[หน้า 53]

การปฏิบัติตามมาตรฐานการรักษาความปลอดภัย ISO/IEC 17799 ของบริษัทจดทะเบียนในมุมมองของผู้ตรวจสอบสารสนเทศ

ฐิติ วิรทัศนุสรณ์
ดร.มนวิกา ผดุงสิทธิ์

ในปัจจุบัน เทคโนโลยีสารสนเทศได้เข้ามามีบทบาทอย่างมากในการปฏิบัติงานขององค์กร ส่งผลให้กิจกรรมต่างๆ ในห่วงโซ่มูลค่า (Value Chain) มีประสิทธิภาพและประสิทธิผลมากขึ้น เนื่องจากเชื่อมโยงเครือข่ายต่างๆ ทั้งภายในองค์กรและระหว่างองค์กร ทำให้มีการประสานงานกันระหว่างกิจกรรมต่างๆ และมีการแลกเปลี่ยนข้อมูลระหว่างกัน

อย่างไรก็ตาม การเปิดกว้างในการติดต่อสื่อสารแลกเปลี่ยนข้อมูลระหว่างกัน ทำให้เพิ่มความเสี่ยงที่ทำให้ข้อมูลหรือระบบข้อมูลขององค์กรถูกโจมตีจากผู้ไม่หวังดี แนวทางปฏิบัติหนึ่งที่องค์กรสามารถนำมาใช้เพื่อรักษาความปลอดภัยของข้อมูลและลดความเสี่ยงที่อาจเกิดขึ้นจากภัยคุกคามต่างๆ คือการประยุกต์ใช้มาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799

งานวิจัยนี้มีวัตถุประสงค์ เพื่อศึกษาถึงการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799 ของบริษัทจดทะเบียนและรับอนุญาตในตลาดหลักทรัพย์แห่งประเทศไทย ข้อจำกัดของการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล และปัจจัยที่มีผลต่อความน่าเชื่อถือของข้อมูล โดยศึกษาในมุมมองของผู้ตรวจสอบสารสนเทศของบริษัทจดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย

ผลการวิจัยสรุปได้ว่า โดยรวมแล้ว บริษัทจดทะเบียนมีการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูลตามมาตรฐาน ISO/IEC 17799 ในระดับปานกลาง ซึ่งเมื่อเปรียบเทียบเทียบกับงานวิจัยในอดีต ระดับการปฏิบัติตามมาตรฐานฯ ของบริษัทจดทะเบียนสูงกว่าระดับการปฏิบัติของหน่วยงานในภาครัฐ อุปสรรคสำคัญที่ทำให้องค์กรไม่สามารถปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูลได้ ได้แก่ การขาดความร่วมมือของหน่วยงานภายในองค์กร มาตรฐานการรักษาความปลอดภัยของข้อมูลมีความซับซ้อน และบุคลากรยังไม่มีความรู้ความสามารถอย่างเพียงพอ นอกจากนี้ ยังพบว่า การปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799 ไม่ได้มีความสัมพันธ์กับความน่าเชื่อถือของข้อมูลอย่างมีนัยสำคัญ แสดงให้เห็นว่าการปฏิบัติตามมาตรฐานดังกล่าวไม่ได้เป็นหลักประกันเพียงอย่างเดียวที่จะทำให้ข้อมูลขององค์กรมีความน่าเชื่อถือ แต่อาจมีปัจจัยอื่นที่ส่งผลต่อความน่าเชื่อถือของข้อมูล

คำสำคัญ: มาตรการรักษาความปลอดภัย บริษัทจดทะเบียน ผู้ตรวจสอบสารสนเทศ

Information technology has played substantial roles in business operations nowadays, which results in the efficiency and effectiveness of various activities in the value chain. The intra-and inter-company networks promote the collaboration of a variety of activities and information sharing across organizations.

However, openness in communication increases the risk of data and information system being under attack by sophisticated adversaries. One of many approaches that an organization can utilize in order to maintain information security and reduce security threats is to adopt the ISO/IEC 17799 security standards.

The purpose of this research is to explore the adoption of the ISO/IEC 17799 security standards of listed companies in Thailand in the perspective of information technology auditors. The study also investigates the limitations of the ISO/IEC 17799 security standards' application as well as the factors contributing to the information reliability.

The evidence shows that, in general, Thai listed companies employ the ISO/IEC 17799 security standards in the average level. The comparison of present study with existing research shows that the level of adoption of the ISO/IEC 17799 security standards in public companies is higher than that in government sectors. Major constraints that limit the application of the standards include the lack of cooperation among business units, the complication of the standard itself, and the deficiency of knowledgeable personnel. In addition, the evidence also shows that there is no significant association between the adoption of the ISO/IEC 17799 security standards and information reliability, which infers that the adoption of the standards is not the only approach that guarantees the information reliability. There may be some other factors contributing to the information reliability.

Key Words: Security Standards, Listed Companies, IT Auditor