การบริหารความเสี่ยงด้านไอที
(IT Risk Management)

การดำเนินการระบบสารสนเทศมีความเสี่ยงต่อการถูกกระทำจากการบุกรุก (intrusion) หรือการแสวงหาประโยชน์จากภาวะเสี่ยง (vulnerability) ที่มีอยู่ในรูปแบบต่างๆ อันอาจทำให้เกิดความเสียหายต่อสารสนเทศ (information) และทรัพยากรเทคโนโลยีสารสนเทศได้. ปัจจุบันมีการติดต่อสื่อสารระหว่างองค์กรหรือบุคลากรสามารถติดต่อกับแหล่งข้อมูลต่างๆ ผ่านระบบเครือข่ายคอมพิวเตอร์ที่มีการเชื่อมโยงออกสู่อินเทอร์เนตทำให้เพิ่มความเสี่ยงมากยิ่งขึ้น. ข้อสารสนเทศจัดเป็นสินทรัพย์อันมีค่าชนิดหนึ่งที่องค์กรใช้ในการดำเนินภารกิจและจำเป็นต้องได้รับการป้องกันอารักขาเช่นเดียวกับทรัพย์สินอื่นๆ. เครือข่ายสารสนเทศในปัจจุบันมีการเชื่อมโยงกันมากขึ้น ทำให้ระบบสารสนเทศมีความเสี่ยงต่อสิ่งคุกคามต่างๆและมีจุดอ่อนมากขึ้นตามไป. สารสนเทศนั้นอาจอยู่ในรูปของ กระดาษ, สิ่งพิมพ์, แผ่นฟิล์ม, บทสนทนา หรือสื่ออิเล็กทรอนิกส์, และมีการส่งผ่านทางไปรษณีย์หรือทางอิเล็กทรอนิกส์. ไม่ว่าจะเป็นรูปแบบใดและใช้ร่วมกันหรือส่งผ่านโดยวิธีการใดๆก็ตาม สารสนเทศเหล่านี้ควรได้รับการอารักขาอย่างเหมาะสม.

ความมั่นคงสารสนเทศ (information security) อันเป็นหลักประกันการมีสารสนเทศใช้ได้อย่างมีประสิทธิภาพ ขึ้นกับความมั่นคงและปลอดภัยของระบบสารสนเทศใน 3 ประการดังต่อไปนี้

1. <u>สภาพพร้อมใช้งาน</u> (availability) หมายถึงว่าระบบอยู่ในสภาพพร้อมที่ให้บริการได้ตลอดเวลา แม้ระบบจะมีช่วงการหยุดให้บริการตามกำหนดการ (planned downtime) ก็เป็นที่ยอมรับได้ เช่น การหยุดบริการเพื่อเปลี่ยนแปลงหรือปรับปรุงระบบฯ. แต่ไม่นับการหยุดให้บริการโดยไม่มีการวางแผนล่วงหน้า (unplanned downtime) อันเป็นผลมาจากความล้มเหลวขององค์ประกอบใดๆในระบบฯ. ตัวอย่างความล้มเหลวนี้ได้แก่ การที่เครือข่ายไม่ทำงานเพราะการคั่งในเครือข่าย, คอมพิวเตอร์ไม่ทำงานเพราะฮาร์ดแวร์หรือซอฟท์แวร์ผิดปรกติ, เครือข่ายถูกโจมตีโดยไวรัส ฯลฯ.
2. <u>บูรณภาพ</u> (integrity) ในแง่ความมั่นคงสารสนเทศ บูรณภาพมี 2 องค์ประกอบคือ บูรณภาพของข้อมูล (data integrity) และบูรณภาพของระบบฯ (system integrity). บูรณภาพของข้อมูลหมายถึงการที่สารสนเทศและโปรแกรมการใช้งานมีการเปลี่ยนแปลงภายใต้การควบคุมและตามสิทธิที่ได้รับ. บูรณภาพของระบบหมายถึงการที่ระบบฯมีสมรรถนะตามที่ควรจะเป็นและไม่มีการเปลี่ยนแปลงใดๆโดยไม่ได้รับอนุญาต. สารสนเทศรวมทั้งระบบฯมีความถูกต้องและการเปลี่ยนแปลงแก้ไขใดๆที่เกิดขึ้นล้วนเป็นไปตามสิทธิในการเข้าถึงและการแก้ไขข้อมูลตามที่กำหนดไว้. ตัวอย่างของความล้มเหลวด้านบูรณภาพนี้ได้แก่ การเข้าถึงเครือข่ายได้โดยไม่รับอนุญาต, การแก้ไขเปลี่ยนแปลงหรือลบข้อมูลโดยไม่สามารถตรวจสอบได้ว่าใครทำ, หรือการเรียกค้นซ้ำข้อมูลชุดเดิมให้ผลไม่ตรงกันเป็นต้น.
3. <u>การไม่เปิดเผยข้อมูลโดยไม่ได้รับอนุญาต</u> (confidentiality) หรือการเก็บรักษาความลับ หมายถึงการที่ผู้ใช้งานเข้าถึงข้อมูลได้ตามสิทธิที่กำหนด (authorization) เท่านั้น. ตัวอย่างความล้มเหลวด้านนี้ได้แก่การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือระบบไม่สามารถตรวจสอบได้ว่ามีใครเข้าถึงข้อมูลไปบ้างแล้ว.

