การจัดการความมั่นคงปลอดภัยทางข้อมูล

Information Security Management

Chapter 3 : Risk Management

เนื้อหา

- การวิเคราะห์ความเสี่ยง (Risk Analysis)
- การบริหารความเสี่ยง (Risk Management)
  - การประเมินความเสี่ยง (Risk Assessment)
  - การรักษาความเสี่ยง (Risk Treatment)

การวิเคราะห์ความเสี่ยง (Risk Analysis)

การวิเคราะห์ความเสี่ยง (Risk Analysis) หมายถึง กระบวนการทางวิทยาศาสตร์ที่มีขั้นตอนเป็นระบบ ให้เหตุผล ข้อมูลและสร้างความมั่นใจ และใช้เป็นเครื่องมือสนับสนุนการตัดสินใจเพื่อลดความเสี่ยงอันเป็นที่ยอมรับในระดับสากล การวิเคราะห์ความเสี่ยงเป็นกระบวนการที่มีองค์ประกอบหลัก 3 ส่วน คือ

1. การบริหารจัดการความเสี่ยง (Risk Management)
2. การประเมินความเสี่ยง (Risk Assessment)
3. การรักษาความเสี่ยง (Risk Treatment)

ทำไมต้องวิเคราะห์ความเสี่ยง

1. เพื่อคุ้มครอง รักษาความปลอดภัยของข้อมูลภายในองค์กร
2. เพื่อจัดระบบการควบคุมความปลอดภัยด้านข้อมูล
3. เพื่อนำมาใช้กำหนดมาตรฐานและมาตรการต่างๆ บนพื้นฐานของข้อมูลและหลักฐานทางวิทยาศาสตร์
4. เพื่อลดความเสียหายที่เกิดจากภัยคุกคามประเภทต่างๆ

การบริหารความเสี่ยง (Risk Management)

กระบวนการที่ใช้ในการบริหารจัดการ ที่จะทำให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลง หรืออยู่ในระดับที่ยอมรับได้ โดยระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดังนี้

1. การประเมินความเสี่ยง (Risk Assessment)
    - 1.1 การระบุความเสี่ยง (Risk Identification)
    - 1.2 การวิเคราะห์ความเสี่ยง (Risk Analysis)
    - 1.3 การประเมินค่าความเสี่ยง (Risk Evaluation)
2. การรักษาความเสี่ยง (Risk Treatment)
3. การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)
4. การรายงานความเสี่ยง (Risk Reporting)

การประเมินความเสี่ยง (Risk Assessment)

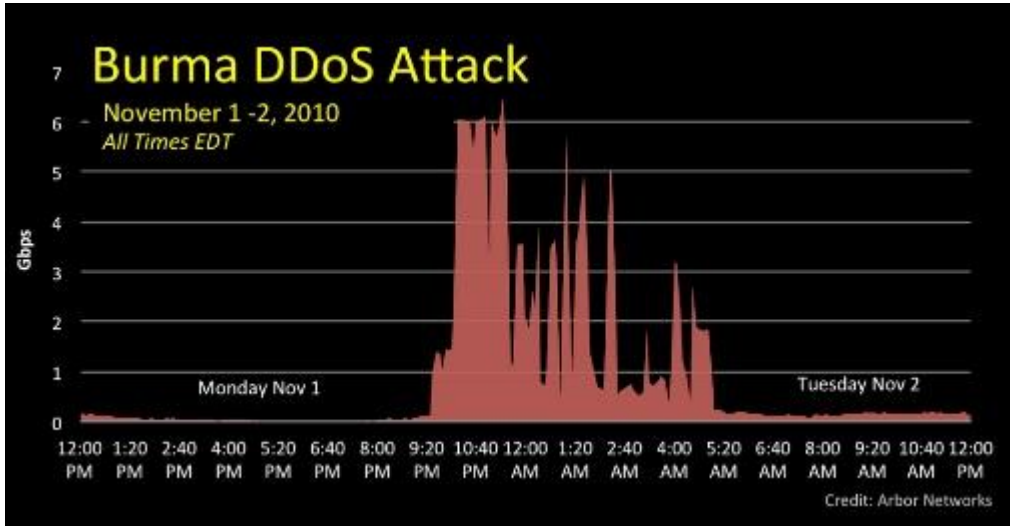
ถือเป็นขั้นตอนสำคัญในการบริหารความเสี่ยง โดยในการประเมินความเสี่ยงสามารถทำได้ 3 วิธี คือ

