กรณีศึกษา: โมเดลทางด้านเทคนิคสำหรับวิธีการประเมินความเสี่ยงความมั่นคงปลอดภัยในระบบสารสนเทศสำหรับโรงพยาบาล

สุรทศ ไตรติลานันท์*
ผู้ช่วยศาสตราจารย์ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล
สุรพล รวยสูงเนิน
นักศึกษา ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล

* ผู้นิพนธ์ประสานงาน โทรศัพท์ 0-2889-2138 อีเมล: suratose.tri@mahidol.ac.th
รับเมื่อ 22 เมษายน 2558 ตอบรับเมื่อ 2 กรกฎาคม 2558 เผยแพร่ออนไลน์ 27 พฤศจิกายน 2558

บทคัดย่อ

ปัจจุบันการประเมินและจัดลำดับระดับความเสี่ยงความมั่นคงปลอดภัยสารสนเทศสำหรับโรงพยาบาลในประเทศไทยยังไม่มีขั้นตอนหรือเทคนิคที่เป็นมาตรฐาน ดังนั้นในงานวิจัยนี้ ผู้วิจัยได้ทำการศึกษาและประยุกต์แนวปฏิบัติ รวมถึงมาตรฐานสากลที่เกี่ยวข้องกับการประเมินความเสี่ยงสารสนเทศ และการทดสอบประเมินความมั่นคงปลอดภัยสารสนเทศโดยการประเมินหาช่องโหว่ (Vulnerability Assessment) ด้วยวิธีการใช้เครื่องมือทางเทคนิคเพื่อช่วยในการตรวจสอบประเมิน และนำไปสู่ขั้นตอนการกำหนดโมเดลการประเมินระดับความมั่นคงปลอดภัยสารสนเทศที่สอดคล้องต่อบริบทสารสนเทศสำหรับโรงพยาบาล โดยจากการทดสอบประเมินด้วยโมเดลและวิธีการทางเทคนิคที่ถูกพัฒนาขึ้นพบว่าผลการประเมินมีระดับความเสี่ยงความมั่นคงปลอดภัยสารสนเทศแปรผันตรงตามปัจจัยผลกระทบธุรกิจที่หน่วยงานกำหนดเพื่อให้สอดคล้องและสะท้อนต่อสภาพแวดล้อมจริงของสารสนเทศสำหรับโรงพยาบาล

คำสำคัญ: โมเดลประเมินความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ ระดับความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ ระดับความมั่นคงปลอดภัยสารสนเทศโรงพยาบาล

การอ้างอิงบทความ: สุรทศ ไตรติลานันท์ และ สุรพล รวยสูงเนิน, "กรณีศึกษา: โมเดลทางด้านเทคนิคสำหรับวิธีการประเมินความเสี่ยงความมั่นคงปลอดภัยในระบบสารสนเทศสำหรับโรงพยาบาล," *วารสารวิชาการพระจอมเกล้าพระนครเหนือ*, ปีที่ 26, ฉบับที่ 1, หน้า 29–40, ม.ค.–เม.ย. 2559. DOI: 10.14416/j.kmutnb.2015.07.002

Case Study: A Technical Model for Security Risk Assessment in Information System of Thailand Hospital

Suratose Tritilanunt*
Assistant Professor, Department of Computer Engineering, Faculty of Engineering, Mahidol University, Nakhon Pathom, Thailand

Surapol Ruaysungnoen
Student, Department of Computer Engineering, Faculty of Engineering, Mahidol University, Nakhon Pathom, Thailand

* Corresponding Author, Tel. 0-2889-2138, E-mail: suratose.tri@mahidol.ac.th
Received 22 April 2015; Accepted 2 July 2015; Published online: 27 November 2015

Abstract

In Thailand, there have not been standard processes or techniques of evaluating and assessing security risk for hospital information system. The researcher has studied and applied a practice and universal standard of security risk assessment in information system by using vulnerability scanning and penetration testing technique for evaluating risk level. This leads to a step of defining a suitable model of security risk assessment in the context of hospital information system. By using the proposed model and technique to assess security risk, it is found that the risk level is a direct variation to a business impact factor that is determined by a hospital in order to reflect an environment of information system.

Keywords: Security Risk Assessment Model, Security Risk Rating, Hospital Security Rating

Please cite this article as: S. Tritilanunt and S. Ruaysungnoen, "Case Study: A Technical Model for Security Risk Assessment in Information System of Thailand Hospital," *The Journal of KMUTNB.*, Vol. 26, No. 1, pp. 29–40, Jan.–Apr. 2016 (in Thai). DOI: 10.14416/j.kmutnb.2015.07.002