เนื่องจากไม่มีเทคโนโลยีใดที่จะสามารถควบคุมพฤติกรรมของมนุษย์ได้โดยสมบูรณ์ จำเป็นต้องมีการดำเนินนโยบายความมั่นคงสารสนเทศเพื่อเป็นหลักประกันว่าระบบสามารถให้บริการโดยมีสภาพพร้อมใช้งาน บูรณการและการไม่เปิดเผยข้อมูลโดยไม่ได้รับอนุญาต. การกำหนดนโยบายที่นำไปปฏิบัติได้จริงจำเป็นต้องอาศัยทรัพยากรในด้านต่างๆ แต่เนื่องจากองค์กรโดยทั่วไปมีทรัพยากรจำกัด จึงจำเป็นต้องกำหนด

นโยบายให้สอดคล้องกับความเสี่ยงที่มีและมีนัยสำคัญต่อองค์กรนั้นๆ. นโยบายความมั่นคงสารสนเทศขององค์กรหนึ่งใดอาจใช้เป็นแนวทางสำหรับองค์กรอื่นๆได้ แต่ต้องดำเนินการอย่างจำแนกและประยุกต์ให้เหมาะสมกับบริบทขององค์กรนั้นๆ. วัตถุประสงค์ของเอกสารนี้เพื่อเป็นบทนำสู่การวิเคราะห์ความเสี่ยงอันจะนำไปสู่การกำหนดนโยบายที่เหมาะสมต่อองค์กรหนึ่งใดต่อไป.

ความเสี่ยง (risk)

ความเสี่ยงหมายถึง ความน่าจะเป็นของเหตุการณ์ใดๆ รวมกับผลที่เกิดขึ้นตามมาเมื่อเกิดเหตุการณ์นั้นจริง. ไม่ว่าจะเป็นเหตุการณ์ใดๆก็ตาม ผลที่ตามมาอาจเป็นผลดีหรือผลเสียต่อองค์กรก็ได้ แต่ในที่นี้ความเสี่ยง หมายถึงเฉพาะความน่าจะเป็นของเหตุการณ์ใดๆที่เมื่อเกิดขึ้นแล้วผลที่ตามมาส่งผลเสียหายต่อองค์กรเท่านั้น. ดังนั้นเพื่อเหลีกเลี่ยงความเสียหายอันอาจเกิดขึ้นจึงจำเป็นต้องมีการบริหารความเสี่ยง.

การบริหารความเสี่ยง (risk management)

การบริหารความเสี่ยงเป็นการบริหารจัดการเชิงกลยุทธ์ที่สำคัญขององค์กร หมายถึงกระบวนการที่มีการดำเนินการอย่างมีระเบียบวิธีในการวิเคราะห์ความเสี่ยงที่เกี่ยวข้องกับภารกิจ หรือกิจกรรมต่างๆขององค์กร เพื่อให้ภารกิจดำเนินต่อไปได้อย่างเหมาะสม.

การบริหารความเสี่ยงเป็นการชี้ระบุและบำบัดความเสี่ยง เพื่อให้ภารกิจสามารถดำเนินต่อไปได้อย่างต่อเนื่องและมีประสิทธิภาพโดยการจัดลำดับปัญหาต่างๆที่สามารถหรืออาจส่งผลต่อองค์กร. การบริหารความเสี่ยงที่เหมาะสมทำให้เกิดโอกาสสำเร็จสูงสุดในการดำเนินภารกิจ และลดโอกาสของความล้มเหลวหรือความไม่แน่นอนที่อาจมีขึ้น.

