัวเองและสามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆ
- ❒ โปรแกรมที่ทำลายระบบคอมพิวเตอร์โดยแฝงมากับโปรแกรมอื่น ๆ

4) Backdoor คืออะไร

- ❒ รูรั่วในการรักษาความปลอดภัยของระบบคอมพิวเตอร์ที่ผู้ออกแบบหรือผู้ดูแลจงใจทิ้งไว
- ❒ ซอฟต์แวร์ที่ออกแบบเพื่อสร้างความสนุกสนาน แต่ก็ทาให้เสียเวลาการทำงานของระบบคอมพิวเตอร์
- ❒ พยายามหลอกล่อให้เหยื่อจ่ายเงินหรือโอนเงิน และมีเทคนิคหลอกลวงที่สมบูรณ์แบบ
- ❒ ประตูหลังของช่องทางที่ให้ Virus เข้าไปโจมตีทำให้คอมเสียหาย

5) สปายแวร์ (Spyware) คืออะไร

- ❒ โปรแกรมคอมพิวเตอร์ประเภทหนึ่งที่ถูกออกแบบมาให้แพร่กระจาย
- ❒ โปรแกรมที่ใช้บางอย่างเพื่อลวงตาแต่ทากิจกรรมบางอย่างในเครื่องคอมพิวเตอร์
- ❒ โปรแกรมที่ทำลายระบบคอมพิวเตอร์โดยแฝงมากับโปรแกรมอื่น ๆ
- ❒ โปรแกรมคอมพิวเตอร์ทุกชนิดที่มีจุดประสงค์ร้ายต่อคอมพิวเตอร์

3.3 แบบทดสอบความรู้การรักษาความปลอดภัยสารสนเทศเกี่ยวกับด้านกฎหมาย ว่าด้วย การกระทำผิด พรบ. เกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 นโยบาย และระเบียบ ของกองบัญชาการกองทัพไทย เกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ

1) พรบ. คอมพิวเตอร์ พ.ศ.2550 มีทั้งหมดกี่หมวด

❒ 1 หมวด ❒ 2 หมวด

❒ 3 หมวด ❒ 4 หมวด

2) ผู้ใดเข้าโดยมิชอบ ซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง ต้องโทษอย่างไร

❒ จำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

❒ จำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

❒ จำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

❒ จำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

3) ผู้ใดเข้าโดยมิชอบ ซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง ต้องโทษอย่างไร

❒ จำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

❒ จำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

❒ จำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

❒ จำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

4) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลอันเป็นเท็จ โดยเกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

❒ จำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

❒ จำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

❒ จำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

❒ จำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

5) ระเบียบ กองบัญชาการทหารสูงสุด ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ ของกองทัพไทย ออกใช้เมื่อไร

❒ 14 ก.พ.2547

❒ 23 ก.พ.2547

❒ 10 มิ.ย.2550

❒ 24 มี.ค.2552

<u>ส่วนที่ 4</u> แบบทดสอบพฤติกรรมเสี่ยงต่อภัยคุกคามต่อเครือข่ายภายใน กองบัญชาการกองทัพไทย