1. บทนำ

การประเมินความเสี่ยงสารสนเทศ (IT Risk Assessment) ของโรงพยาบาลกรณีศึกษา มีการประเมินความเสี่ยงตามนโยบายบริหารความเสี่ยงขององค์กร ซึ่งอาจไม่สะท้อนและไม่สามารถจัดระดับความมั่นคงปลอดภัยในระบบสารสนเทศได้ รวมทั้งหน่วยงานยังไม่เคยมีการประเมินระดับความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ (Security Risk Assessment) เนื่องด้วยไม่มีขั้นตอน/เทคนิคที่เป็นมาตรฐานเพื่อใช้ในการประเมิน ทำให้ผู้บริหาร/ผู้กับกำดูแลระบบสารสนเทศไม่สามารถทราบถึงระดับของความเสี่ยงความมั่นคงปลอดภัยสารสนเทศที่มีอยู่จริงได้ ดังนั้นในงานวิจัยนี้ผู้วิจัยได้ทำการศึกษาและประยุกต์แนวปฏิบัติ รวมถึงมาตรฐานสากลที่เกี่ยวข้องกับการประเมินความเสี่ยงสารสนเทศ และการทดสอบประเมินความมั่นคงปลอดภัยสารสนเทศโดยการประเมินหาช่องโหว่ (Vulnerability Assessment) ด้วยวิธีการใช้เครื่องมือทางเทคนิคเพื่อช่วยในการตรวจสอบประเมินและนำไปสู่ขั้นตอนของการกำหนดโมเดลการประเมินระดับความมั่นคงปลอดภัยสารสนเทศที่สอดคล้องต่อบริบทสารสนเทศของโรงพยาบาล โดยวิธีการประเมินที่ใช้ในงานวิจัยนี้แบ่งได้เป็น 3 ขั้นตอนคือ การระบุความเสี่ยงหรือช่องโหว่ การประเมินค่าระดับความเสี่ยง และผลลัพธ์ระดับความสำคัญของความเสี่ยง การระบุความเสี่ยงคือขั้นตอนการระบุหรือค้นหาจุดอ่อนของระบบสารสนเทศโดยใช้เครื่องมือช่วยตรวจสอบประเมินหาช่องโหว่อัตโนมัติ การประเมินค่าระดับความเสี่ยงคือขั้นตอนการกำหนดค่าของโอกาส และผลกระทบโดยคำนวณจากเกณฑ์ที่เป็นมาตรฐาน คือ CVSS Base Score รวมถึงการเพิ่มปัจจัยผลกระทบทางธุรกิจ และการประเมินระดับความสำคัญของความเสี่ยงโดยประยุกต์ใช้วิธีการประเมินความเสี่ยงตามมาตรฐานขององค์กร OWASP RISK RATING โดยจากการทดสอบประเมินพบว่าระดับความเสี่ยงแปรผันตรงตามปัจจัยผลกระทบธุรกิจที่หน่วยงาน กำหนดเพื่อให้สอดคล้องและสะท้อนต่อสภาพแวดล้อมจริงของสารสนเทศสำหรับโรงพยาบาล

2. องค์ความรู้และรูปแบบวิธีการประเมิน

งานวิจัยนี้ทำการศึกษา วิเคราะห์และเปรียบเทียบกรอบแนวทางมาตรฐานการประเมินความเสี่ยงด้านสารสนเทศและการตรวจประเมินหาช่องโหว่ เพื่อนำมาประยุกต์กำหนดเป็นโมเดลประเมินระดับความมั่นคงปลอดภัยสารสนเทศสำหรับโรงพยาบาล โดยได้ทำการศึกษาแบ่งออกเป็น 3 หัวข้อประกอบด้วย 1) ความมั่นคงปลอดภัยสารสนเทศทางสุขภาพ (Health Information Security) 2) การประเมินความเสี่ยงความมั่นคงสารสนเทศ (Security Risk Assessment) และ 3) การทดสอบประเมินหาช่องโหว่ (Vulnerability Assessment)

2.1 ความมั่นคงปลอดภัยสารสนเทศทางสุขภาพ

มาตรฐานการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศด้านสาธารณสุข ISO27799 ได้ใช้มาตรฐาน ISO/IEC 27002 เพื่อบริหารจัดการความมั่นคงปลอดภัยสารสนเทศได้อธิบายและกำหนดนิยามเกี่ยวกับ Health Information Security [1] ไว้ดังนี้

2.1.1 สารสนเทศทางสุขภาพ (Health Informatics) คือการประมวลผลข้อมูลสารสนเทศ การติดต่อสื่อสาร การศึกษาวิจัย รวมถึงเทคโนโลยีสารสนเทศที่สนับสนุนกิจกรรมทางสุขภาพ หรือทางการแพทย์

2.1.2 ระบบสารสนเทศทางสุขภาพ (Health Information System) คือระบบที่เกี่ยวกับการเก็บรวบรวมข้อมูลสุขภาพ หรือทางการแพทย์ ในรูปแบบต่างๆ ในคอมพิวเตอร์ มีการจัดเก็บและการรับส่งข้อมูลที่ปลอดภัย มีการควบคุมสิทธิการเข้าถึงอย่างเหมาะสม

2.1.3 ความมั่นคงปลอดภัยสารสนเทศ (Information Security) คือความการรักษาความมั่นคงปลอดภัยสารสนเทศ สินทรัพย์ (Asset) ความรับผิดชอบ (Accountability) ความเชื่อมั่น (Assurance) ความพร้อมใช้ (Availability) การประเมินความเพียงพอของนโยบาย (Compliance Assessment) การกำกับดูแลที่ดี (IT Governance) การบริหารจัดการความเสี่ยง (Risk Management) มีเป้าหมายเพื่อรักษาความมั่นคงสารสนเทศสุขภาพ (Health Information

Security Goals) คือการรักษาความลับ (Confidentiality) ความพร้อมใช้ (Availability) ความถูกต้อง (Integrity) สิทธิการเข้าถึง (Authentication) หน้าที่ความรับผิดชอบ (Accountability) และตรวจสอบติดตาม (Accounting)

2.1.4 ภัยคุกคาม/ช่องโหว่ความมั่นคงปลอดภัยสารสนเทศทางสุขภาพ (Threats and Vulnerabilities in Health Information Security) ภัยคุกคาม/ช่องโหว่จะแตกต่างกันตามสภาพแวดล้อมการควบคุม การกำกับดูแลอุปกรณ์เครื่องมือเข้าถึงได้ง่ายเป็นความเสี่ยงทางกายภาพ ความรู้ความเชี่ยวชาญของบุคลากร รวมถึงการบำรุงรักษาอย่างไม่เหมาะสม อุปกรณ์เครื่องมือต่างๆ ไม่ได้รับการปรับปรุงให้มีความมั่นคง และที่สำคัญคือการเข้าถึงข้อมูลโดยไม่มีสิทธิทำการแก้ไขข้อมูลหรือโจรกรรมข้อมูลผู้ป่วย ซึ่งโรงพยาบาลจะต้องพิจารณาตามสภาพแวดล้อมของโรงพยาบาล