การบริหารความเสี่ยงควรเป็นกระบวนการที่มีการดำเนินการและมีการพัฒนาอยู่ตลอดเวลา เพราะเงื่อนไขปัจจัยภายนอกอาจเปลี่ยนแปลงตลอดเวลา.

ตารางที่ 1 กระบวนการบริหารความเสี่ยง

1. การประเมินความเสี่ยง (risk assessment)
A. การวิเคราะห์ความเสี่ยง (risk analysis)
A.1 การชี้ระบุความเสี่ยง (risk identification)
A.2 การบรรยายลักษณะความเสี่ยง (risk description)
A.3 การประมาณความเสี่ยง (risk estimation)
B. การประเมินค่า (risk evaluation)
2. การรายงานความเสี่ยง (risk reporting)
3. การบำบัดความเสี่ยง (risk treatment)
4. การรายงานความเสี่ยงตกค้าง (residual risk reporting)
5. การเฝ้าสังเกต (monitoring)

กระบวนการบริหารจัดการความเสี่ยง

กระบวนการนี้ประกอบด้วย 5 ขั้นตอนดังตารางที่ 1 นี้

1. การประเมินความเสี่ยง (risk assessment) ประกอบด้วยกระบวนการวิเคราะห์ความเสี่ยงและการประเมินค่าความเสี่ยง.
   a. การวิเคราะห์ความเสี่ยง (risk analysis) ประกอบด้วย 3 ขั้นตอนดังนี้

1. การชี้ระบุความเสี่ยง (risk identification)
2. ลักษณะรายละเอียดของความเสี่ยง (risk description)
3. การประมาณความเสี่ยง (risk estimation)

b. ประเมินค่าความเสี่ยง (risk evaluation)

2. การรายงานผลการวิเคราะห์ความเสี่ยง (risk reporting)
3. กระบวนการบำบัดความเสี่ยง (risk treatment)
4. การรายงานความเสี่ยงตกค้าง (residual risk reporting)
5. การเฝ้าสังเกต (monitoring)

<u>การวิเคราะห์ความเสี่ยง</u>

การวิเคราะห์ความเสี่ยงประกอบด้วย 3 กระบวนการคือ

1. <u>การชี้ระบุความเสี่ยง (risk identification)</u> เป็นการชี้ให้เห็นถึงปัญหาความไม่แน่นอนที่องค์กรเผชิญอยู่. กระบวนการนี้จำเป็นต้องอาศัยความรู้ความเข้าใจองค์กร, ภารกิจและกิจกรรม, สิ่งแวดล้อมด้านกฎหมาย สังคม การเมืองและวัฒนธรรม, พัฒนาการและปัจจัยที่มีต่อความสำเร็จขององค์กร, รวมทั้งโอกาสและสิ่งคุกคามที่มีต่อองค์กร. การชี้ระบุความเสี่ยงควรได้ดำเนินการอย่างทั่วถึงครอบคลุมกิจกรรมในทุกๆด้านขององค์กร. สาเหตุสำคัญของความเสี่ยงคือการมีสิ่งคุกคาม (threat) ที่อาจส่งผลให้เกิดการละเมิดความมั่นคงสารสนเทศและส่งผลเสียตามมา.

ตัวอย่างที่มาของสิ่งคุกคามด้านสารสนเทศ

ก. ด้านกายภาพและสิ่งแวดล้อม (physical and environmental threats)
- การปนเปื้อน (contamination) จากสารเคมี สิ่งสกปรก หรือรังสีเป็นต้น
- เหตุการณ์แผ่นดินไหว (earthquake)
- การรบกวนทางอิเล็กทรอนิกส์ (electronic interference)
- ภาวะอุณหภูมิและความชื้นสุดขั้ว (extremes of temperature and humidity) เช่นร้อนหรือเย็นหรือความชื้นสูงหรือต่ำ เกินไป
- แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้ากระเพื่อม (power supply failure or fluctuations)
- ไฟไหม้ (fire) จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง หรืออื่นๆ
- น้ำท่วม (flood) จากกระแสน้ำ ฝนตกหลังคารั่ว หรือท่อน้ำชำรุดแตก
- พายุ (storm)
- สัตว์ เช่นสัตว์กัดแทะ (vermin) ประเภทหนู และสัตว์อื่นๆเช่น แมลง เป็นต้น
- การทำลายระบบและข้อมูลโดยเจตนาร้าย (malicious destruction of data and facilities)

