การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

โรงพยาบาลโนนไทย

การจัดการความเสี่ยง (Risk Management) เป็นกลไกสำคัญ สำหรับการควบคุมคุณภาพระบบงานทุกระบบ เพราะหากเราต้องการให้ระบบงานมีคุณภาพ เราต้องประเมินและตรวจสอบความเสี่ยงที่จะให้ระบบงานของเราด้อยคุณภาพให้ครอบคลุมความเสี่ยงทุกด้าน แล้วจัดการป้องกันไม่ให้ความเสี่ยงเหล่านั้นมีโอกาสมารบกวน และทาให้ระบบงานของเราด้อยคุณภาพลงไปได้

ระบบเทคโนโลยีสารสนเทศโรงพยาบาลก็เป็นระบบหนึ่งที่ต้องใช้การจัดการความเสี่ยงเป็นกลไกสำคัญในการควบคุมเพื่อให้มั่นใจว่าระบบดำเนินไปได้อย่างมีคุณภาพ ดังนั้น ผู้บริหาร และผู้ปฏิบัติงานในระบบเทคโนโลยีสารสนเทศโรงพยาบาลจึงต้องมีความเข้าใจวิธีการจัดการความเสี่ยงเป็นอย่างดี เพื่อให้สามารถดำเนินการจัดการความเสี่ยงได้อย่างมีประสิทธิภาพ

ปัจจัยสำคัญที่ทำให้เกิดความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

ปัจจัยสำคัญที่ทำให้เกิดความเสี่ยงในระบบเทคโนโลยีสารสนเทศ ประกอบไปด้วยปัจจัยดังนี้

1. จุดอ่อน หรือ ช่องโหว่
2. ภัยคุกคาม

จุดอ่อน หมายถึง ข้อบกพร่องทางด้าน กายภาพ การจัดระบบ ขั้นตอนการทำงาน บุคลากรการบริหารจัดการ ครุภัณฑ์ โปรแกรม หรือข้อมูลสารสนเทศสำคัญ ดังตัวอย่างต่อไปนี้

- ไม่มีการติดตั้งกุญแจประตูห้องเครื่องแม่ข่าย
- ไม่มีระบบดักจับควัน และระบบดับเพลิงอัตโนมัติในห้องควบคุมระบบเครื่องแม่ข่าย
- ไม่กำหนดขั้นตอนมาตรฐานในการสำรองข้อมูล
- บุคคลากรไม่ทาตามระเบียบปฏิบัติด้านการตั้งรหัสผ่าน
- ไม่มีการดำเนินการควบคุมความมั่นคงปลอดภัย
- ไม่มีเครื่องแม่ข่ายสารอง
- ใช้โปรแกรมระบบงานสำคัญร่วมกับโปรแกรมส่วนตัว
- ติดตั้งโปรแกรมที่ดาวน์โหลดจากอินเทอร์เน็ตได้โดยอิสระ
- ไม่มีการควบคุมการเข้าถึงข้อมูลสารสนเทศที่สำคัญ

ภัยคุกคาม หมายถึง ภัยอันตรายต่างๆ ทั้งที่มีสาเหตุมาจากมนุษย์และสาเหตุอื่นๆ อันมีโอกาสจะทำให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ ดังอย่างต่อไปนี้

- ไฟไหม้
- น้ำท่วม
- ขโมย
- ไวรัสคอมพิวเตอร์
- กระแสไฟฟ้าขัดข้อง

ความเสี่ยง คือความเป็นไปได้หรือโอกาสที่ภัยคุกคามจะเข้ามาสร้างความเสียหายให้กับระบบ โดยจุดอ่อนของระบบจะเพิ่มโอกาสให้ภัยคุกคามเข้ามาสร้างความเสียหายให้กับระบบเทคโนโลยีสารเทศได้ การจัดการความเสี่ยง จึงมีเป้าหมายสำคัญเพื่อ ลดโอกาส ที่ภัยคุกคามจะเข้ามาสร้างเสียหายให้กับระบบนั่นเอง

ขั้นตอนสำคัญในการจัดการความเสี่ยง

ขั้นตอนที่สำคัญในการจัดการความเสี่ยง ประกอบไปด้วย ขั้นตอนดังต่อไปนี้

1. การค้นหาและประเมินความเสี่ยง (Risks Identification and Risks Assessment)
2. การวางแผนกลยุทธ์จัดการความเสี่ยง (Risk Management Strategic Planning)
3. การดำเนินการจัดการความเสี่ยง (Risk Treatment)