2.2 กรอบแนวทางสำหรับระบบบันทึกข้อมูลสุขภาพอิเล็กทรอนิกส์ และระบบข้อมูลยา

กรอบแนวทางสำหรับระบบบันทึกข้อมูลสุขภาพอิเล็กทรอนิกส์และระบบข้อมูลยา (Conceptual Framework of Interoperable Electronic Health Record and ePrescribing Systems Version 1.0) [2] ได้อธิบายถึงระบบข้อมูลสุขภาพอิเล็กทรอนิกส์คือ การจัดเก็บ การบำรุงรักษาข้อมูลสารสนเทศสุขภาพ โดยจัดเก็บเรียกใช้ได้เฉพาะผู้ที่เกี่ยวข้อง ซึ่งรวมถึงข้อมูลการสังเกตอาการ ผลการตรวจทางห้องปฏิบัติการ ผลหรือภาพถ่ายทางการแพทย์ การวางแผนการรักษา ผลการรักษา และข้อมูลยา เป็นต้น

2.3 กรอบการพัฒนาคุณภาพเทคโนโลยีสารสนเทศโรงพยาบาล

กรอบการพัฒนาคุณภาพเทคโนโลยีสารสนเทศโรงพยาบาล (Hospital IT Quality Improvement Framework: HITQIF) [3], [4] ได้กำหนดแนวทางพัฒนาแบ่งเป็น 7 หัวข้อคือ โครงสร้างบทบาท (Structure and Role) เทคโนโลยี (Technology) บุคลากร (People) กระบวนการ (Processes) การควบคุม (Control) การวัด (Metrics) และข้อมูลสารสนเทศ (Data & Information) ซึ่งหัวข้อการควบคุมได้กล่าวถึงระบบการควบคุมสารสนเทศโดยเฉพาะการบริหารความเสี่ยงด้านสารสนเทศ (IT Risk Management) และการประเมินความมั่นคงสารสนเทศ (Security Assessment)

2.4 การประเมินความเสี่ยงและการจัดการความมั่นคงสารสนเทศในโรงพยาบาล

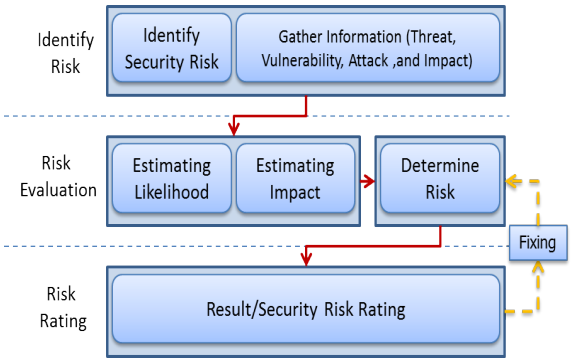
การประเมินความเสี่ยงและการจัดการความมั่นคงสารสนเทศในโรงพยาบาล (Risk Analysis and Security Management) [5], [6] ได้กล่าวถึงการประยุกต์ใช้แนวทางการประเมินความเสี่ยงโดยใช้แบบสอบถาม (Check List) ตรวจสอบตามนโยบายความมั่นคงปลอดภัย (Security Audit) [5] และการทดสอบประเมินระบบ (Penetration Test) ซึ่งใช้วิธีประเมินความเสี่ยงเมตริก 4 × 4 (โอกาส × ผลกระทบ) โดยโอกาสประเมินจากจำนวนภัยคุกคามที่เกิด × ระดับการควบคุม และผลกระทบประเมินจากระดับของประเภทการโจมตี

2.5 การประเมินความเสี่ยงสารสนเทศ

มีแนวทางการประเมินความเสี่ยงด้านความมั่นคงสารสนเทศที่นิยมใช้กันซึ่งแต่ละแนวทางมีวิธีการประเมินความเสี่ยงแตกต่างกันแต่สามารถสรุปขั้นตอนที่สำคัญกำหนดเป็นเป็นแนวทางการประเมินระดับความมั่นคงปลอดภัยสารสนเทศสำหรับโรงพยาบาล สำหรับงานวิจัยนี้โดยแบ่งเป็น 3 ขั้นตอนคือ 1) การระบุความเสี่ยงหรือช่องโหว่ 2) การประเมินค่าระดับความเสี่ยง และ 3) แสดงระดับความสำคัญของความเสี่ยงโดยแสดงในรูปที่ 1 และมีผลการเปรียบเทียบตามตารางที่ 1

2.6 การทดสอบประเมินหาช่องโหว่

การทดสอบประเมินหาช่องโหว่ (Vulnerability Assessment) [11] คือการประเมินความมั่นคงปลอดภัยสารสนเทศโดยการใช้เครื่องมือตรวจสอบประเมินหาช่องโหว่



รูปที่ 1 Risk Assessment Process

ในระบบสารสนเทศ เช่น Nessus Nikto และ Shadow Security Scanner เป็นต้น

2.7 สถาบันให้การรับรองเทคโนโลยีสารสนเทศที่ช่วยวิเคราะห์

IATAC [12] ได้นำเสนอรายงานรับรองเครื่องมือสนับสนุนการตรวจสอบหาช่องโหว่ ซึ่งแต่ละเครื่องมือมีคุณสมบัติแตกต่างกันขึ้นอยู่กับขอบเขตของการทดสอบ ความรู้ความเชี่ยวชาญของผู้ทำการทดสอบ โดยแบ่งเป็น 7 ประเภทสรุปคุณลักษณะได้ตามตารางที่ 2

ตารางที่ 1 ผลการวิเคราะห์เปรียบเทียบแนวปฏิบัติหรือมาตรฐานการประเมินความเสี่ยงด้านสารสนเทศ