- การประเมินความเสี่ยงเชิงปริมาณ
- การประเมินความเสี่ยงเชิงคุณภาพ

การประเมินความเสี่ยงเชิงปริมาณ

จะใช้ค่าตัวเลขเพื่อกำหนดผลกระทบ (Impact) และโอกาสที่จะเกิดความเสี่ยง (Likelihood) โดยใช้ข้อมูลจากแหล่งต่างๆ เช่น บันทึกที่จัดเก็บไว้ ผลการดำเนินงานในอดีต ข้อมูลสถิติการโจมตี

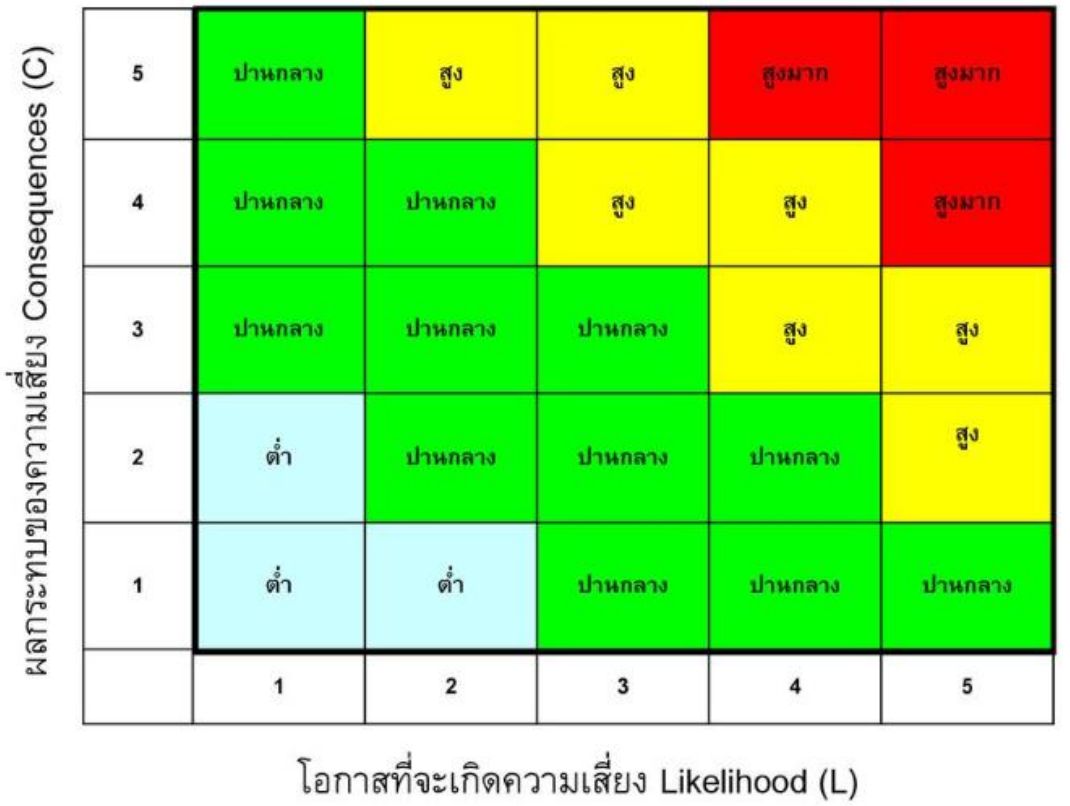
วิธีนี้มักใช้กับภาคเอกชนหรือธุรกิจ ซึ่งจะเกี่ยวข้องกับการเงิน ซึ่งหลายหน่วยงานมักใช้จำนวนเงินเป็นตัวแทนในการวิเคราห์ความเสี่ยง