ข. ด้านระบบ (systems threats)
- แฮ็กเกอร์ (hackers)
- การโจมตีเพื่อห้ามการบริการ [Denial of Service (DoS) attacks]
- การแอบฟัง (eavesdropping)
- การประท้วงหยุดงานของพนักงาน (industrial action)
- คำสั่งเจตนาร้าย (malicious code)
- การอำพรางหรือสวมรอย (masquerade)
- การปฏิเสธไม่ยอมรับ (repudiation)
- การก่อวินาศกรรม (sabotage)

- การเข้าถึงข้อมูล การเข้าถึงโดยใช้โมเด็ม หรือการเปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต (unauthorized data access, dial-in access, or software changes)
- ความล้มเหลวในด้านการสื่อสารหรือการบริการภายนอก (failure of communications services or outsourced operations)
- การส่งข้อความผิดเส้นทางหรือส่งซ้ำ (misrouting/re-routing of messages)
- ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม (software/programming errors)
- ความล้มเหลวทางเทคนิค (technical failures)
- ความผิดพลาดด้านการส่งผ่านข้อมูล (transmission errors)

ค. ด้านการบริหารจัดการ (administrative threats)

- การสังคมวิศวกรรม (social engineering)
- การลักทรัพย์และการฉ้อฉล (theft and fraud)
- การใช้โปรแกรมละเมิดลิขสิทธิ์ (use of pirated software)
- การแทรกซอนเว็บไซต์ (web site intrusion)

การชี้ระบุความเสี่ยงอาจพิจารณาถึงเหตุการณ์หรือสิ่งที่เคยเกิดขึ้นมาแล้วในอดีตกับองค์กรนั้น หรือองค์กรอื่นใด หรืออาจเป็นสิ่งที่มีความเป็นไปได้ว่าจะเกิดขึ้นแม้ไม่เคยเกิดขึ้นมาก่อนก็ได้. กระบวนการในชี้ระบุความเสี่ยงอาจใช้วิธีการต่างๆ ร่วมกันดังนี้ เช่น

1. การระดมสมอง (brain storming)
2. การออกแบบสอบถาม (questionnaire)
3. การวิเคราะห์กระบวนการทำงานหรือกิจกรรมในภารกิจ (business process analysis)
4. การวิเคราะห์สภาพการณ์เหตุการณ์ละเมิดความมั่นคง (scenario analysis)
5. การประชุมเชิงปฏิบัติการด้านการประเมินความเสี่ยง (risk assessment workshop)
6. การสืบสวนเหตุการณ์ละเมิดความมั่นคงสารสนเทศ (incident investigation)
7. การตรวจสอบและการตรวจสภาพระบบ (auditing and inspection)
8. การวิเคราะห์ HAZOP (hazard and operability studies)
9. การวิเคราะห์สถานการณ์ (SWOT analysis)

2. <u>ลักษณะรายละเอียดของความเสี่ยง (description of risk)</u>

เมื่อชี้ระบุความเสี่ยงได้แล้วพึงบรรยายรายละเอียดและลักษณะของความเสี่ยงนั้น เช่น

ตารางที่ 2 รายละเอียดของความเสี่ยงเพื่อประกอบการทำรายงาน

ชื่อความเสี่ยง (name)	การละเมิดหลักปฏิบัติด้านรหัสผ่าน
ขอบเขต (scope)	มีการเขียน id/password ติดไว้ตามโต๊ะทำงานในห้องทำงานและหอผู้ป่วย
ลักษณะความเสี่ยง (nature)	การฝ่าฝืนหลักปฏิบัติความมั่นคงสารสนเทศ
ผู้ที่ส่วนได้เสีย	ผู้ใช้งานระบบ ฐานข้อมูลในระบบ
ลักษณะเชิงประมาณ	รุนแรงมากและพบได้ประปราย (แสดงเป็นแมทริกซ์, ตารางที่ 3)
การยอมรับความเสี่ยง	องค์กรยอมรับความเสี่ยงได้น้อยมาก เพราะการเปลี่ยนแปลงหรือทำลายข้อมูลอาจมีผลทางคดีหรือกฎหมายหรือชีวิตผู้ป่วย
การบำบัดและการ	การบำบัดและกลไกการควบคุม เช่น การรายงานและตักเตือน การบังคับ