#	GUIDELINE				Grouping
	ISMS [7]	**NIST [8]**	**OWASP [9]**	**HIPAA [10]**	
1	Identify Major Assets	System Characterization	NA	System Characterization	Information Gathering
2	Assess Asset Value		NA	System Mission	
2	Identify Threats	Threat Identification	Identifying Risk	Identify any Vulnerability or Weak-ness in Security Procedures or Safe-guards	
3	Identify Vulnerabilities	Vulnerability Identification			
4	NA	Control Analysis			
5	NA	Likelihood Determination	Estimating Likelihood	NA	Information Evaluation
6	NA	Impact Analysis	Estimating Impact	Identify Impact	
7	Identify Measures of Risk	Risk Determination	Determining Severity Risk	NA	
8	Security Requirements	Control Recommendations	Deciding What to Fix	Recommend Security Controls	Recommend
9	Security Controls				
10	Reduce Risks	NA	NA	NA	
11	Risk Acceptance	NA	NA	NA	
12	NA	NA	NA	Determine Residual Risk	
13	NA	Results Documentation	NA	Document all Outputs	Document
14	NA	NA	Customizing Risk Rating Model	NA	Fixing

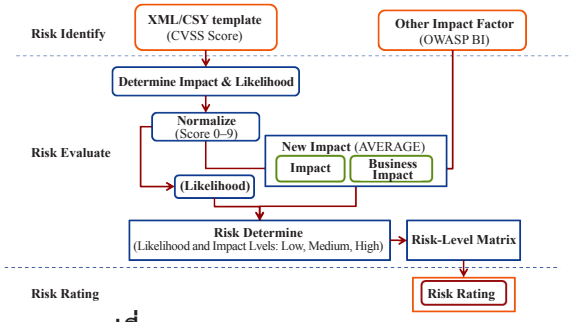
ตารางที่ 2 ตัวอย่างเครื่องมือทดสอบประเมินหาช่องโหว่

Type	Tool	Target	License	Standards
Network Scanner	eEye Retina	Network, OS, Web App/Services, DB	Commercial	SCAP, OVAL, CVE, CVSS
	GFI LANguard	UNIX, Windows	Commercial/Freeware	OVAL, CVE
Host Scanner	Assuria Auditor/ Auditor RA	Windows, UNIX, Linux	Shareware	CVE, CVSS
	NileSOFT Secuguard SSE		Commercial	CVE
DB Scanner	Imperva Scuba	Oracle, DB2, SQL Server, Sybase	Freeware	NA
	Safety-Lab Shadow	Oracle, DB2, SQL Server, Sybase, MySQL, SAP DB	Commercial	
Web Application Scanner	Acunetix	NA	Commercial	NA
	Burp Suite			
	Nikto	HTTP/HTTPS, Web Server	Open Source	
Multi Scanner	Open VAS	Network, Web App	Open Source	NA
	Symantec Risk Automation suite	Network Devices, Host Oss, DB, Network App	Commercial	SCAP, OVAL, CVE, CVSS
	Nessus	Network, Windows, Unix, Linux, SQL DB, Web server	Commercial/Freeware	CVE,CVSS
Automated Penetration Test Tools	CANVAS	All Common Platform and App	Commercial	NA
	Metasploit	Web App, Network, DB Server		CVE
Vulnerability Scan Consolidators	Prolific Solutions pro VM Auditor	NA	Commercial	NA
	ASG			SCAP, OVAL, CVE, CVSS
	Skybox Risk Control	Systems, Devices		CVE

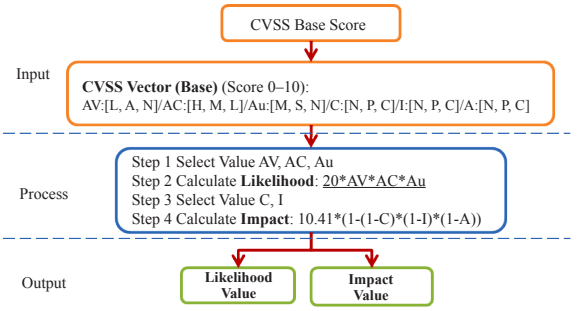
สำหรับงานวิจัยนี้เลือกใช้ผลลัพธ์ที่ได้จากเครื่องมือช่วยทดสอบประเมินความเสี่ยงช่องโหว่ที่ไม่มีค่าลิขสิทธิ์รองรับมาตรฐาน CVSS Score และเป็นที่นิยมใช้กัน โดยทั่วไปเนื่องจาก CVSS Score เป็นค่ามาตรฐานที่สามารถนำมาใช้อ้างอิง เพื่อส่งต่อไปยังและนำไปใช้กับเครื่องมือการทดสอบเจาะช่องโหว่ได้

3. วิธีดำเนินงานวิจัย

การทดลองนี้ได้ทำการจำลองโมเดลการประเมินความเสี่ยงความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาลกรณีศึกษา 2 แห่ง ที่มีระบบสารสนเทศและสภาพแวดล้อมใกล้เคียงกันคือเป็นโรงพยาบาลเฉพาะทาง ขนาดเตียง 80–100 เตียง ระบบสารสนเทศที่สำคัญ เช่น Electronic Medical Records (EMR) System, Laboratory Information System (LIS), Radiology Information System (RIS), และ Picture Archiving and Communication System (PACS) เป็นต้น โดยแบ่งเป็น 3 ขั้นตอนคือ 1) การระบุความเสี่ยงหรือช่องโหว่ 2) การประเมินค่าระดับความเสี่ยง และ 3) แสดงระดับความสำคัญของความเสี่ยงแสดงในรูปที่ 2



รูปที่ 2 Security Risk Evaluate Model



รูปที่ 3 CVSS Base Score Method

3.1 การระบุความเสี่ยงช่องโหว่

คือขั้นตอนการระบุ ค้นหาจุดอ่อนของระบบสารสนเทศโดยการทดสอบประเมินความมั่นคงปลอดภัยสารสนเทศโดยประยุกต์แนวทาง Penetration Test และใช้เครื่องมือช่วยตรวจสอบประเมินหาช่องโหว่อัตโนมัติ งานวิจัยนี้เลือกใช้เครื่องมือตรวจสอบประเมินความเสี่ยงช่องโหว่ที่อัตโนมัติคือ Nessus ซึ่งรองรับ CVSS SCORE และใช้การแสดงผลลัพธ์ในรูปแบบ XML Format ทำการสำเนาหรือนำเข้า Excel Data Sheet หรือ Access Data Table หรือฐานข้อมูลอื่นๆ ที่สามารถคำนวณหรือประมวลผลได้