1. การค้นหาและประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

การค้นหาและประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล ทำโดยการสำรวจระบบเทคโนโลยีสารสนเทศของโรงพยาบาล เพื่อค้นหาจุดอ่อนและภัยคุกคามที่มีโอกาสจะเข้ามาทำความเสียหายให้กับระบบ แล้วประเมินระดับคะแนนความเสี่ยง เพื่อนำมาพิจารณาวางแผนจัดการความเสี่ยงต่อไป

มาตรฐาน ISO/IEC 27001 : 2013 ซึ่งเป็นมาตรฐานนานาชาติสำหรับระบบบริหารความปลอดภัยของข้อมูล (Security Management Systems, ISMS) ได้กล่าวถึงความเสี่ยงในระบบเทคโนโลยีสารสนเทศไว้มากมาย ดังอย่างเช่น

- acts of terrorism การก่อการร้าน
- air conditioning failure ระบบปรับอากาศหยุดทางาน
- airborne particles/dust ฝุ่นละออง
- bomb attack การวางระเบิด
- breach of legislation or regulations การละเมิดนโยบายและระเบียบปฏิบัติด้านความปลอดภัย
- breaches of contractual obligations การละเมิดข้อตกลงหรือสัญญาที่ผูกพัน

- compromise of security ความย่อหย่อนในระบบรักษาความปลอดภัย
- damage caused by penetration tests ความเสียหายจากการทดลองเจาะเข้าระบบ
- damage caused by third parties ความเสียหายจากบุคคลที่สาม
- destruction of records ข้อมูลถูกทำลาย
- destruction of the business continuity plans แผนกู้คืนถูกทำร้าย
- deterioration of media สื่อที่เก็บข้อมูลเสื่อมสภาพ
- disasters (natural of man-made) ภัยพิบัติ (จากธรรมชาติ หรือ จากมนุษย์)
- ฯลฯ

การค้นหาและประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล จึงควรเริ่มจาก การตรวจสอบรายการความเสี่ยงที่อาจเกิดขึ้นได้ทั้งหมด โดยอาจใช้แบบประเมินความเสี่ยง เช่น แบบประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล ที่พัฒนาโดย สมาคมเวชสารสนเทศไทย โดยเมื่อคาดว่าอาจเกิดความเสี่ยงเรื่องใดแล้ว คณะผู้ประเมินจะต้องประเมินรายละเอียดเพิ่มเติม ได้แก่

1. โอกาสที่จะเกิดความเสี่ยงนั้น Probability
2. ความเสียหายที่จะเกิดขึ้น Impact

การประเมินความเสี่ยงโอกาสที่จะเกิดความเสี่ยงและผลเสียหาย จะประเมินค่าเป็นระดับ 1-5 ดังนี้

ประเมินโอกาสที่จะเกิดความเสี่ยง มีค่าได้เป็น

1. ต่ำมาก ไม่น่าจะเกิดเหตุการณ์นี้ได้ หรือมีโอกาสเกิดได้น้อยมาก
2. ต่ำ มีโอกาสเกิดเหตุการณ์ได้น้อย อาจพบได้สักครั้ง ในรอบ 1 ปี
3. ปานกลาง มีโอกาสเกิดเหตุการณ์ได้บ้าง อย่างน้อย เดือนละ 1 ครั้ง
4. สูง มีโอกาสเกิดเหตุการณ์ได้บ่อย เดือนละหลายครั้ง
5. สูงมาก มีโอกาสเกิดเหตุการณ์ได้บ่อยมาก พบทุกๆ สัปดาห์

ประเมินผลเสียหาย มีค่าได้เป็น

1. ต่ำมาก ไม่น่าจะเกิดผลกระทบต่อการให้บริการ หรือมีผลกระทบน้อยมาก
2. ต่ำ มีผลกระทบต่อการให้บริการของโรงพยาบาลในบางจุด
3. ปานกลาง มีผลกระทบต่อการให้บริการของโรงพยาบาลใน 1 - 2 แผนก
4. สูง มีผลกระทบต่อการให้บริการของโรงพยาบาล 3 - 4 แผนก
5. สูงมาก มีผลกระทบต่อการให้บริการของโรงพยาบาลเป็นวงกว้าง อาจเกิดอันตรายต่อผู้ป่วย