การประเมินความเสี่ยงเชิงคุณภาพ

จะใช้คำอธิบายเพื่อแบ่งระดับผลกระทบ (Impact) และโอกาสที่จะเกิดความเสี่ยง (Likelihood) วิธีนี้เป็นวิธีที่ง่ายและนิยมใช้งาน ตัวอย่างระดับความเสี่ยง เช่น สูง กลาง ต่ำ

วิธีนี้มักใช้กับงานที่มีความเสียหายที่ไม่สามารถประเมิน หรือระบุเป็นเงินได้ หรือประเมินค่าได้ยาก



ขั้นตอนการประเมินความเสี่ยง

1. การระบุทรัพย์สิน (Asset Identification)
2. การระบุภัยคุกคาม (Threat Identification)
3. การระบุช่องโหว่ (Vulnerability Identification)
4. การประเมินโอกาสที่จะเกิดขึ้น (Likelihood)
5. การประเมินผลกระทบ (Impact)
6. การประเมินความเสี่ยง (Risk)

การระบุทรัพย์สิน (Asset Identification)

เป็น**กระบวนที่สำคัญ** เนื่องจากใช้ในการกำหนดขอบเขตกำหนดว่าอะไรจะทำหรือไม่ทำในระหว่างการประเมิน และระบุว่าอะไรเราจะปกป้อง

ขั้นตอนแรก คือ สำรวจว่ามีทรัพย์สินอะไรบ้าง รวมถึงการประเมินมูลค่าของทรัพย์สินเหล่านั้น ข้อมูลเหล่านี้จะช่วยให้สามารถวิเคราะห์ลำดับความสำคัญของการจัดหาระบบป้องกันได้

ประเภทของทรัพย์สิน

ประเภทของทรัพย์สิน	ตัวอย่าง
ฮาร์ดแวร์ (Hardware)	คอมพิวเตอร์ อุปกรณ์เครือข่าย มีเดียจัดเก็บข้อมูล ซีดี เทป อาคาร สถานที่ทำงาน เป็นต้น
ซอฟต์แวร์ (Software)	ระบบปฏิบัติการ แอพพลิเคชัน โปรแกรมอรรถประโยชน์ เป็นต้น
ข้อมูล (Information)	ข้อมูลทางธุรกิจ ค่าคอนฟิกกูเรชันของอุปกรณ์ต่างๆ เอกสาร ข้อมูลส่วนบุคคล ฐานข้อมูล เป็นต้น
บริการ (Services)	การเชื่อต่ออินเทอร์เน็ต การบริการด้านไอที แหล่งจ่ายไฟฟ้า เป็นต้น
บุคลากร (People)	ผู้บริหาร ฝ่ายธุรการ วิศวกร นักพัฒนาซอฟต์แวร์ ฝ่ายบุคคล เป็นต้น

การระบุภัยคุกคาม (Threat Identification)

เป็นกระบวนที่ชี้ให้เห็นถึงความเสี่ยงที่หน่วยงานเผชิญอยู่ โดยการระบุภัยคุกคามอาจพิจารณาถึงเหตุการณ์ที่เกิดขึ้นมาในอดีตหรือมีแนวโน้มว่าจะเกิดขึ้น

โดยปกติเมื่อพูดถึงภัยคุกคาม จะหมายถึง ปัจจัยจากภายนอกที่อาจเข้ามาทำลายหรือก่อให้เกิดความเสียหายต่อข้อมูลและทรัพย์สินขององค์กร เช่น

- ภัยคุกคามจากคนภายในองค์กร เช่น การฉ้อโกง การทำงานผิดพลาดโดยไม่ได้ตั้งใจ

- ภัยคุกคามจากคนภายนอกองค์กร เช่น การเจาะเข้ามาในระบบ การก่อวินาศกรรม การโจรกรรม

การระบุภัยคุกคาม (Threat Identification)

- ภัยธรรมชาติ เช่น น้ำท่วม แผ่นดินไหว ไฟไหม้ พายุ ฟ้าฝ่า

- ภัยคุกคามจากสภาพแวดล้อมที่ไม่เหมาะสม เช่น น้ำรั่วซึม ฝุ่นละออง สารเคมี อุณหภูมิร้อนเกินไป ความชื้น