ควบคุม	เปลี่ยนรหัสผ่านตามกำหนดเวลา การใช้ PIN กำกับ
แนวทางการปรับปรุง	แนวทางปฏิบัติเพื่อแก้ไข ได้แก่การมีมาตรการและการฝึกอบรม การให้หัวหน้างานลาดตระเวนดูเหตุ
การพัฒนากลยุทธ์และนโยบาย	กลยุทธ์และการพัฒนานโยบาย เช่น สร้างความตื่นตัวเรื่องความมั่นคงสารสนเทศ การสัมมนา การทำคดีศึกษา และอื่นๆ

3. <u>การประมานความเสี่ยง (risk estimation)</u>

ขั้นตอนนี้เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (incident) หรือเหตุการณ์ (event) ว่ามีมากน้อยเพียงไรและผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด

โอกาส หรือ ความน่าจะเป็น (probability) หรือความบ่อยครั้งของการเกิดเหตุหรือเหตุการณ์ อาจแบ่งแบบง่ายๆเป็น 5 ระดับจากน้อยไปหามาก เช่น

- บ่อย (frequent) พบได้บ่อยครั้งเป็นประจำ
- ประปราย (probable)
- ตามโอกาส (occasional)
- น้อยครั้งมาก (remote)
- แทบไม่เกิดเลย (improbable)

ความรุนแรงของสิ่งที่เกิดขึ้นตามมา (severity of consequence) อาจแบ่งเป็น 4 ระดับคือ

- สูงมาก (severe)
- สูง (high)
- ปานกลาง (moderate)
- ต่ำ (low)

โดยทั่วไปนิยมใช้การทำตาราง 2 มิติ แล้วนำเสนอว่าปัญหาความเสี่ยงนั้นอยู่ในย่านใดของตาราง.

ตารางที่ 3 Risk Assessment Matrix

Severity Level	Probability of Occurrence				
	Frequent	Probable	Occasional	Remote	Improbable
Severe	**(1)**	**(1)**	**(1)**	**(2)**	**(3)**
High	**(1)**	**(1)**	**(2)**	**(2)**	**(3)**
Moderate	**(1)**	**(2)**	**(2)**	**(3)**	**(3)**
Low	**(3)**	**(3)**	**(4)**	**(4)**	**(4)**

(1) เหตุการณ์ไม่พึงประสงค์ที่ต้องได้รับการแก้ไขทันที
(2) เหตุการณ์ไม่พึงประสงค์ที่ต้องแก้ไขทันทีแต่ฝ่ายบริหารต้องตัดสินใจว่าจะทำวิธีใดและอย่างไร
(3) เหตุการณ์ที่ยอมรับได้แต่ต้องผ่านการรับรู้หรือตัดสินใจของฝ่ายบริหาร
(4) เหตุการณ์ที่ยอมรับได้โดยไม่ต้องให้ฝ่ายบริหารตัดสินใจ

ตัวอย่าง

(1) เหตุการณ์ไม่พึงประสงค์ที่ต้องลงมือแก้ไขทันที เช่น การที่เครือข่ายมีสภาพล้มเหลวเพราะมีวงวน (loop) เกิดขึ้น, คอมพิวเตอร์แม่ข่ายมี power supply เพียงตัวเดียวที่ใช้การได้ พึงดำเนินการหา power supply สำรองมาให้ได้โดยทันที, หรือมีข่าวประกาศว่าไวรัสตัวใหม่ระบาด จำเป็นต้องหา virus profile มา update ในระบบทันที เป็นต้น.

(2) เหตุการณ์ไม่พึงประสงค์ที่ต้องแก้ไขทันทีแต่ฝ่ายบริหารต้องตัดสินใจว่าจะทำวิธีไหนอย่างไร เช่น database server มีเนื้อที่เหลือน้อย ถ้า disk เต็มจะทำให้ระบบไม่สามารถบริการได้. ฝ่ายบริหารอาจพิจารณาตัดสินใจในแง่การดำเนินการโดยการ หา disk มาเพิ่ม, เปลี่ยนแปลงระบบและขนาดของ RAID, หา server ใหม่มาเปลี่ยน ฯลฯ.