คำชี้แจง โปรดทำเครื่องหมาย ✓ เลือกคำตอบตรงตามความเป็นจริง

ลำดับ	ความรู้ความเข้าใจการรักษาความมั่นคงปลอดภัยสารสนเทศ	การปฏิบัติ	
		เคย	ไม่เคย
1.	ท่านเคยจดบันทึกรหัสผ่านเพื่อง่ายต่อการจดจำใกล้บริเวณโต๊ะคอมพิวเตอร์หรือไม่		
2.	ท่านเคย Backupไฟล์ข้อมูลอยู่อย่างสม่ำเสมอหรือไม่		
3.	ท่านเคยส่งซ่อมคอมพิวเตอร์โดยไม่ Backup ข้อมูลออกก่อน		
4.	ท่านเคยแชร์ไฟล์ข้อมูลที่สำคัญโดยเข้ารหัสหรือไม่		
5.	ท่านเคยแชร์ข้อมูลผ่านเครือข่ายแบบ อ่านได้เขียนได้		
6.	ท่านเคยใช้ Free Email ในเครือข่ายกองบัญชาการกองทัพไทย		
7.	ท่านเคยใช้คอมพิวเตอร์ดาวน์โหลด โปรแกรมฟรีแวร์จากเว็บไซต์อินเตอร์เน็ตมาติดตั้งหรือไม่		
8.	ท่านเคยศึกษานโยบายการป้องกัน Virus บนคอมพิวเตอร์ขององค์กรหรือไม่		
9.	ท่านเคยนำ USB flash drive ไปใช้กับคอมพิวเตอร์ ที่ไม่มีระบบป้องกัน Antivirus		
10.	ท่านเคยศึกษาวิธีป้องกันเกี่ยวกับภัยคุกคามเพื่อป้องกันภัยจากคอมพิวเตอร์ ในระบบสารสนเทศ		

<u>ส่วนที่ 5</u> ความคิดเห็นและข้อเสนอแนะอื่น ๆ เกี่ยวกับเรื่องระบบการรักษาความมั่นคงปลอดภัยสารสนเทศ ของ กองบัญชาการกองทัพไทย

.....

.....

.....

.....

.....

.

ขอขอบคุณสำหรับความร่วมมือมา ณ ที่นี้

ภาคผนวก ข

ระเบียบ กองบัญชาการทหารสูงสุด ว่าด้วยการรักษาความปลอดภัย ระบบสารสนเทศ ของ กองบัญชาการกองทัพไทย พ.ศ.2547

ระเบียบ กองบัญชาการทหารสูงสุด
วาดวยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพไทย
พ.ศ.๒๕๔๗

เพื่อให้การรักษาความปลอดภัยระบบสารสนเทศของกองทัพไทยเป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ จึงวางระเบียบไว้ ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบกองบัญชาการทหารสูงสุด ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพไทย พ.ศ.๒๕๔๗”

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๓ บรรดาระเบียบ และคำสั่งอื่นใดในส่วนที่กำหนดไว้แล้ว ซึ่งขัดหรือแย้งกับระเบียบนี้ให้ใช้ระเบียบนี้แทน

ข้อ ๔ ระเบียบนี้ให้ใช้บังคับแก่ส่วนราชการ ข้าราชการ และลูกจ้างที่มีการปฏิบัติเกี่ยวกับ ระบบสารสนเทศ รวมทั้ง บุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศของ กองบัญชาการทหารสูงสุด และเหล่าทัพ

ข้อ ๕ ในระเบียบนี้

๕.๑ ระบบสารสนเทศ (Information System) หมายความว่า ระบบข่าวสารของ กองทัพไทย ที่นำเอาเทคโนโลยีของระบบคอมพิวเตอร์ และระบบสื่อสาร มาช่วยในการสร้างสารสนเทศ ของกองทัพไทย และสามารถนำข่าวสารมาใช้ในการวางแผน การบริหาร การพัฒนาและควบคุมซึ่งมีองค์ประกอบดังนี้

๕.๑.๑ ระบบคอมพิวเตอร์ (Computer System) หมายถึง ระบบที่ประกอบด้วยฮาร์ดแวร์ (Hardware) ซอฟตแวร์ (Software) และบุคลากรทางคอมพิวเตอร์ (Peopleware)

๕.๑.๒ ระบบสื่อสาร (Communication System) หมายความว่า ระบบที่ประกอบด้วยผู้รับ ผู้ส่งและสื่อกลางในระบบสื่อสารที่ใช้ในการส่งผ่านข้อมูล ทั้งระบบวงจรทางสาย และระบบไร้สาย รวมถึงอุปกรณ์ต่อพวงอื่น ๆ เช่น Hub, Switching, Router เป็นต้น

๕.๑.๓ สารสนเทศ (Information) ข้อเท็จจริงที่ได้จากการสกัดข้อมูลให้มีความหมายโดยผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของ ตัวเลข ข้อความหรือ

/ภาพกราฟฟิก ...