การระบุช่องโหว่ (Vulnerability Identification)

เป็นกระบวนที่ระบุช่องโหว่หรือจุดอ่อน โดยปกติแล้ว**ภัยคุกคามและช่องโหว่จะถูกพิจารณาไปด้วยกัน** เพราะถ้าภัยคุกคามจากภายนอกแต่ระบบของเราไม่มีจุดอ่อน ภัยนั้นก็จะไม่สามารถทำอันตรายอะไรได้

ช่องโหว่ขององค์กรสามารถแบ่งออกเป็นประเภทต่างๆ ได้แก่

- ช่องโหว่ทางนโยบาย
- ช่องโหว่เกี่ยวกับคน
- ช่องโหว่ทางเทคนิค
- ช่องโหว่ทางกายภาพ

ช่องโหว่ทางนโยบาย

เป็นช่องโหว่ที่เกิดจากการบริหารจัดการ ซึ่งส่วนใหญ่ขาดจากขาดกฎ ระเบียบ หรือกฎหมายที่บังคับ หรือห้ามอย่างใดอย่างหนึ่ง เช่น

- นโยบายการรักษาความปลอดภัยทั่วไป
- นโยบายการรักษาความปลอดภัยข้อมูล
- คู่มือปฏิบัติงานของพนักงาน
- ผังระบบเครือข่าย

ช่องโหว่เกี่ยวกับคน

เป็นช่องโหว่ที่เกิดจากการปฏิบัติหน้าที่ของพนักงานหรือผู้รับจ้าง จนเกิดเป็นช่องโหว่ที่ทำให้ผู้ไม่หวังดีสามารถใช้ประโยชน์ได้ เช่น

- การเขียนรหัสผ่านบนกระดาษ
- การ Log on เข้าระบบทิ้งไว้แล้วตนเองไม่อยู่
- ผู้ดูแลระบบ ละเลยการตรวจเช็ค logfile ของระบบ

ช่องโหว่ทางเทคนิค

เป็นช่องโหว่ที่เกิดจากข้อผิดพลาดของการเขียนโปรแกรม หรือกำหนดค่า Config ที่ไม่สมบูรณ์หรือปลอดภัย เช่น

- ประเภทและจำนวนของระบบต่างๆ ที่ใช้ในเครือข่าย
- ลิงค์ที่เชื่อมต่อเข้ากับอินเทอร์เน็ต
- การควบคุมการเข้าถึงเราท์เตอร์
- กฎของไฟล์วอลล์จุดที่เชื่อมต่อเข้ากับระบบ

ควรใช้เครื่องมือเฉพาะด้าน Scan หาช่องโหว่ทางเทคนิค

ช่องโหว่ทางกายภาพ

เป็นช่องโหว่ที่เกิดจากการป้องกันและรักษาความปลอดภัยทางกายภาพ เช่น

- การควบคุมการเข้าออกสถานที่
- การล็อคประตูหน้าต่าง
- ระบบไฟฟ้าของสถานที่และอาคารมีแหล่งที่มาอย่างไร
- ระบบป้องกันอัคคีภัยของดาต้าเซ็นเตอร์เป็นอย่างไร

การประเมินความเสี่ยง (Risk Assessment)

การระบุความเสี่ยง (Risk Identification)

รหัส	ความเสี่ยง	ลักษณะความเสี่ยง
R01	ความเสี่ยงจากการนำอุปกรณ์ส่วนตัวมาใช้ที่ทำงาน	ผู้ใช้นำมาใช้งานที่ทำงานและเชื่อมต่อกับเครือข่าย อาจทำให้ข้อมูลรั่วไหล หรืออุปกรณ์ส่วนตัวนั้นอาจนำไวรัสมาแพร่กระจายที่ทำงาน
R02	ความเสี่ยงจากการถูก Hack	Hacker อาจเจาะเข้ามาในระบบทางอินเทอร์เน็ตเพื่อขโมยข้อมูล หรือทำให้ระบบใช้งานไม่ได้
R03	มัลแวร์แพร่กระจายในเครือข่าย	การแพร่กระจายของมัลแวร์หรือไวรัส ซึ่งอาจเข้ามาผ่านช่องทางต่างๆ
R04	ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง	เกิดไฟฟ้าขัดข้องหรือกระแสไฟฟ้าไม่คงที่ ซึ่งอาจทำให้อุปรณ์เสียหาย
R05	เครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง	อุปกรณ์ชำรุดตามอายุการใช้งาน หรือขัดข้องด้วยสาเหตุทางเทคนิค
R06	การโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	โจรกรรมเครื่องคอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้

