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