ภาพกราฟฟิกที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

๕.๒ เครือข่ายระบบสารสนเทศ หมายความว่า การติดต่อสื่อสาร หรือการส่งข้อมูลกันระหว่างระบบสารสนเทศภายใน บก.ทหารสูงสุด, เหล่าทัพ และการติดต่อสื่อสาร หรือการส่งข้อมูลกันระหว่าง เหล่าทัพ กับ บก.ทหารสูงสุด

ข้อ ๖ ให้ เจ้ากรมการสนเทศทหาร กองบัญชาการทหารสูงสุด เป็นผู้รักษาการให้เป็นไปตามระเบียบนี้

หมวด ๑

กล่าวทั่วไป

ข้อ ๗ ความมุ่งหมายของระเบียบนี้

๗.๑ เพื่อกำหนดหลักการและมาตรการในการรักษาความปลอดภัยระบบสารสนเทศ ของ กองทัพไทย

๗.๒ พิทักษ์รักษาและป้องกัน มิให้ข้อมูลและสิ่งที่เป็นความลับของทางราชการรั่วไหลหรือรู้ไปถึง หรือตกไปอยู่ในมือของฝ่ายตรงข้ามหรือบุคคลผู้ไม่มีอำนาจหน้าที่

๗.๓ ป้องกันการจารกรรมทั้งจากบุคคลภายในและภายนอกส่วนราชการ

๗.๔ พิทักษ์รักษาและป้องกันการก่อวินาศกรรมแก่เครื่องจักรคำนวณ อุปกรณ์เครื่องใช้ อาคาร สถานที่ และเอกสาร เป็นต้น

ข้อ ๘ หัวหน้าส่วนราชการสามารถกำหนดมาตรการรักษาความปลอดภัยให้ระบบสารสนเทศของส่วนราชการ และแต่งตั้งเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยระบบสารสนเทศของส่วนราชการเพิ่มเติมได้โดยให้สอดคล้องและไม่ขัด หรือแย้งกับระเบียบนี้

ข้อ ๙ เหตุผลในการประกาศใช้ระเบียบนี้ คือ วางระเบียบกองบัญชาการทหารสูงสุดในการรักษาความปลอดภัยระบบสารสนเทศของ กองทัพไทย เกี่ยวกับระบบคอมพิวเตอร์, ระบบสื่อสาร, สารสนเทศเครือข่ายระบบสารสนเทศ เพื่อให้ใช้บังคับแก่ส่วนราชการ ข้าราชการและลูกจ้าง ที่มีการปฏิบัติเกี่ยวกับระบบสารสนเทศ รวมทั้งบุคคลภายนอก ที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศ ของ กองบัญชาการทหารสูงสุด และเหล่าทัพ

ข้อ ๑๐ ในการกำหนดชั้นความลับของสารสนเทศให้เป็นไปตาม พรบ. ข้อมูลข่าวสารของทางราชการ พ.ศ.๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ หรืออื่น ๆ ที่ได้ประกาศใช้ทดแทน

/หมวด ๒ ...

หมวด ๒

การรักษาความปลอดภัยเกี่ยวกับบุคคล

ข้อ ๑๑ ความมุ่งหมาย เพื่อเป็นการคัดเลือด ให้ได้บุคคลที่มีลักษณะเหมาะสมแก่การบรรจุใน อัตราที่เกี่ยวกับการปฏิบัติหน้าที่ที่ระบบสารสนเทศ และเพื่อกำหนดระดับความไว้วางใจในการมอบหมายหน้าที่เกี่ยวกับความลับของทางราชการ ตลอดจนควบคุมบุคคลที่ไม่เกี่ยวข้องและหรือบุคคลภายนอกที่เข้ามาเกี่ยวข้องกับระบบสารสนเทศ

ข้อ ๑๒ บุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศ ให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๗ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔

ข้อ ๑๓ หัวหน้าส่วนราชการ จะต้องจัดให้มีการควบคุม ดูแล และตรวจสอบสิทธิ์การเข้าถึงระบบสารสนเทศอย่างเข็มงวด โดยคำนึงถึงความปลอดภัยของระบบสารสนเทศเป็นหลัก

หมวด ๓

การรักษาความปลอดภัย สถานที่

ข้อ ๑๔ การรักษาความปลอดภัยเกี่ยวกับสถานที่ของระบบสารสนเทศให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๗ โดย

๑๔.๑ ส่วนราชการกำหนดมาตรการรักษาความปลอดภัยสถานที่จากการเข้าถึงโดยการได้ยิน และการมองเห็นของผู้ไม่มีอำนาจหน้าที่

๑๔.๒ ส่วนราชการกำหนดพื้นที่รักษาความปลอดภัยแบ่งเขตหวงห้ามเฉพาะเขตหวงห้ามเด็ดขาด ให้เหมาะสม

ข้อ ๑๕ ส่วนราชการจะต้องจัดทำแผนสำหรับเตรียมรับสถานการณ์ต่าง ๆ ได้แก่ แผนป้องกันระบบสารสนเทศ แผนการดำเนินการฟื้นฟูระบบคอมพิวเตอร์ แผนการเคลื่อนย้ายและแผนการทำลายระบบสารสนเทศในเวลาจำเป็นให้พร้อมที่จะปฏิบัติหน้าที่ได้ทันท่วงที และจัดให้มีการซักซ้อมความเข้าใจอย่างสม่ำเสมอ

ข้อ ๑๖ ส่วนราชการควรจัดให้มีสถานที่สำรองในการดำเนินการระบบสารสนเทศ

หมวด ๔

การรักษาความปลอดภัยระบบสารสนเทศ

ข้อ ๑๗ ส่วนราชการจะต้องจัดให้มีมาตรการรักษาความปลอดภัยระบบสารสนเทศที่เหมาะสม และดำเนินการตามมาตรการนั้นโดยเคร่งครัด เพื่อให้เกิดความปลอดภัยสูงสุดต่อระบบสารสนเทศ

/ข้อ ๑๘ ...

ข้อ ๑๘ ส่วนราชการต้องจัดทำระบบสำรองและการกู้คืนสภาพข้อมูลสารสนเทศตามวงรอบที่เหมาะสมและทันสมัยที่สุด

ข้อ ๑๙ ส่วนราชการต้องจัดให้มีแผนการสำรองและแผนการกู้คืนสภาพระบบสารสนเทศและทดสอบอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒๐ ต้องจัดให้มีแผนการรักษาและป้องกันความลับของข้อมูล

๒๐.๑ ต้องไม่เข้าถึงข้อมูลผู้อื่น โดยไม่ได้รับอนุญาตจากเจ้าของข้อมูล

๒๐.๒ ห้ามทำการพิมพ์หรือทำสำเนาข้อมูลที่เป็นชั้นความลับ เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๒๐.๓ ต้องมีการกำหนดผู้รับผิดชอบอุปกรณ์คอมพิวเตอร์ในระบบสารสนเทศของหน่วย

ข้อ ๒๑ การรักษาความปลอดภัยเกี่ยวกับเครือข่ายคอมพิวเตอร์

๒๑.๑ ส่วนราชการเจ้าของเรื่องสารสนเทศในเครือข่ายระบบสารสนเทศ ผู้มีสิทธิ์และอำนาจในสายงาน ที่มีการติดต่อแลกเปลี่ยนสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์เป็นผู้พิจารณาคุณสมบัติของผู้ใช้ที่ได้รับอนุญาตให้เข้าถึงและดำเนินการกับสารสนเทศดังกล่าว รวมทั้งพิจารณาระดับการป้องกันที่ต้องการ

๒๑.๒ การส่งข้อมูลที่มีชั้นความลับผ่านเครือข่ายคอมพิวเตอร์ จะต้องได้รับอนุมัติจากผู้มีสิทธิ์และอำนาจในสายงานที่กำหนดชั้นความลับนั้นก่อน แล้วจึงส่งเข้ารหัสตามมาตรฐานที่ได้รับการรับรองจากส่วนราชการ