การประเมินโอกาสที่จะเกิดขึ้น (Likelihood)

โอกาสที่จะเกิด (Likelihood)

ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	เหตุการณ์ภัยคุกคามมีโอกาสที่เกิดเกือบจะแน่นอน
4	สูง	เหตุการณ์ภัยคุกคามมีโอกาสที่เกิดสูง (4 ครั้ง/ปี)
3	ปานกลาง	เหตุการณ์ภัยคุกคามมีโอกาสที่เกิดปานกลาง (3 ครั้ง/ปี)
2	น้อย	เหตุการณ์ภัยคุกคามมีโอกาสที่เกิดน้อย (2 ครั้ง/ปี)
1	น้อยมาก	เหตุการณ์ภัยคุกคามแทบจะไม่มีโอกาสที่จะเกิด (ไม่เกิน 1 ครั้ง/ปี)

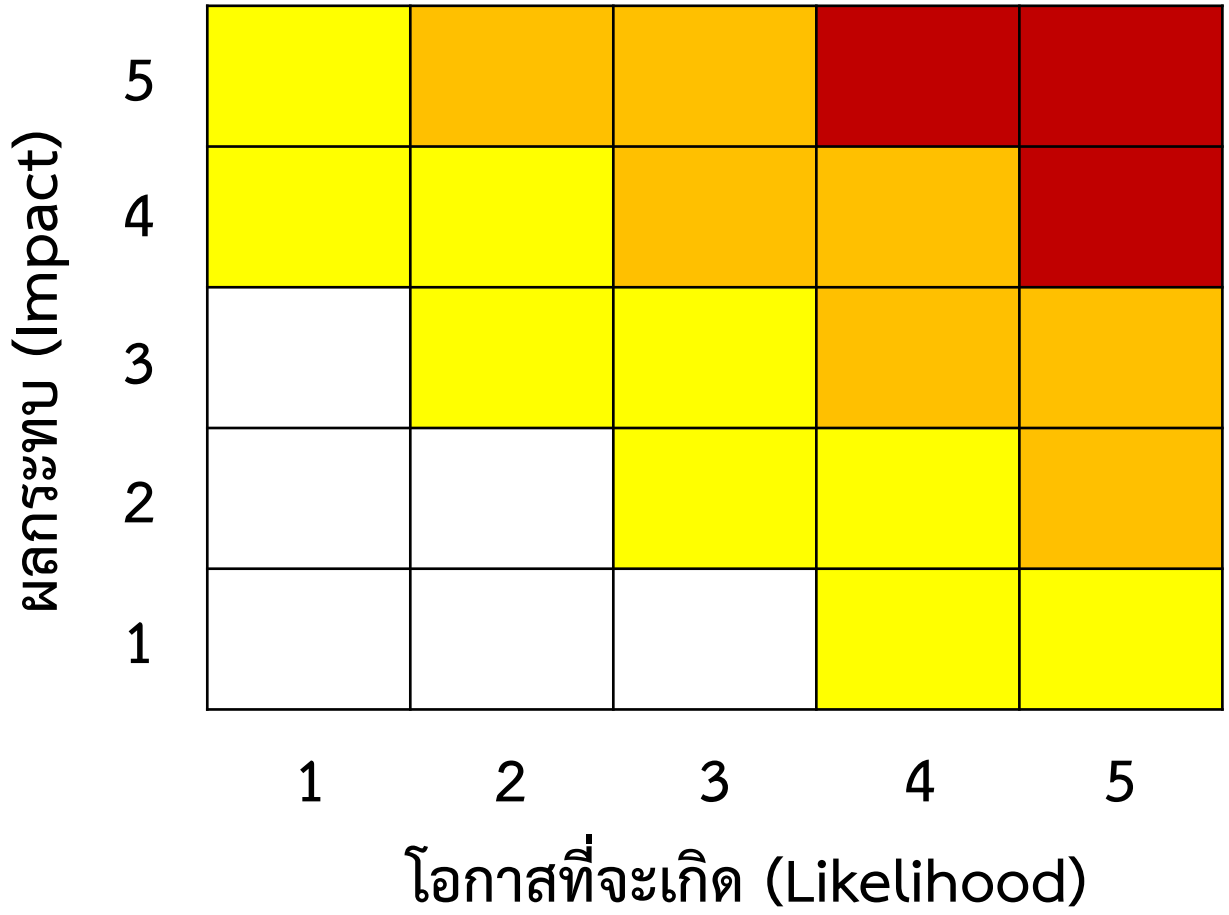
การประเมินผลกระทบ (Impact)