(3) เหตุการณ์ที่ยอมรับได้แต่ต้องผ่านการรับรู้หรือตัดสินใจของฝ่ายบริหาร เช่น การเปิดโปรแกรมการใช้งานทิ้งไว้โดยเดินเครื่องเปล่า (idle) ที่เกิน 15 นาที ระบบจะปิดโปรแกรมโดยอัตโนมัติและบุคลากรจะต้องทำการ login ใหม่. ฝ่ายบริหารอาจรับรู้ในหลักการและอาจมีข้อคิดเห็นในแง่ของระยะเวลาอาจสั้นหรือยาวกว่า 15 นาที.

(4) เหตุการณ์ที่ยอมรับได้ไม่ต้องให้ฝ่ายบริหารตัดสินใจ เช่น ผู้ใช้งานระบบอาจทำรหัสผ่านหาย. เมื่อเกิดขึ้นก็ทำตามหลักปฏิบัติ เช่น ไปรายงานตัวพร้อมบัตรประจำตัว ณ หน่วยงานไอที เพื่อยกเลิกรหัสผ่านเดิมและออกรหัสผ่านให้ใหม่ เป็นต้น.

<u>การประเมินค่าความเสี่ยง (risk evaluation)</u>

เมื่อได้ความเสี่ยง โดยมีรายละเอียด, การประมาณเชิงกึ่งปริมาณเป็นแมทริกซ์แล้ว จึงนำมาประเมินค่าความเสี่ยงโดยการเปรียบเทียบกับหลักเกณฑ์ความเสี่ยงที่ยอมรับได้ เช่น.

หลักเกณฑ์ยอมรับความเสี่ยง (risk acceptance criteria) ว่าจะยอมรับได้มากน้อยเพียงใดเพื่อประกอบการตัดสินใจว่าจะบำบัดความเสี่ยงนั้นๆต่อไปอย่างไร พึงพิจารณาในแง่ต่างๆดังต่อไปนี้ เช่น

- ค่าใช้จ่าย ประโยชน์และความคุ้มทุนที่จะได้รับจากการแก้ไขบำบัดความเสี่ยง (costs and benefits)
- ข้อกำหนดด้านกฎหมายและกฎระเบียบขององค์กร (legal requirements)
- ปัจจัยด้านเศรษฐกิจและสังคม (socioeconomic factors)
- ปัจจัยด้านสิ่งแวดล้อม (environmental factors)
- ประเด็นสาระสำคัญในมุมมองของผู้มีส่วนได้เสีย (concerns of stakeholders)
- อื่นๆ

<u>การรายงานผลการวิเคราะห์ความเสี่ยง (risk reporting)</u>

เมื่อประเมินความเสี่ยงแล้วเสร็จจำเป็นต้องออกรายงานการประเมินเป็นเอกสารที่ผู้อื่นสามารถอ่านได้. เอกสารนี้จะเป็นสาระสำคัญในการสื่อสารให้บุคลากรทั้งองค์กรได้รับรู้. รายงานประกอบด้วยรายละเอียดอย่างน้อยตามตารางที่ 2. การออกรายงานมีวัตถุประสงค์ให้ส่วนต่างๆได้รับรู้ดังต่อไปนี้.

ฝ่ายบริหาร ควรได้ข้อมูลการรายงานเพื่อวัตถุประสงค์ดังต่อไปนี้ เช่น

- รับรู้นัยสำคัญของความเสี่ยงที่องค์กรเผชิญอยู่
- เข้าใจผลที่กระทบต่อผู้มีส่วนได้เสียต่างๆในกรณีที่เกิดมี เหตุ หรือ เหตุการณ์และเกิดผลเสียต่อภารกิจและผลประกอบการ
- ดำเนินการเพื่อสร้างความตระหนักในปัญหาความเสี่ยงให้เกิดการรับรู้ทั่วทั้งองค์กร
- เข้าใจผลกระทบที่อาจมีต่อความมั่นใจของผู้ส่วนได้เสีย

- ให้แน่ใจว่ากระบวนการบริหารความเสี่ยงกำลังเป็นไปอย่างได้ผล
- ออกนโยบายบริหารความเสี่ยงที่มีเนื้อหาด้านปรัชญาและความรับผิดชอบของหน่วยงานและบุคลากรต่างๆในการบริหารความเสี่ยง