หลังจากนั้นให้ประเมินคะแนนความเสี่ยง คำนวณได้จาก คะแนนโอกาส คูณ กับ คะแนนผลเสียหาย เช่น โอกาสเกิดความเสี่ยง = 3 ผลเสียหาย = 5 ดังนั้น คะแนนความเสี่ยง = 3x5 = 15

เมื่อคำนวณคะแนนความเสี่ยงแล้ว ให้นาคะแนนความเสี่ยงมาพิจารณา ตามแผนผังประเมินความเสี่ยงดังนี้

ค่าความเสี่ยง (ระดับ)			โอกาสที่จะเกิดความเสียหาย (Likelihood : L				
			ต่ำมาก	ต่ำ	ปานกลาง	สูง	สูงมาก
			1	2	3	4	5
ความรุนแรงของผลกระทบ (Impact : I)	สูงมาก	5	5	10	15	20	25
	สูง	4	4	8	12	16	20
	ปานกลาง	3	3	6	9	12	15
	ต่ำ	2	2	4	6	8	10
	ต่ำมาก	1	1	2	3	4	5

ระดับการประเมินความเสี่ยง

ระดับการประเมินความเสี่ยง		
ระดับคะแนนความเสี่ยง	ระดับความเสี่ยง	คำอธิบาย
1 - 3	ต่ำ (Low)	เป็นระดับความเสี่ยงที่องค์กรสามารถยอมรับได้
4-9	ปานกลาง (Medium)	เป็นระดับความเสี่ยงที่องค์กรพอสามารถยอมรับ แต่ต้องมีมาตรการควบคุมความเสี่ยง/ปรับปรุงความเสี่ยงในระดับที่องค์กรยอมรับได้
10 – 16	สูง (High)	ระดับที่ไม่สมารถยอมรับได้โดยต้องจัดการความเสี่ยง เพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป
17 - 25	สูงมาก(Very High)	เป็นระดับที่องค์กรไมสามารถยอมรับได้/มีการปรับปรุงอย่างเร่งด่วน

มีการจัดลาดับความสำคัญของเหตุการณ์ที่ทำให้เกิดความเสี่ยง โดยค่าที่มีความเสี่ยงสูงมาก (17-25) จะถือว่าเป็นความเสี่ยงที่ไม่สามารถยอมรับได้ ต้องเร่งจัดการให้ยอมรับได้โดยทันที

มีการกำหนดวิธีแก้ไขความเสี่ยง ให้กับเหตุการณ์ต่างๆ และมีแผนจัดการเหตุการณ์ไม่ปกติ ซึ่งกำหนดแนวทางการปฏิบัติอย่างชัดเจน ทำให้มั่นใจได้ว่าผลการประเมินถูกต้องและสามารถนำผลการประเมินมาใช้ได้

กลยุทธ์ในการแก้ไขความเสี่ยง

กลยุทธ์ที่ 1 การลดความเสี่ยง

กลยุทธ์ที่ 2 การย้ายความเสี่ยง

กลยุทธ์ที่ 3 การหลีกเลี่ยงความเสี่ยง

กลยุทธ์ที่ 4 การยอมรับความเสี่ยง

ศูนย์คอมพิวเตอร์และสารสนเทศ ได้มีการนำแผนงาน/โครงการ มาวิเคราะห์รายละเอียดความเสี่ยงภายใต้ภารกิจรับผิดชอบ ดังนี้

ผลการประเมินความเสี่ยงในระบบสารสนเทศของโรงพยาบาลโนนไทยตามมาตรฐาน TMI

ลำดับ	ส่วนประกอบทางด้านสารสนเทศ	P	I	ค่าคะแนน	ระดับความเสี่ยง
1	Hacking / Intrusion / Malware	2	2	4	ปานกลาง
2	Server crash/failure	2	5	10	สูง
3	Network crash/failure	2	5	10	สูง
4	External fire	2	1	2	ต่ำ
5	Workstation failure	2	2	4	ต่ำ
6	Project failure	2	2	4	ต่ำ
7	OS failure	3	2	6	ปานกลาง
8	Front office (HOSxP, PACs, LIS)	3	2	6	ปานกลาง
9	Back office (Finance)	2	2	4	ต่ำ
10	No program document / comments	2	2	4	ต่ำ
11	Vender stop support	2	2	4	ต่ำ
12	Internal flood	1	2	2	ต่ำ
13	Internal fire	1	2	2	ต่ำ

