บทคัดย่อ

การศึกษาเรื่อง "การสร้างมาตรฐานการบริหารความปลอดภัยของข้อมูลโดยการประยุกต์ใช้ ISO 17799 กรณีศึกษาของบริษัทผู้ให้บริการด้านการจัดซื้อออนไลน์" มีวัตถุประสงค์ในการนำเสนอความเสี่ยงและภัยคุกคาม ทางด้านข้อมูลและระบบสารสนเทศขององค์กร ที่ได้จากการเก็บข้อมูลทั้งแบบสอบถามและแบบประเมินความคิดเห็นกับบุคคลภายในองค์กร เพื่อนำไปศึกษา วิเคราะห์และจัดหาแนวทางตามมาตรฐานการรักษาความปลอดภัยระดับสากลอย่าง ISO 17799 มาประยุกต์ใช้ให้เหมาะสมกับองค์กรในการควบคุมความเสี่ยงแต่ละด้าน

ผลการศึกษาพบว่าองค์กรตัวอย่างได้ให้ความสำคัญต่อการรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศเป็นอย่างมาก เนื่องจากรูปแบบธุรกิจที่ให้บริการมีความเกี่ยวข้องกับระบบสารสนเทศและการจัดเก็บข้อมูลที่เป็นความลับของลูกค้าอยู่เป็นจำนวนมาก โดยผลจากการวิเคราะห์พบว่าความเสี่ยงที่มีระดับสูงที่พบในองค์กรมีทั้งหมด 7 ภัยคุกคาม ได้แก่ การเก็บรวบรวมข้อมูลสำคัญไว้ที่เดียวกันหมด ,การสูญเสียลูกค้าเนื่องจากระบบไม่สามารถให้บริการได้ , การใช้ชื่อ (User ID)ร่วมกันเพื่อเข้าใช้ข้อมูล ,การพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม ,ผู้บุกรุกสามารถเข้าถึง (Access) เครื่องคอมพิวเตอร์ในองค์กรได้ ,Router / Firewall เสียทำให้ไม่สามารถใช้งานได้ และ ฐานข้อมูล(database)ถูกขัดจังหวะการทำงาน(corrupt)เนื่องจากฮาร์ดแวร์หรือซอฟแวร์อาจทำงานผิดพลาด

ซึ่งการวิเคราะห์ผลนั้นพบว่าทั้ง 7 คุกคาม องค์กรได้ให้ความตระหนักในการป้องกันอยู่ก่อนแล้ว เช่น มีมาตรการในการป้องกันและรักษาความปลอดภัย, จัดทำแผนสำรองกรณีฉุกเฉิน, จัดเตรียมสถานที่ที่เหมาะสม, จัดทำระบบสำรอง เป็นต้น แต่จากการประเมินที่ยังพบความเสี่ยงสูงอยู่ อาจเนื่องมากจากการขาดการประชามสัมพันธ์ให้แก่บุคลากรในองค์กรให้ทั่วถึง ทำให้การรับทราบเกิดเฉพาะในกลุ่มที่ทำงานหรือมีความเกี่ยวข้องกับระบบสารสนเทศโดยตรง

ดังนั้นทางผู้วิจัยจึงได้ทำการทดสอบสมมติฐาน โดยอิงมาตรฐาน ISO 17799 โดยทดสอบความสัมพันธ์ในแต่ละข้อของ ISO 17799 กับ ตัวแปรอิสระคือ หน่วยงานทางด้าน IT กับ Non-IT และจาก ช่วงอายุงานในการทำงานที่องค์กรปัจจุบัน ซึ่งผลส่วนใหญ่แตกต่างกันไปในแต่ละหัวข้อ เพื่อให้ผู้บริหารนำไปประกอบการพิจารณาจัดทำแผนในการพัฒนาหรือให้ความสำคัญตามแต่ละกลุ่มที่แตกต่างกันออกไป