หัวหน้างาน ควรได้ข้อมูลการรายงานเพื่อวัตถุประสงค์ดังต่อไปนี้ เช่น

- ตระหนักในความเสี่ยงอันเกี่ยวข้องกับภาระหน้าที่ของตน ผลกระทบที่อาจมีต่อหน่วยงานอื่นหรือกิจกรรมอื่นในองค์กร
- มีดัชนีชี้วัดสมรรถนะของกิจกรรมในหน่วยงานเพื่อดูว่าระบบงานของตนเองได้รับผลกระทบจากความเสี่ยงมากน้อยเพียงใด
- รายงานผลกระทบจากความเสี่ยงในกรณีเกิดหรือจะเกิดเหตุและเสนอแนะแนวทางการแก้ไข
- รายงานความเสี่ยงใดๆที่เกิดใหม่หรือความล้มเหลวใดๆในมาตรการการควบคุมหรือป้องกันอารักขาสารสนเทศที่มีอยู่

ผู้ปฏิบัติงาน ควรได้ข้อมูลการรายงานเพื่อวัตถุประสงค์ดังต่อไปนี้ เช่น

- เข้าในบทบาทภาระหน้าที่และความรับผิดชอบในความเสี่ยงแต่ละรายการ
- เข้าใจบทบาทในการดำเนินการพัฒนาอย่างต่อเนื่องด้านการบริหารความเสี่ยง
- เข้าใจการบริหารความเสี่ยงและความตระหนักต่อความเสี่ยงในการเป็นวัฒนธรรมองค์กรที่สำคัญอย่างหนึ่ง

<u>กระบวนการบำบัดความเสี่ยง (risk treatment)</u>

เมื่อผู้บริหารได้รับรายงานการประเมินความเสี่ยงแล้วจำเป็นต้องทำการตัดสินใจ โดยพิจารณาจากหลักเกณฑ์การยอมรับความเสี่ยงที่องค์กรมีอยู่ว่าจะยอมรับโดยไม่ทำอะไร หรือจะดำเนินการบำบัดความเสี่ยง ซึ่งได้แก่กระบวนการดังต่อไปนี้

1. การยอมรับความเสี่ยง (acceptance) เป็นการยอมรับในความเสี่ยงโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เช่น การพิสูจน์ตัวจริงเพียงใช้ id/password มีความเสี่ยงเพราะอาจมีการขโมยไปใช้ได้. การให้มีใช้ชีวมาตร (biometrics) เช่น การตรวจลายนิ้วมือหรือม่านตา อาจมีค่าใช้จ่ายสูงไม่คุ้มค่า. โรงพยาบาลอาจยอมรับความเสี่ยงของระบบปัจจุบันและทำงานต่อไปโดยไม่ทำอะไร.
2. การเลี่ยงความเสี่ยง (avoidance) การหลีกเลี่ยงความเสี่ยง เช่น เมื่อพบว่าปัจจุบันโรงพยาบาลมีการสำรองข้อมูลเพียง 1 ชุดและจัดเป็นความเสี่ยงต่อการสูญเสีย การเลี่ยงความเสี่ยงนี้อาจได้แก่การทำสำรองข้อมูล 2 ชุดและแยกเก็บในสถานที่ต่างกัน. การบริหารจัดการการเชื่อมโยงสู่เครือข่ายผ่านโมเด็ม ถ้าเป็นการยากต่อการควบคุมหรือบริหารจัดการ องค์กรอาจเลือกทางออกโดยการยกเลิกไม่ให้ใช้บริการ และแนะนำให้พนักงานใช้บริการผ่านทางไอเอสพี. ในช่วงที่มีการระบาดของไวรัสอย่างหนัก องค์กรอาจมีเลือกระงับไม่ให้ใช้คอมพิวเตอร์ที่ไม่ได้ติดตั้ง antivirus เป็นต้น.
3. การโอนย้ายความเสี่ยง (transfer) เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังขาย (maintenance service) เป็นต้น.

4. การลดความเสี่ยง (reduction) ได้แก่การมีมาตรการควบคุมมากชนิดขึ้น หรือชนิดที่เข้มงวดมากขึ้นเพื่อลดความเสี่ยง เช่น การใช้ชีวมาตร (biometrics) เพื่อใช้ในการพิสูจน์ตัวจริงนอกเหนือไปจากการใช้ id/password ที่มีอยู่เดิม.