3.2 การประเมินค่าระดับความเสี่ยง

คือขั้นตอนการคำนวณหรือประเมินค่าระดับความสำคัญของความเสี่ยงแบ่งเป็น 6 ขั้นตอนดังนี้

3.2.1 การประเมินค่าโอกาสและผลกระทบใช้วิธีการคำนวณตาม CVSS Base Vector [13] มีขั้นตอนตามรูปที่ 3 และมีวิธีการคำนวณตามสมการ (1) และ (2)

$$Imp = 10.41*(1-(1-C)*(1-I)*(1-A)) \quad (1)$$

$$Lik = 20* AV*AC*Au \quad (2)$$

เมื่อ Imp คือ Impact Value
Lik คือ Likelihood หรือ Exploitability Value
C, I, A, AV, AC, Au มีค่าตามตารางที่ 3

ตารางที่ 3 ความหมายและค่า Base Metric [13]

Base Metric	Case of Metric	Value
AccessVector (AV)	L: requires local access	0.395
	A: adjacent network accessible	0.646
	N: network accessible	1
AccessComplexity (AC)	H: high	0.35
	M: medium	0.61
	L: low	0.71
Authentication (AU)	M: requires multiple instances of authentication	0.45
	S: requires single instance of authentication	0.56
	N: requires no authentication	0.704
ConfidentialityImpact (C)	N: none	0
IntegrityImpact (I)	P: partial	0.275
AvailabilityImpact (A)	C: complete	0.66

3.2.2 การปรับค่าคะแนนให้อยู่ในช่วงระดับคะแนนให้สอดคล้อง OWASP RISK RATING ให้มีช่วงคะแนนอยู่ระหว่าง 1–9 มีวิธีการคำนวณตามสมการ (3), (4) และ (5)

$$NLik = Norm(Likelihood\ Value) \quad (3)$$

$$NImp = Norm(Impact\ Value) \quad (4)$$

$$Norm(X_i) = 9*(X_i)/X_n \quad (5)$$

เมื่อ NLik คือ Normalize Likelihood Value
NImp คือ Normalize Impact Value

X_i คือ Likelihood or Impact Value

X_n คือ Rate Number of Old Value

3.2.3 การเพิ่มปัจจัยด้านผลกระทบ Business Impact Factor [9] โดยทำการประเมินผลกระทบทางธุรกิจของแต่ละสารสนเทศโดยใช้สมมุติฐานกรณีสินทรัพย์/ระบบสารสนเทศ ล้มเหลว/ไม่สามารถใช้งานได้ มีวิธีการคำนวณตามสมการ (6)

$$BI = AVERAGE(Fd[x], Rd[x], Np[x], Pv[x]) \quad (6)$$

BI คือ Business Impact Value

Fd[x], Rd[x], Np[x], Pv[x] ใช้ค่าตามตารางที่ 4

ตารางที่ 4 ปัจจัยประเมินผลกระทบทางธุรกิจ [9]

Business Impact Factor	Case of Metric	Rating
Financial damage (Fd)	L: Less than the cost to fix vulnerability	1
	M: Minor effect on annual profit	3
	S: Significant effect on annual profit	7
	B: Bankruptcy	9
Reputation damage (Rd)	M: Minimal damage	1
	L: Loss of major accounts	4
	G: Loss of goodwill	5
	B: Brand damage	9
Non-compliance (Nc)	M: Minor violation	2
	C: Clear violation	5
	H: High profile violation	7
Privacy violation (Pv)	O: One individual	3
	H: Hundreds of people	5
	T: Thousands of people	7
	M: Millions of people	9

3.2.4 การประเมินค่าปัจจัยผลกระทบรวมโดยมีวิธีการคำนวณตามสมการ (7) [9]

$$New\ Impact(NI) = Average(I_1, I_2, \ldots, I_n) \quad (7)$$

I_n คือ Impact Value

3.2.5 การประเมินระดับโอกาส และระดับผลกระทบ โดยใช้ค่า NLik จากขั้นตอนที่ 3.2.2 เป็นค่า Likelihood Value และค่า New Impact จากขั้นตอนที่ 3.2.4 เป็นค่า Impact Value ประเมินตามตารางที่ 5

ตารางที่ 5 ช่วงคะแนนโอกาส และผลกระทบ [9]

Likelihood and Impact Levels	
0 to < 3	LOW (1)
3 to < 6	MEDIUM (2)
6 to 9	HIGH (3)

3.2.6 การประเมินระดับความสำคัญของความเสี่ยงของแต่ละความเสี่ยงโดยนำค่า Likelihood Level และ Impact Level ประเมินตามตารางที่ 6

ตารางที่ 6 เมตริกความเสี่ยงของ OWASP [9]

Overall Risk Severity				
Impact	High (3)	Medium	High	Critical
	Medium (2)	Low	Medium	High
	Low (1)	Note	Low	Medium
		Low (1)	Medium (2)	High (3)
	Likelihood			

3.3 การสรุปผล

โดยแสดงระดับความสำคัญของความเสี่ยงสารสนเทศภาพรวม หรือแสดงแยกตามระบบสารสนเทศเป้าหมาย

4. ผลการทดสอบ

การทดสอบประเมินค่าระดับความเสี่ยงตามโมเดลที่กำหนดโดยนำเข้าผลลัพธ์ที่ได้จากเครื่องมือ Nessus และผลการประเมินผลกระทบทางธุรกิจของสารสนเทศเป้าหมายซึ่งมีผลการประเมินตามตารางที่ 7 และ 8