ข้อ ๒๒ ส่วนราชการเจ้าของเรื่องสารสนเทศในเครือข่ายระบบสารสนเทศ ผู้มีสิทธิ์และอำนาจในสายงานสามารกำหนดระเบียบปฏิบัติของการเข้าใช้ที่สอดคล้องกับระเบียบนี้

ข้อ ๒๓ ส่วนราชการต้องจัดให้มีการรักษาความปลอดภัยฐานข้อมูล

เพื่อกำหนดมาตรการป้องกันฐานข้อมูลจากการเข้าถึง การเปลี่ยนแปลง การโอนถ่ายข้อมูล หรือการกระทำใด ๆ โดยผู้ไม่เกี่ยวข้อง โดย

๒๓.๑ ข้อมูล ข่าวสาร สารสนเทศทุกประเภท ในฐานข้อมูลต้องได้รับการจัดระดับ การป้องกัน ผู้มีสิทธิ์เข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่น ๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย

๒๓.๒ ส่วนราชการเจ้าของฐานข้อมูล ผู้มีสิทธิ์และอำนาจในสายงาน เป็นผู้พิจารณาคุณสมบัติของผู้ใช้และโปรแกรมที่ได้รับอนุญาตให้กระทำการใด ๆ กับข้อมูลนั้นได้ตามสิทธิ์ และจัดให้มีแฟ้มลงบันทึกเข้าออก (Log File) การใช้งานสำหรับฐานข้อมูลตามความจำเป็นเพื่อประโยชน์ในการตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

/ ๒๓.๓ ในกรณี ...

๒๓.๓ ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างราชการให้จัดทำข้อตกลงการใช้

๒๓.๔ ต้องจัดให้มีแผนการป้องกันไวรัสคอมพิวเตอร์เพื่อป้องกันฐานข้อมูลถูกทำลายโดย

๒๓.๔.๑ ห้ามเจ้าหน้าที่นำคอมพิวเตอร์ซอฟต์แวร์ หรือข้อมูลที่ไม่มั่นใจว่าติดไวรัสคอมพิวเตอร์มาติดตั้ง หรือใช้งาน เว้นแต่คอมพิวเตอร์ซอฟแวร์นั้น ได้ผ่านการตรวจสอบจากเจ้าหน้าที่ความคุมการรักษาความปลอดภัยระบบสารสนเทศของส่วนราชการก่อน

๒๓.๔.๒ ห้ามเจ้าหน้าที่ปรับแต่ง หรือยกเลิก การทำงานของคอมพิวเตอร์ซอฟต์แวร์ป้องกันไวรัสที่ติดตั้งใช้งานในเครื่องคอมพิวเตอร์ตามที่เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยระบบสารสนเทศของส่วนราชการจัดหามาให้

๒๓.๔.๓ กรณีที่มีการเชื่อมต่อกับระบบอินเตอร์เน็ต จะต้องจัดให้มีแผนการใช้งานคอมพิวเตอร์ ในระบบอินเตอร์เน็ต โดยคำนึงถึงความปลอดภัยของระบบสารสนเทศเป็นหลัก

ข้อ ๒๔ ส่วนราชการจะต้องจัดทำเอกสารประกอบระบบสารสนเทศให้สมบูรณ์ครบถ้วนในทุกด้าน เพื่อความสะดวกในการปรับปรุง แก้ไข และพัฒนาระบบใหม่ เมื่อมีความจำเป็น

หมวด ๕

การรักษาความปลอดภัยในการพัฒนาระบบสารสนเทศ

ข้อ ๒๕ ในการพัฒนาระบบสารสนเทศ ส่วนราชการจะต้องมีมาตรการที่เหมาะสม ในการรักษาความปลอดภัย ต่องานที่กำลังพัฒนา