ผลกระทบ (Impact)

ระดับ	ผลกระทบ	คำอธิบาย
5	สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
4	สูง	เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
3	ปานกลาง	ระบบมีปัญหาและมีความสญเสียไม่มาก
2	น้อย	เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
1	น้อยมาก	เกิดเหตุร้ายที่ไม่มีความสำคัญ

การประเมินความเสี่ยง (Risk Assessment)

เกณฑ์การประเมินค่าความเสี่ยง (Risk Evaluation)



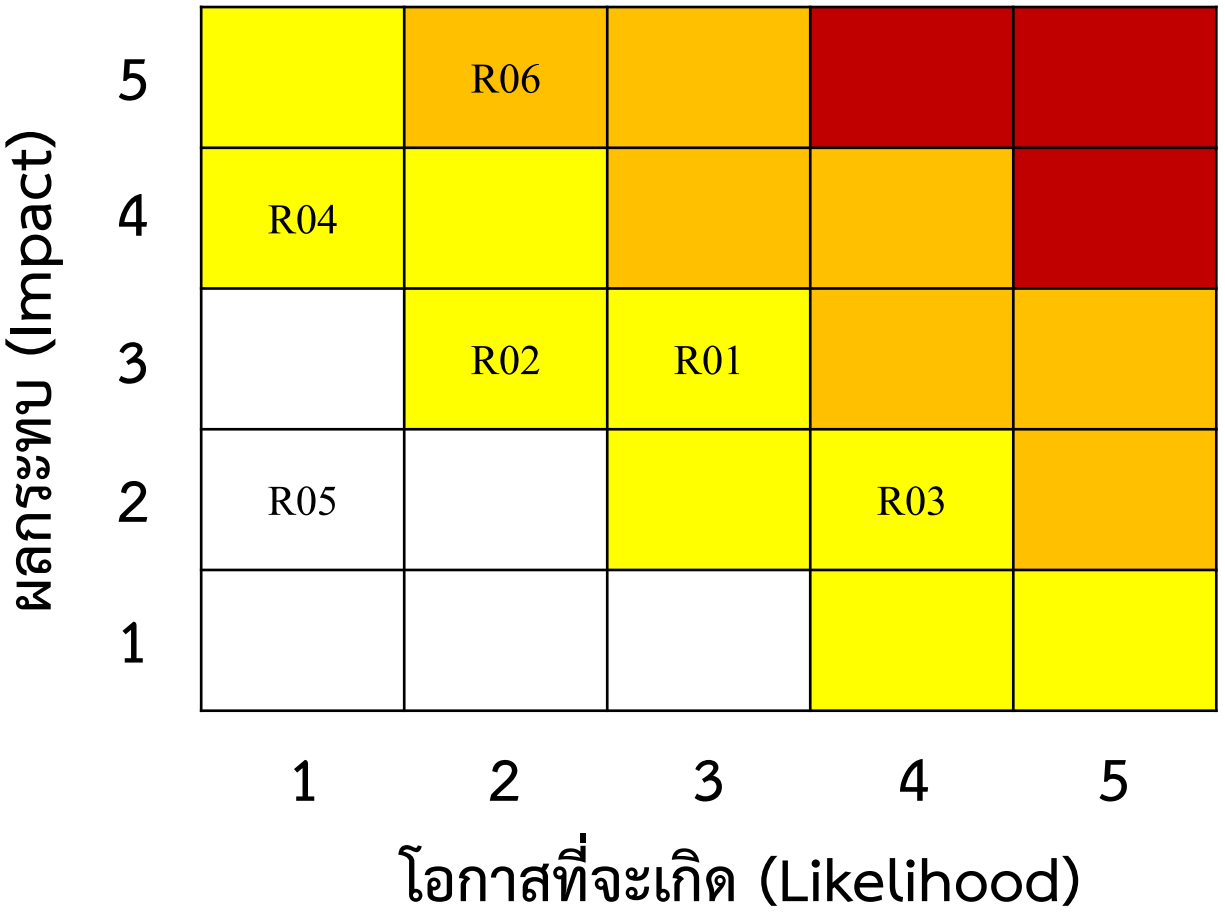
การคำนวณระดับความเสี่ยง (Risk Determination)