14	Electricity	3	3	9	ปานกลาง
15	Theft / Break-ins / Protest / Mob	1	2	2	ต่ำ
16	Intranet / Internet	1	2	2	ต่ำ
17	Backup error / Data loss	1	2	2	ต่ำ
18	No data dictionary / System blueprint	1	2	2	ต่ำ
19	External flood	1	1	1	ต่ำ

หมายเหตุ ประเมินเมื่อ 31 ม.ค. 2565

วิธีแก้ไขความเสี่ยง (Risk treatment)

ระดับความเสี่ยงสูง

เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม	ผู้รับผิดชอบ
1. Server crash / failure 1.1 Mysql Database เกิดความเสียหายจากการอัพเดท Version ของ Mysql	1. ลดโอกาสเกิด	1.ปรับปรุงโครงสร้างฐานข้อมูลใหม่เป็นประจำเมื่อมีการอัพเดทออกมา 2.แจ้งผู้พัฒนาโปรแกรม HOSxP ให้ปรับปรุงแก้ไขข้อผิดพลาด	ชาคริต เสนาสังข์
1.2 เกิดความเสียหายจากการอัพเดท โครงสร้างของ HOSxP	2. ลดความเสียหาย	1. สำรองข้อมูลอย่างสม่ำเสมอ 2. มีระบบฐานข้อมูลสำรองที่พร้อมใช้งานตลอดเวลา	ชาคริต เสนาสังข์
2. Network crash/failure 2.1 Switch หลักเสีย 2.2 Switch หลักเกิด IP Loop	1. ลดโอกาสเกิด	1.ใช้เครื่องสำรองไฟฉุกเฉินที่มีคุณสมบัติป้องกันไฟกระชากกับสวิตช์หลักให้ครอบคลุมทุกจุด 2.ใช้นโยบายควบคุมป้องกันการลักลอบเชื่อมต่ออุปกรณ์ที่ไม่ได้รับอนุญาตกับเครือข่ายของรพ. 3.ทบทวนและกำหนดแนวทางการควบคุมการซ่อมบำรุงสายไฟโดยช่างจากภายนอกรพ.ร่วมกับแผนกซ่อมบำรุง	ชาคริต เสนาสังข์
	2. ลดความเสียหาย	1.มีสวิตช์สำรองที่พร้อมใช้งานอย่างเพียงพอ 2.มีแบตเตอรี่สำรองเครื่องสำรองไฟฉุกเฉินที่พร้อมใช้งานอย่างเพียงพอ	ชาคริต เสนาสังข์

แผนกิจกรรมการจัดการความเสี่ยงในระบบสารสนเทศ

ชื่อกลุ่มงาน ประกันสุขภาพ และสารสนเทศทางการแพทย์ หน่วยงาน ศูนย์สารสนเทศ วันที่จัดทำ 31 ม.ค. 2565