การรายงานความเสี่ยงตกค้าง (residual risk reporting)

เมื่อมีการบำบัดความเสี่ยงแล้ว จำเป็นต้องมีการรายงานและทบทวนอยู่เสมอเพื่อดูว่ามีการประเมินและการประเมินค่าความเสี่ยงอยู่ตลอดเวลา และดูว่ามาตรการควบคุมต่างๆที่ออกมาใช้ได้ผลหรือไม่เพียงไร. วิธีการมาตรฐานที่ใช้กันโดยทั่วไป คือการมีหน่วยงานภายในหรือภายนอกทำการตรวจสอบโดยกระบวนการ IT auditing ที่เหมาะสม. เนื่องจากสิ่งแวดล้อมและกฎระเบียบมีพลวัตรและการเปลี่ยนแปลงเกิดขึ้นตลอดเวลา จึงจำเป็นต้องมีการบริหารความเสี่ยงและการตรวจสอบเป็นประจำ.

การเฝ้าสังเกต (monitoring)

กระบวนการเฝ้าสังเกตเป็นหลักประกันว่า องค์กรมีมาตรการต่างๆที่จำเป็นและเหมาะสมสำหรับการบริหารความเสี่ยงต่างๆ และมาตรการเหล่านั้นมีผู้ปฏิบัติตามและบังเกิดผลจริง. ดังนั้นกระบวนการเฝ้าสังเกตพึงพิจารณาว่า

- ได้มีการปฏิบัติตามมาตรการต่างๆและบังเกิดผล
- กระบวนงานที่กำหนดขึ้นมาสามารถปฏิบัติได้จริง
- มีการเรียนรู้เกิดขึ้นในหน่วยงานอันเป็นผลมาจากการบริหารความเสี่ยง

บทสรุป

การประเมินความเสี่ยงเป็นขั้นตอนสำคัญที่เลี่ยงไม่ได้ ผลการวิเคราะห์ความเสี่ยงคือตัวชี้นำในการกำหนดนโยบายและการดำเนินการด้านความมั่นคงสารสนเทศ ถ้าไม่ทำการวิเคราะห์ความเสี่ยงให้เป็นประจำตามระยะเวลาที่กำหนดไว้องค์กรก็ไม่สามารถรู้ได้ว่าปัญหามีอะไรบ้าง การกำหนดนโยบายความมั่นคงสารสนเทศโดยไม่มีผลการวิเคราะห์ความเสี่ยงชี้นำ ก็เป็นการนโยบายที่ไม่มีหลักการและย่อมไม่ส่งผลดีต่อความมั่นคงสารสนเทศขององค์กร. องค์กรที่ดำเนินการด้านสารสนเทศโดยไม่มีนโยบายความมั่นคง หรือมีเกิดความล้มเหลวเพราะนโยบายไม่มีสิ่งชี้นำ อาจนำไปสู่ระบบสารสนเทศที่ไม่สามารถดำเนินการได้โดยมีสภาพพร้อมใช้งาน บูรณการและการเก็บรกษาความลับที่เหมาะสม. ระบบสารสนเทศที่มีอาจส่งผลให้เกิดความเสียหายด้านความปลอดภัยต่อชีวิตและทรัพย์สินของผู้มีส่วนได้เสีย อีกทั้งอาจเป็นสาเหตุที่ทำให้เกิดภาวะเสี่ยงต่อการฟ้องร้องดำเนินคดีได้.

เอกสารอ้างอิง

1. Risk Management Standard © AIRMIC, ALARM, IRM: 2002. Downloaded from http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf, November 2005.
2. Information technology — Security techniques — Code of practice for information security management. INTERNATIONAL STANDARD: ISO/IEC 17799, Second edition, 2005-06-15.
3. Rebecca Herold. Practical Guide to Managing Risks. Realtimepublications.com
4. An Introduction to Computer Security: The NIST Handbook. NIST Special Publication 800-12, 1996.
5. Risk Management Guide for Information Technology System. NIST Special Publication 800-30, 2001.

ดำรงศักดิ์ บุลยเลิศ
เรียบเรียง
พฤศจิกายน 2548

รายละเอียดของความเสี่ยงเพื่อประกอบการทำรายงาน

ชื่อความเสี่ยง (name)	
ขอบเขต (scope)	
ลักษณะความเสี่ยง (nature)	
ผู้ที่ส่วนได้เสีย (stakeholders)	
ลักษณะเชิงประมาณ (quantitative nature)	
การยอมรับความเสี่ยง (risk acceptance)	
การบำบัดและการควบคุม (treatment & control)	
แนวทางการปรับปรุง (improvement guideline)	
การพัฒนากลยุทธ์และนโยบาย (strategy and policy development)	