ตัวอย่างการคำนวณระดับความเสี่ยง (Risk Determination)

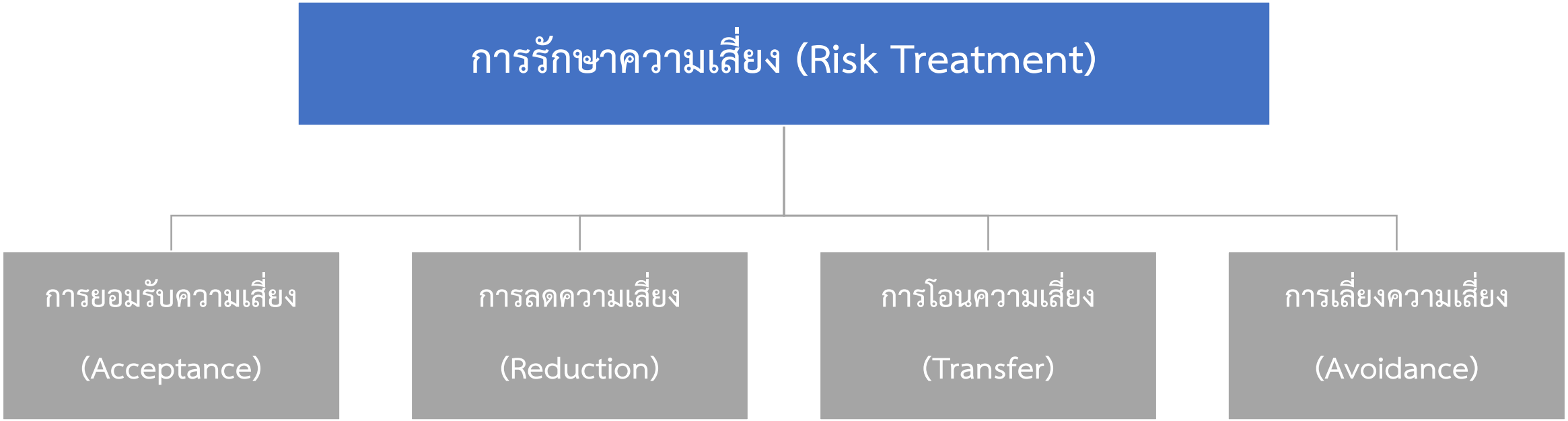
รหัส	ความเสี่ยง	ลักษณะความเสี่ยง	Likelihood	Impact
R01	ความเสี่ยงจากการนำอุปกรณ์ส่วนตัวมาใช้ที่ทำงาน	ผู้ใช้นำมาใช้งานที่ทำงานและเชื่อมต่อกับเครือข่าย อาจทำให้ข้อมูลรั่วไหล หรืออุปกรณ์ส่วนตัวนั้นอาจนำไวรัสมาแพร่กระจายที่ทำงาน	3	3
R02	ความเสี่ยงจากการถูก Hack	Hacker อาจเจาะเข้ามาในระบบทางอินเทอร์เน็ตเพื่อขโมยข้อมูล หรือทำให้ระบบใช้งานไม่ได้	2	3
R03	มัลแวร์แพร่กระจายในเครือข่าย	การแพร่กระจายของมัลแวร์หรือไวรัส ซึ่งอาจเข้ามาผ่านช่องทางต่างๆ	4	2
R04	ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง	เกิดไฟฟ้าขัดข้องหรือกระแสไฟฟ้าไม่คงที่ ซึ่งอาจทำให้อุปรณ์เสียหาย	1	4
R05	เครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง	อุปกรณ์ชำรุดตามอายุการใช้งาน หรือขัดข้องด้วยสาเหตุทางเทคนิค	1	2
R06	การโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	โจรกรรมเครื่องคอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	2	5