ตารางที่ 7 ผลการประเมินระดับผลกระทบต่อระบบสารสนเทศ Hospital A

Asset/Systems	Fd	Rd	Nc	Pv	BI Rating
APP SERVER	7	5	2	7	5.25
DB SERVER	7	5	2	7	5.25
WEBSITE	3	9	2	5	4.75
LIS	3	5	2	5	3.75
PACS	3	5	2	5	3.75
INTRANET	3	4	2	5	3.50

ตัวอย่างที่ 1 APP SERVER (Hospital A)

a) ระบุระดับผลกระทบทางธุรกิจตามตารางที่ 4 Business Impact Factor

Financial damage (Fd) = S|Significant effect on annual profit|7

Reputation damage (Rd) = G|Loss of goodwill|5

Non-compliance (Nc) = M|Minor violation |2

Privacy violation (Pv) = T|Thousands of people |7

b) คำนวณผลกระทบทางธุรกิจตามสมการที่ (6)

BI = AVERAGE (Fd[S], Rd[G], Np[M], Pv[T])

BI = AVERAGE (7, 5, 2, 7) = 5.25

ดังนั้นระดับผลกระทบ (BI Rating) คือ 5.25

ตารางที่ 8 ผลการประเมินระดับผลกระทบต่อระบบสารสนเทศ Hospital B

Asset/ Systems	Fd	Rd	Nc	Pv	BI Rating
PACS	7	5	7	7	6.5
LIS	3	5	7	7	5.5
HIS-APP	1	5	7	7	5
HIS-DB	1	5	7	7	5
WEBSITE	1	1	7	7	4

ตัวอย่างที่ 2 PACS (Hospital B)

a) ระบุระดับผลกระทบทางธุรกิจตามตารางที่ 4 Business Impact Factor

Financial damage (Fd) = S|Significant effect on annual profit|7

Reputation damage (Rd) = L| Loss of goodwill |5

Non-compliance (Nc) = H|High profile violation |7

Privacy violation (Pv) = T|Thousands of people |7

b) คำนวณผลกระทบทางธุรกิจตามสมการที่ (6)

BI = AVERAGE (Fd[S], Rd[G], Np[H], Pv[T])

BI = AVERAGE (7, 5, 7, 7) = 6.5

ดังนั้นระดับผลกระทบ (BI Rating) คือ 6.5

4.1 ผลการประเมินสารสนเทศ

โดยใช้โมเดลที่กำหนดมีผลการประเมินโดยมีตัวอย่างผลตามตารางที่ 9 และ 10

ตารางที่ 9 ตัวอย่างผลการประเมินระดับผลกระทบต่อระบบสารสนเทศ Hospital A

Asset	Vulnerability	L × I	Risk	L × NI	Risk+
Intranet	Cross Site Scripting (Form)	3 × 1	Med	3 × 2	High
Website	Cross Site Scripting (URL)	3 × 1	Med	3 × 2	High
LIS	SSL Certificate Expiry	3 × 1	Med	3 × 2	High
PACS	Terminal Services Encryption Level is not FIPS-140 Compliant	2 × 1	Low	2 × 2	Med
APP SERVER	SMB Signing Required	3 × 1	Med	3 × 2	High
DB SERVER	Symantec Backup Exec for Windows Multiple Vulnerabilities	3 × 3	Critical	3 × 3	Critical

ตารางที่ 9 ตัวอย่างผลการประเมินระดับผลกระทบต่อระบบสารสนเทศ Hospital A (ต่อ)

Asset	Vulnerability	CVSS	L	I	BI	NI
Intranet	Cross Site Scripting (Form)	CVSS2#AV:N/ AC:M/Au:N/ C:N/I:P/A:N	7.73	2.574	3.5	3.04
Website	Cross Site Scripting (URL)	CVSS2#AV:N/ AC:M/Au:N/ C:N/I:P/A:N	7.73	2.574	4.75	3.66
LIS	SSL Certificate Expiry	CVSS2#AV:N/ AC:L/Au:N/ C:N/I:P/A:N	9	2.574	3.75	3.16
PACS	Terminal Services Encryption Level is not FIPS-140 Compliant	CVSS2#AV:N/ AC:H/Au:N/ C:P/I:N/A:N	4.44	2.574	3.75	3.16
APP SERVER	SMB Signing Required	CVSS2#AV:N/ AC:L/Au:N/ C:N/I:P/A:N	9	2.574	5.25	3.91
DB SERVER	Symantec Backup Exec for Windows Multi Vulnerabilitie	CVSS2#AV:N/ AC:L/Au:N/ C:C/I:C/A:C	9	9	5.25	7.13

ตัวอย่างที่ 3 Intranet (Hospital A) มีค่า CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

a) คำนวณค่าผลกระทบ (Imp) ตามสมการ (1)

Imp = 10.41*(1-(1-C[N])*(1-I[P])*(1-A[N]))

Imp = 10.41*(1-(1-0)*(1-0.275)*(1-0)) = 2.86

b) คำนวณค่าโอกาส (Lik) จากสมการ (2)

Lik = 20*AV[N]*AC[M]*Au[N]

Lik = 20*1*0.61*0.704 = 8.59

c) ปรับค่าผลกระทบใหม่ (NImp) ตามสมการ (3)

$NImp = Norm(Lik) = 9*(X_i)/X_n$

NImp = 9*2.86/10 = 2.574

ดังนั้นค่าคะแนนผลกระทบ (Impact) I คือ 2.574

d) ปรับค่าโอกาสใหม่ (NLik) ตามสมการ (4)

$NLik = Norm(Lik) = 9*(X_i)/X_n$

NLik = 9*8.59/10 = 7.73

ดังนั้นค่าคะแนนผลกระทบ (Likelihood) L คือ 7.73

e) นำค่าผลกระทบทางธุรกิจ (BI) จากตารางที่ 7

BI = 3.5

f) คำนวณค่าผลกระทบใหม่ (NI) ตามสมการที่ (7)

NI = Average (I, BI)