ทรัพย์สิน	ภัยคุกคามทั้งหมดที่เป็นไปได้	แผนการจัดการ	ผู้รับผิดชอบ	งบประมาณ	ช่วงเวลาดำเนินการ
หมวด 1 ข้อมูลและเอกสารสำคัญเวชระเบียนผู้ป่วยนอกและใน	1. ข้อมูลถูกจารกรรม 2. ข้อมูลเสียหาย จากโปรแกรมที่ประสงค์ร้าย 3. ระบบเก็บข้อมูล ถูกบุกรุก 4. สถานที่เก็บข้อมูลทางกายภาพถูกบุกรุก 5. สถานที่เก็บข้อมูลทางกายภาพถูกทำลายจากภัยพิบัติ เช่น ไฟไหม้ ฟ้าผ่า	1. ตั้งค่า Firewall .ให้ครอบคลุมการป้องกัน 2. ตรวจสอบ Log อย่างสม่ำเสมอ 3. ปรับปรุงระบบให้บริการเว็บให้ทันสมัยเพื่ออุดช่องโหว่ของระบบบริการ 4. ปรับปรุงระบบปฏิบัติการให้ทันสมัย (Windows 10 patch) เพื่ออุดช่องโหว่ของระบบ 5. นโยบายด้านความปลอดภัยของข้อมูล : ผู้ใช้งาน และผู้ดูแลระบบ 6. ติดตั้งระบบกล้องวิดีโอวงจรปิด พร้อมจัดเวรยามเพื่อสังเกตการณ์ตลอด 24 ชม 7. อุปกรณ์ตรวจจับความชื้นห้องแม่ข่าย	ชาคริต เสนาสังข์ ชาคริต เสนาสังข์ ชาคริต เสนาสังข์ ทีม IT ชาคริต เสนาสังข์ ชาคริต เสนาสังข์ ชาคริต เสนาสังข์		ปี 2556-ปัจจุบัน ปี 2556-ปัจจุบัน ปี 2556-ปัจจุบัน ปี 2556-ปัจจุบัน ปี 2556-ปัจจุบัน ปี 2556-ปัจจุบัน ปี 2556-ปัจจุบัน
หมวด 2 ครุภัณฑ์ระบบสารสนเทศ 2.1 เครื่อง Server 2.1.1 Database HOSxP	1. Database structure corrupt 2. Data loss cause application (HOSxP) crash	1. ดำเนินการเฝ้าระวังฐานข้อมูลทำงานผิดพลาด และ Re up structure ทุกเดือน 2. จัดทำแผนสำรองข้อมูล 3. จัดหาคอมพิวเตอร์แม่ข่ายสำรองให้พร้อมใช้งาน(DR site) 4. แจ้งผู้พัฒนาโปรแกรม HOSxP ให้ดำเนินการปรับปรับแก้ไขข้อผิดพลาด 5. จัดระบบงานสำรองเพื่อใช้งานแทนระบบหลักที่ขัดข้อง	ชาคริต เสนาสังข์ ชาคริต เสนาสังข์ ชาคริต เสนาสังข์ ชาคริต เสนาสังข์ ชาคริต เสนาสังข์		ปี 2556-ปัจจุบัน ปี 2556-ปัจจุบัน ปี 2556-ปัจจุบัน ปี 2556-ปัจจุบัน ปี 2556-ปัจจุบัน

		ได้แก่ OPD scan viewer, HOSxP with database on notebook, PACS viewer			
		8. จัดทำแผนกู้คืนระบบงานหลักและระบบข้อมูลเมื่อเกิดความเสียหาย	ชาคริต เสนาสังข์		ปี 2556-ปัจจุบัน
2.1.2 Gateway (HOSxP LIS-PACs) server	3. ภัยพิบัติทางกายภาพ ได้แก่ ความร้อน และไฟไหม้	9. ติดตั้งถังดับเพลิงสีเขียวและสีแดงไว้บริเวณห้องคอมพิวเตอร์แม่ข่ายและห้องปฏิบัติงาน	ซ่อมบำรุง, ชาคริต		ปี 2556-ปัจจุบัน
x-ray server		10. ดำเนินการตรวจสอบความพร้อมใช้งานของถังดับเพลิงอย่างสม่ำเสมอทุกเดือน	ซ่อมบำรุง, ชาคริต		ปี 2556-ปัจจุบัน
2.1.3 Internet server	4. ระบบไฟฟ้าสำรองและระบบไฟฟ้าหลักไม่สเถียร (ไฟตกไฟดับบ่อย)	11. ติดตั้งกล้องวิดีโอวงจรปิดพร้อมจัดเวรยามเพื่อสังเกตการณ์ตลอด 24 ชม	ชาคริต		ปี 2556-ปัจจุบัน
2.1.4 Image server		12. ดำเนินการตรวจสอบประสิทธิภาพของเครื่องสำรองไฟฟ้าฉุกเฉินสำหรับเครื่องคอมพิวเตอร์แม่ข่ายอย่างสม่ำเสมอทุกเดือน	ชาคริต		ปี 2556-ปัจจุบัน
2.1.5 web server		13. ดำเนินการตรวจสอบอุณหภูมิในห้องคอมพิวเตอร์แม่ข่ายทุกวัน	ชาคริต		ปี 2556-ปัจจุบัน
2.1.6 other server	5. การถูกบุกรุกทางกายภาพและโจรกรรม (เนื่องจากในเวรดึกไมมีเจ้าหน้าที่ขึ้นปฏิบัติงานทั้งอาคารซึ่งอยู่ห่างไกลจากจุดที่มีผู้ปฏิบัติงาน และไม่มีอุปกรณ์ในการช่วยเฝ้าระวังที่มีประสิทธิภาพ)	14. จัดทำนโยบายควบคุมการทำงานของเจ้าหน้าที่ศูนย์คอมพิวเตอร์ และประกาศใช้	ชาคริต		ปี 2556-ปัจจุบัน