การประเมินความเสี่ยง (Risk Assessment)

ตัวอย่างการประเมินค่าความเสี่ยง (Risk Evaluation)



การรักษาความเสี่ยง (Risk Treatment)



การยอมรับความเสี่ยง (Acceptance)

เป็นการยอมรับในความเสี่ยงโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากอาจจะไม่สามารถทำได้ในทางปฏิบัติ หรือไม่คุ้มค่า เช่น

การพิสูจน์ตัวจริงเพียงใช้ id และ password มีความเสี่ยงเพราะอาจมีการขโมยไปใช้ได้ การให้มี ใช้ชีวมาตร (Biometrics) เช่น การตรวจลายนิ้วมือหรือม่านตา อาจมีค่าใช้จ่ายสูงไม่คุ้มค่า โรงพยาบาลอาจยอมรับความเสี่ยงของระบบปัจจุบันและทำงานต่อไปโดยไม่ทำอะไร

การลดความเสี่ยง (Reduction)

พิจารณาหาวิธีในการควบคุมแก้ไขความเสี่ยงให้ลดลงมาอยู่ในระดับที่องค์กร หรือหน่วยงานสามารถยอมรับได้ เช่น

การมีมาตรการควบคุมมากชนิดขึ้น หรือชนิดที่เข้มงวดมากขึ้นเพื่อลดความเสี่ยง เช่น การใช้ชีวมาตร (Biometrics) เพื่อใช้ในการพิสูจน์ตัวจริงนอกเหนือไปจากการใช้ id/ password ที่มีอยู่เดิม

การโอนความเสี่ยง (Transfer)

พิจารณาถ่ายโอนความเสี่ยงไปให้ผู้อื่นรับผิดชอบแทน เช่น

อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันเพียงหนึ่งปีเพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังขาย (Maintenance service) เป็นต้น

การเลี่ยงความเสี่ยง (Avoidance)

การหลีกเลี่ยงความเสี่ยงโดย ยกเลิกกระบวนการทำงานหรือทรัพย์สิน ที่ก่อให้เกิดความเสี่ยงขึ้น ซึ่งมักจะกระทำการแก้ไขความเสี่ยงด้วยวิธีอื่น เช่น

เมื่อพบว่าปัจจุบันโรงพยาบาล มีการสำรองข้อมูลเพียง 1 ชุดและจัดเป็นความเสี่ยงต่อการสูญเสีย การเลี่ยงความเสี่ยงนี้อาจ ได้แก่ การทำสำรองข้อมูล 2 ชุด และแยกเก็บในสถานที่ต่างกัน การบริหารจัดการการเชื่อมโยงสู่เครือข่ายผ่านโมเด็ม ถ้าเป็นการยากต่อการควบคุมหรือบริหารจัดการ องค์กรอาจเลือกทางออกโดยการยกเลิกไม่ให้ใช้บริการ และแนะนำให้พนักงานใช้บริการผ่านทาง ISP ในช่วงที่มีการระบาดของไวรัสอย่างหนัก องค์กรอาจมีเลือกระงับไม่ให้ใช้คอมพิวเตอร์ที่ไม่ได้ติดตั้ง Antivirus เป็นต้น

การรักษาความเสี่ยง (Risk Treatment)