NI = Average (2.574, 3.5) = 3.04

ดังนั้นค่าคะแนนผลกระทบใหม่ NI คือ 3.04

g) นำค่า L, I, และ NI จากขั้นตอน c), d), f) ประเมินระดับโอกาส/ผลกระทบตามตารางที่ 5

L × I = HIGH (3) × LOW (1) = 3 × 1

L × NI = HIGH (3) × MEDIUM (2) = 3 × 2

h) นำค่า L × I และ L × NI จากขั้นตอน g) ประเมินระดับความสำคัญความเสี่ยงก่อนเพิ่มผลกระทบทางธุรกิจ (RISK) และหลังเพิ่มผลกระทบทางธุรกิจ (RISK+) ตามตารางที่ 6

RISK = L × I = 3 × 1 = Medium

RISK+ = L × NI = 3 × 2 = High

ดังนั้นระดับความเสี่ยงก่อนเพิ่มผลกระทบธุรกิจ (RISK) คือ MEDIUM และหลังเพิ่มธุรกิจ (RISK+) คือ HIGH

ตารางที่ 10 ผลการประเมินระดับผลกระทบต่อระบบสารสนเทศ Hospital B

Asset	Vulnerability	L × I	Risk	L × NI	Risk+
Website	Web Server Uses Plain Text Authentication Forms	2 × 1	Low	2 × 2	Med
HIS	SMB Signing Disabled	3 × 1	Med	3 × 2	High
PACS	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution	3 × 3	Critical	3 × 3	Critical
LIS	Terminal Services Encryption Level is Medium or Low	3 × 1	Med	3 × 2	High
HIS-DB	MS09-050: Microsoft Windows SMB2 – Smb2Validate ProviderCallback	3 × 3	Critical	3 × 3	Critical

ตารางที่ 10 ผลการประเมินระดับผลกระทบต่อระบบสารสนเทศ Hospital B (ต่อ)

Asset	Vulnerability	CVSS	L	I	BI	NI
Website	Web Server Uses Plain Text Authentication Forms	CVSS2# AV:N/AC:H/ Au:N/C:P/ I:N/A:N	4.44	2.574	4	3.29
HIS	SMB Signing Disabled	CVSS2# AV:N/AC:L/ Au:N/C:N/ I:P/A:N	9	2.574	5	3.79
PACS	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution	CVSS2# AV:N/AC:M/ Au:N/C:C/ I:C/A:C	7.73	9	6.5	7.75
LIS	Terminal Services Encryption Level is Medium or Low	CVSS2# AV:N/AC:M/ Au:N/C:P/ I:N/A:N	7.73	2.574	5.5	4.04
HIS-DB	MS09-050: Microsoft Windows SMB2 Smb2Validate ProviderCallback	CVSS2# AV:N/AC:M/ Au:N/C:P/ I:N/A:N	9	9	5	7

ตัวอย่างที่ 4 Website (Hospital B) มีค่า CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

a) คำนวณค่าผลกระทบ (Imp) ตามสมการ (1)

Imp = 10.41*(1-(1-C[P])*(1-I[N])*(1-A[N]))

Imp = 10.41*(1-(1-0.275)*(1-0)*(1-0)) = 2.86

b) คำนวณค่าโอกาส (Lik) จากสมการ (2)

Lik = 20* AV[N]*AC[H]*Au[N]

Lik = 20* 1*0.35*0.704 = 4.93

c) ปรับค่าผลกระทบใหม่ (NImp) ตามสมการ (3)

$NImp = Norm(Lik) = 9*(X_i)/X_n$

NImp = 9*2.86/10 = 2.574

ดังนั้นค่าคะแนนผลกระทบ (Impact) I คือ 2.574

d) ปรับค่าโอกาสใหม่ (NLik) ตามสมการ (4)

$NLik = Norm(Lik) = 9*(X_i)/X_n$

NLik = 9*4.93/10 = 4.44

ดังนั้นค่าคะแนนผลกระทบ (Likelihood) L คือ 4.44

e) นำค่าผลกระทบทางธุรกิจ (BI) จากตารางที่ 7

B I= 3.5

f) คำนวณค่าผลกระทบใหม่ (NI) ตามสมการที่ (7)

NI = Average (I, BI)

NI = Average (2.574, 4) = 3.29

ดังนั้นค่าคะแนนผลกระทบใหม่ NI คือ 3.29

g) นำค่า L, I, และ NI จากขั้นตอน c), d), f) ประเมินระดับโอกาส/ผลกระทบตามตารางที่ 5

L × I = MEDIUM (2) × LOW (1) = 2 × 1

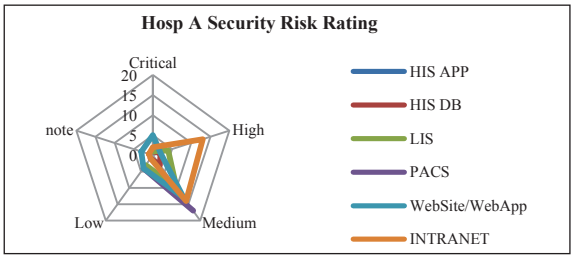
L × NI = MEDIUM (2) × MEDIUM (2) = 2 × 2

h) นำค่า L × I และ L × NI จากขั้นตอน g) ประเมินระดับความสำคัญความเสี่ยงก่อนเพิ่มผลกระทบทางธุรกิจ (RISK) และหลังเพิ่มผลกระทบทางธุรกิจ (RISK+) ตามตารางที่ 6

