CASE STUDY: APPLYING OF SECURITY RISK ASSESSMENT PROCESS FOR INFORMATION SYSTEM IN HOSPITAL

AUTTHAPON TONGSRISOMBOON 5237447 EGTI/M

M.Sc.(TECHNOLOGY OF INFORMATION SYSTEM MANAGEMENT)

THESIS ADVISORY COMMITTEE: SURATOSE TRITILANUNT, Ph.D., WARESSARA WEERAWAT, Ph.D., SUPAPORN KIATTISIN, Ph.D.

ABSTRACT

This thesis proposes the technique to apply the risk assessment framework into the information system of the hospital in Thailand. By using our proposed framework, the hospital's IT administrators would be able to manually collect and evaluate some system vulnerabilities and risk of the IT system by themselves. The risk assessment process consists of 6 steps including (1) Information gathering, (2) current capabilities to control vulnerability, (3) Number of threat occurrence from the past, (4) Evaluation of threat's likelihood, (5) Threat's impact measurement, and (6) Risk evaluation and determination. This research applies the technique which is called Penetration Testing and Vulnerability Assessment in order to explore system vulnerabilities inside the IT system, and subsequently examine the capability to control these vulnerabilities. This testing can be divided into 3 steps (1) Information gathering (2) Vulnerability assessment, and (3) Exploitation.

After developing a conceptual model and process of risk assessment, this framework has been used at 2 medium-size hospital. As the pre-forecasting evaluated from factors such as system readiness, hardware readiness, as well as user readiness, the results are consistent with the outcome when we apply our conceptual framework into the hospital's IT system. Moreover, the experimental result shows the risk inside the IT system, severity of vulnerability and consequent impact that may occur when IT system is under attack. The results of this research can be used to fix and strengthen the IT system in the hospitals in order to efficiently reduce the level of risks.

KEY WORDS: RISK ASSESSMENT / RISK ANALYSIS / INFORMATION SECURITY / VULNERABILITY ASSESSMENT / PENETRATION TESTING

135 pages

กรณีศึกษา: การประยุกต์ใช้กระบวนการประเมินความเสี่ยงด้านความมั่นคงในระบบสารสนเทศของโรงพยาบาล
CASE STUDY: APPLYING OF SECURITY RISK ASSESSMENT PROCESS FOR INFORMATION SYSTEM IN HOSPITAL

อรรถพล ทองศรีสมบรณ์ 5237447 EGTI/M

วท.ม. (เทคโนโลยีการจัดการระบบสารสนเทศ)

คณะกรรมการที่ปรึกษาวิทยานิพนธ์: สุรทศ ไตรติลานันท์, Ph.D., วเรศรา วีระวัฒน์, Ph.D., สุภาภรณ์ เกียรติสิน, Ph.D.

บทคัดย่อ

งานวิจัยฉบับนี้จะกล่าวถึงการประยุกต์ใช้โมเดลของการประเมินความเสี่ยงทางด้านเทคนิคมาประยุกต์ใช้กับระบบสารสนเทศของโรงพยาบาลภายในประเทศไทย เพื่อที่โรงพยาบาลจะสามารถนำกรอบแนวคิดไปประยุกต์ใช้ในการประเมินความเสี่ยงในด้านเทคนิคด้วยตนเองได้ กระบวนของการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยในระบบสารสนเทศประกอบไปด้วย 6 ขั้นตอน ได้แก่ (1) การรวบรวมข้อมูล (2) การประเมินความสามารถในการควบคุมช่องโหว่ในปัจจุบัน (3) การรวบรวมจำนวนครั้งที่เคยเกิดการโจมตีในอดีต (4) การประเมินหาโอกาสหรือความน่าจะเป็นในการที่จะเกิดภัยคุกคาม (5) การคำนวณหาผลกระทบที่เกิดจากภัยคุกคาม (6) การประเมินและกำหนดความเสี่ยงที่เกิดขึ้นในโรงพยาบาล โดยงานวิจัยฉบับนี้จะประยุกต์วิธีการที่เรียกว่า Penetration Testing and Vulnerability Assessment มาใช้ในการตรวจสอบหาช่องโหว่และประเมินถึงระดับของความเสี่ยงที่ตรวจพบในระบบสารสนเทศของโรงพยาบาล โดยหลักการทำงานของกระบวนการนี้จะถูกแบ่งขั้นตอนการทดสอบเป็น 3 ขั้นตอนได้แก่ 1) Information gathering 2) Vulnerability assessment และ 3) Exploitation

หลังจากที่ได้พัฒนาโมเดลและขั้นตอนกระบวนการของการประเมินความเสี่ยงขึ้นมา กระบวนการประเมินความเสี่ยงนี้ได้ถูกนำไปทดสอบกับโรงพยาบาลขนาดกลาง 2 แห่ง โดยได้มีการคาดการณ์ความเสี่ยงเบื้องต้นจากปัจจัยแวดล้อมต่างๆ ทั้งด้านความพร้อมของระบบ ความพร้อมของอุปกรณ์ ความพร้อมของบุคคลากร ซึ่งผลที่ได้จากการคาดการณ์เบื้องต้นนั้นสอดคล้องกับความเสี่ยงที่ได้จากการนำกรอบแนวคิดและเครื่องมือต่างๆ เข้าไปทดสอบ ซึ่งผลจากการทดสอบทำให้ทราบถึงช่องโหว่ต่างๆและความเสี่ยงที่เกิดขึ้นในระบบสารสนเทศของโรงพยาบาล ความรุนแรงของช่องโหว่และผลกระทบที่อาจเกิดขึ้นเมื่อถูกโจมตี ซึ่งเราสามารถนำผลที่ได้ไปใช้ในการปรับปรุงแก้ไขระบบเพื่อลดความเสี่ยง รวมไปถึงการแก้ไขช่องโหว่ที่เกิดขึ้นภายในระบบสารสนเทศของโรงพยาบาลได้อย่างมีประสิทธิภาพ

135 หน้า