ข้อ ๒๖ เมื่อพัฒนาระบบสารสนเทศแล้ว จะต้องจัดให้มีการทดสอบระบบสารสนเทศที่พัฒนาขึ้นมาอย่างละเอียดถี่ถ้วน โดยทดสอบในระบบที่แยกต่างหากจากระบบที่มีอยู่เดิมจนกว่าจะเกิดความมั่นใจในการใช้งาน จึงนำมาใช้งานจริงร่วมกัน หรือทดแทนระบบที่มีอยู่เดิม

ข้อ ๒๗ บุคคลภายนอกที่เข้ามาพัฒนาระบบสารสนเทศ ให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๗ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ โดยเคร่งครัด

/ หมวด ๖ ...

หมวด ๖

การปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ

ข้อ ๒๘ ความมุ่งหมาย เพื่อให้ทราบถึงสาเหตุแห่งการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ การปฏิบัติของเจ้าหน้าที่ และความรับผิดชอบของผู้บังคับบัญชาเมื่อปรากฏการละเมิด

ข้อ ๒๙ สาเหตุแห่งการละเมิดการรักษาความปลอดภัย

การละเมิดการรักษาความปลอดภัยอันเป็นเหตุให้ความลับของทางราชการรั่วไหล เครื่องจักรคำนวณ อุปกรณ์วัสดุ และสถานที่ ถูกทำลาย หรือข้อมูลถูกลบล้าง แก้ไข จนเกิดความเสียหายขึ้น มีสาเหตุจากการขาดจิตสำนึกและวินัยในการรักษาความปลอดภัย ประมาทเลินเล่อเกียจคร้าน ไม่เคร่งครัดต่อหน้าที่ หรือเห็นแก่ประโยชน์ส่วนตัว รวมถึงการจารกรรมและการก่อวินาศกรรมอันเกิดจากการกระทำของบุคคลภายนอก หรือข้าราชการที่ตกเป็นเครื่องมือของฝ่ายตรงข้าม

ข้อ ๓๐ การปฏิบัติเพื่อปรากฏการละเมิดการรักษาความปลอดภัย

๓๐.๑ ผู้ใดตรวจพบหรือทราบว่ามีการละเมิด หรือสงสัยว่าจะมีการละเมิดการรักษาความปลอดภัยเกิดขึ้น ต้องรีบรายงานผู้บังคับบัญชา หรือเจ้าหน้าที่ควบคุมการรักษาความปลอดภัย หรือเจ้าหน้าที่ผู้รับผิดชอบ

๓๐.๒ เมื่อปรากฏว่าการละเมิดการรักษาความปลอดภัยได้เกิดขึ้นแล้ว เจ้าหน้าที่ที่เกี่ยวข้องหรือเจ้าหน้าที่ควบคุมการรักษาความปลอดภัย ต้องรีบดำเนินการดังนี้

๓๐.๒.๑ รายงานผู้บังคับบัญชา และแจ้ง เจ้ากรมการสนเทศทหาร กองบัญชาการทหารสูงสุด เพื่อให้คำแนะนำช่วยเหลือในเรื่องดังกล่าว

๓๐.๒.๒ สำรวจความเสียหายอันเกิดจากการละเมิดการรักษาความปลอดภัย ค้นหาสาเหตุแห่งการละเมิด ตลอดจนจุดอ่อน ข้อบกพร่อง และความปลอดภัยของเครื่องจักรคำนวณและอุปกรณ์

๓๐.๒.๓ ในกรณีที่ระบบการรหัสของหน่วยสูญหาย หรือสงสัยว่ารั่วไหลให้เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยของหน่วย รายงานด่วนให้ผู้บังคับบัญชาตามลำดับชั้นทราบ โดยเร็วที่สุด และพิจารณานำระบบรหัสสำรองที่เตรียมไว้ใช้แทน

๓๐.๒.๔ หากปรากฏหลักฐานหรือสงสัยว่า ถูกจารกรรม หรือก่อวินาศกรรมให้รายงานผู้บังคับบัญชา ตามลำดับชั้นทราบ เพื่อสั่งการให้เจ้าหน้าที่ผู้มีอำนาจในด้านการสืบสวนและสอบสวนดำเนินการต่อไป

/ ข้อ ๓๑ ...