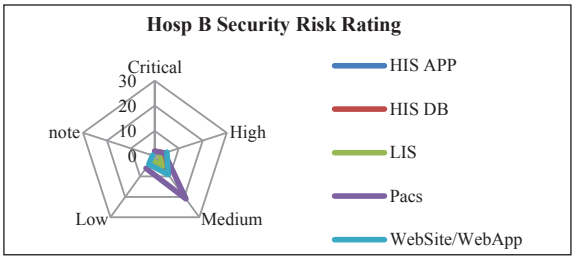
RISK = L × I = 2 × 1 = Low

RISK+ = L × NI = 2 × 2 = Medium

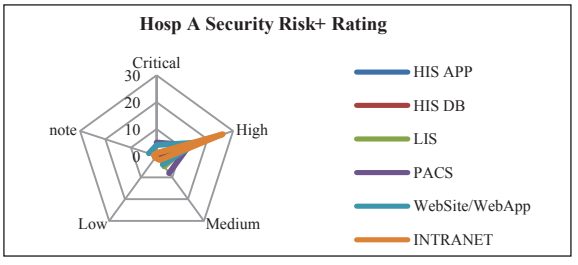
ดังนั้นระดับความเสี่ยงก่อนเพิ่มผลกระทบธุรกิจ (RISK) คือ LOW และหลังเพิ่มธุรกิจ (RISK+) คือ MEDIUM



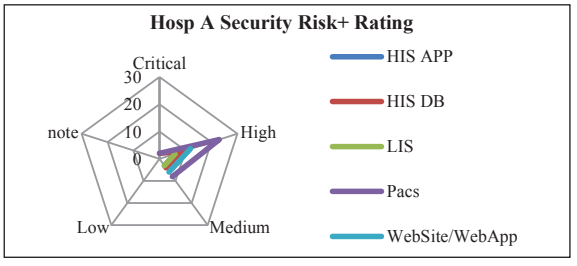
รูปที่ 4 Security Risk Rating Hospital A



รูปที่ 5 Security Risk Rating Hospital B



รูปที่ 6 Security Risk+ Rating Hospital A



รูปที่ 7 Security Risk+ Rating Hospital B

4.2 สรุปผลการทดสอบประเมิน

พบว่าก่อนเพิ่มปัจจัยผลกระทบธุรกิจของสารสนเทศ พบว่าภาพรวมสารสนเทศทั้ง 2 โรงพยาบาลมีแนวโน้มระดับความเสี่ยงอยู่ในระดับปานกลาง และหลังเพิ่มปัจจัยทั้งโรงพยาบาล A และ B มีแนวโน้มความเสี่ยงอยู่ในระดับสูง ซึ่งแสดงดังรูปที่ 4 ถึง 7

5. สรุป

การประเมินความมั่นคงปลอดภัยสารสนเทศโดยใช้เครื่องมือตรวจสอบประเมินหาช่องโหว่อัตโนมัติสามารถแสดงรายงานระดับความเสี่ยงตามมาตรฐานซึ่งมีความน่าเชื่อถือแต่อาจยังไม่สอดคล้องต่อสภาพแวดล้อมของหน่วยงาน ซึ่งมีความสำคัญต่อการตอบสนองต่อความเสี่ยง และการวางแผนปรับปรุงระบบความมั่นคงสารสนเทศของโรงพยาบาล จากการทดสอบประเมินกรณีศึกษาทั้ง 2 แห่ง ด้วยโมเดลประเมินความเสี่ยงความมั่นคงปลอดภัยในระบบสารสนเทศ โดยให้หน่วยงานเลือกทำการประเมินปัจจัยผลกระทบทางธุรกิจเพิ่มพบว่าผลการประเมินมีระดับความเสี่ยงความมั่นคงปลอดภัยสารสนเทศแปรผันตรงตามปัจจัยผลกระทบธุรกิจที่หน่วยงานกำหนดซึ่งสอดคล้องและสะท้อนต่อสภาพแวดล้อมจริงของสารสนเทศสำหรับโรงพยาบาล

อย่างไรก็ตามผลการประเมินผลกระทบทางธุรกิจหน่วยงานควรทำการระดมสมองจากผู้เกี่ยวข้องหรือสามารถเพิ่มปัจจัยอื่นๆ เพื่อให้ผลการประเมินสอดคล้องและเหมาะสมตรงตามสภาพแวดล้อมจริงของระบบสารสนเทศของโรงพยาบาล

6. กิตกรรมประกาศ

งานวิจัยนี้ได้รับการสนับสนุนจากคณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล และสำนักงานคณะกรรมการวิจัยแห่งชาติ

เอกสารอ้างอิง

[1] *Health informatics-Information security management in health using ISO/IEC 27002*, ISO 27799, 2008.

[2] DG INFSO and Media, *The conceptual framework of interoperable electronic health record and ePrescribing systems Version 1.0*, April 2008.

[3] *HA-SPA (Standards Practice Assessment), Healthcare Accreditation Institute (Public Organisation)*, October 2009.

[4] *Hospital IT Quality Improvement Framework (HITQIF)*, *Thai Medical Informatics Association*, March 15, 2012.

[5] P. Chaitasanangam, "Risk Analysis and Security Management of IT Information in Hospital," in *Proc. the 2nd Nat. and Int. Graduate Study Conf.*, 2012 May 10–11, Bangkok, Thailand, 2012 (in Thai).

[6] S. Tritilanunt and A. Tongsrisomboon, "Risk Analysis and Security Management of IT Information in Hospital," *International Journal of Computer and Information Technology*, vol. 4, no. 2, 2014 (in Thai).

[7] *ISMS-201 IT Risk Management Standard Version 2.0*, ISO, 2012.

[8] G. Stoneburner, A. Goguen, and A. Feringa, "Risk Management Guide for Information Technology System," National Institute of Standards and Technology, July, 2002.

[9] *OWASP Testing Guide*, The Open Web Application Security Project (OWASP), 2008.

[10] *HIPAA Security Procedures Resource Manual*, North Dakota State University (NDSU), September 2012.

[11] K. Graves, *Certified Ethical Hacker STUDY GUIDE*, Wiley Publishing, Inc., 2010.

[12] *Information Assurance Tools Report–Vulnerability Assessment*, *Information Assurance Technology Analysis Center (IATAC)*, *6th ed.*, May 2, 2011.

[13] P. Mell, K. Scarfone, and S. Romanosky, "CVSS: A complete Guide to the Common Vulnerability Scoring System Version 2.0," *National Institute of Standards and Technology*, June 2006.