ข้อ ๓๑ ความรับผิดชอบของผู้บังคับบัญชา

๓๑.๑ แจ้งให้ส่วนราชการเจ้าของเรื่องเดิม หรือเจ้าของข้อมูลที่มีข่ายงานร่วมกันทราบทันที

๓๑.๒ สั่งการสอบสวนหาตัวผู้กระทำผิด และผู้รับผิดชอบโดยเร็วที่สุด

๓๑.๓ พิจารณาแก้ไขข้อบกพร่อง และป้องกันมิให้เหตุการณ์เช่นนี้อุบัติซ้ำอีก

๓๑.๔ พิจารณาสั่งการลงทัณฑ์ หรือดำเนินคดีตามกฎหมายต่อผู้ละเมิด ผู้เกี่ยวข้องกับการละเมิด และผู้รับผิดชอบเมื่อมีการละเมิด หรือไม่ปฏิบัติตามระเบียบนี้ จะโดยเจตนาหรือไม่เจตนาและการละเมิดนั้นจะเกิดความเสียหาย หรือยังไม่เกิดความเสียหายต่อทางราชการก็ตาม

ข้อ ๓๒ ความรับผิดชอบของเจ้าของเรื่องเดิม

เมื่อได้รับแจ้งว่าได้เกิดการละเมิดการรักษาความปลอดภัย ให้ส่วนราชการเจ้าของเรื่องเดิมดำเนินการดังนี้

๓๒.๑ พิจารณาว่าเอกสารกรรมวิธีข้อมูล ประมวลลับ หรือรหัสที่จำเป็นในการใช้วงจรสื่อสารทางสายมีผลกระทบกระเทือนเสียหายอย่างใดหรือไม่

๓๒.๒ ขจัดความเสียหายที่เกิดขึ้นหรือคาดว่าจะเกิดขึ้นจากการละเมิดโดยทันทีในการนี้อาจจะต้องดำเนินการแก้ไขเปลี่ยนแปลงแผนงานและวิธีปฏิบัติ พร้อมทั้งปัจจัยต่าง ๆ ที่เกี่ยวข้องตามที่เห็นควร

ข้อ ๓๓ ในกรณีที่การละเมิดการรักษาความปลอดภัยเกิดผลกระทบกระเทือนเสียหายอย่างร้ายแรงให้อยู่ในดุลพินิจของผู้บังคับบัญชาแก้ไขเปลี่ยนแปลงแผนงานและวิธีปฏิบัติหากจำเป็นให้รายงานหน่วยเหนือตามความเหมาะสม

ข้อ ๓๔ ให้ส่วนราชการที่มีหน่วยกรรมวิธีข้อมูลอัตโนมัติอยู่ในสังกัด ออกระเบียบปลีกย่อยได้ โดยไม่ขัดต่อระเบียบนี้

ประกาศ ณ วันที่ ๒๓ กุมภาพันธ์ ๒๕๔๗

(ลงชื่อ) พลเอก สมทัต อัตตะนันทน์

(สมทัต อัตตะนันทน์)

ผู้บัญชาการทหารสูงสุด

กรมการสนเทศทหาร

ประวัติผู้เขียน

ชื่อ – นามสกุล	จ่าสิบเอก ศรวัสย์ สนธิ
ประวัติการศึกษา	ปีการศึกษา 2548 ปริญญาตรี บริหารธุรกิจบัณฑิต โปรแกรมวิชา การบริหารธุรกิจ แขนงวิชา คอมพิวเตอร์ธุรกิจ มหาวิทยาลัยราชภัฏพระนคร
ตำแหน่งและสถานที่ทำงานปัจจุบัน	ตำแหน่ง เสมียนแผนกธุรการ กองวิชาการทั่วไป ศูนย์ฝึกศึกษา สำนักงานทหารพัฒนา หน่วยบัญชาการทหารพัฒนา กองบัญชาการกองทัพไทย