

ความสำคัญในการบริหารความเสี่ยง ขององค์กรสำหรับข้อมูลสารสนเทศ



ธวัชชัย ศิริขวัญชัย *

(Risk Management in Information System)

ต่อจากฉบับที่แล้ว



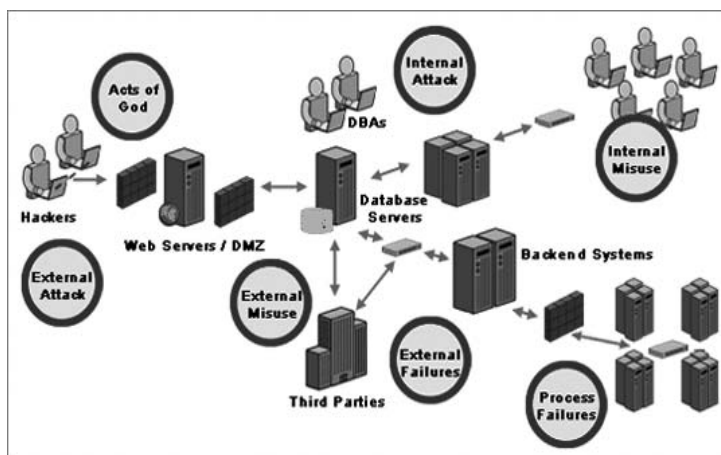
>>> สำหรับการบริหารความเสี่ยงของข้อมูลสารสนเทศ ในการประเมินความเสี่ยง (Risk Assessment) นั้น องค์กรทั้งหลายมักใช้การประเมินความเสี่ยงในการตรวจสอบขอบเขตของความเสี่ยงและภัยคุกคามที่สัมพันธ์กับระบบสารสนเทศ ซึ่งมักรวมไปถึงช่วงชีวิตของการพัฒนาระบบ (SDLC: System Development Life Cycle) ด้วย ซึ่งผลที่ได้จากกระบวนการนี้ช่วยให้สามารถหาวิธีการควบคุมที่เหมาะสมสำหรับการลดหรือกำจัดความเสี่ยงที่เกิดขึ้นได้เป็นอย่างดี เนื่องจากความเสี่ยงเป็นฟังก์ชันของโอกาสที่จะเกิดเหตุการณ์ใดๆ ที่ก่อให้เกิดภัยคุกคามในระบบที่มีการป้องกันอ่อนแอกับความรุนแรงของผลกระทบที่จะเกิดขึ้นจากภัยคุกคามนั้น ดังนั้นในการตรวจสอบโอกาสที่จะเกิดเหตุการณ์หรือภัยคุกคามหนึ่งๆ ในอนาคตที่มีต่อระบบข้อมูลขององค์กรนั้น ก็จะมาวิเคราะห์ที่ความอ่อนแอและวิธีการควบคุมของระบบกับผลกระทบที่เกิดขึ้น ซึ่งจะพิจารณาจากความรุนแรงเป็นสำคัญ

วิธีการประเมินความเสี่ยงสามารถแบ่งเป็น 9 ขั้นตอน ดังนี้ (จากแหล่งข้อมูล: National Institute of Standards

and Technology Special Publication 800-30, Risk Management Guide for Information Technology Systems, (2002), PP. 8-26)

1. การอธิบายลักษณะของระบบ (System Characterization)
2. การบ่งชี้ภัยคุกคาม (Threat Identification)
3. การบ่งชี้ความไม่มั่นคง (Vulnerability Identification)
4. การวิเคราะห์การควบคุม (Control Analysis)
5. การตรวจสอบโอกาสในการเกิดภัยคุกคาม (Likelihood Determination)
6. การวิเคราะห์ผลกระทบ (Impact Analysis)
7. การตรวจสอบความเสี่ยง (Risk Determination)
8. การเสนอวิธีการควบคุม (Control Recommendations)
9. การทำเอกสารสรุปผล (Result Documentation)

ในที่นี้จะขอยกตัวอย่างถึงการวิเคราะห์ภัยคุกคามที่มีต่อระบบข้อมูลสารสนเทศ จากที่กล่าวมาแล้วก็จะไปวิเคราะห์ที่ความอ่อนแอ ไม่มั่นคงของสภาพแวดล้อมของระบบ ซึ่งจะใช้เป็นตัวการบ่งชี้ความไม่มั่นคง (Vulnerability Identification) นั่นเอง เป้าหมายของขั้นตอนนี้คือการพัฒนารายการความไม่มั่นคงของระบบที่ทำให้ระบบมีโอกาสได้รับภัยคุกคาม



* อาจารย์คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีไทย-ญี่ปุ่น

ตัวอย่างความไม่มั่นคงของระบบซึ่งก่อให้เกิดภัยคุกคามแสดงดังตารางข้างล่าง

ความไม่มั่นคง (Vulnerability)	แหล่งกำเนิดภัยคุกคาม (Threat-Source)	ปฏิกิริยาภัยคุกคาม (Threat-Action)
ไม่มีการลบข้อมูลของพนักงานที่ออกจากบริษัทไปแล้วจากระบบ	พนักงานที่หมดสภาพการเป็นพนักงานของบริษัท	การแอบเข้ามาดึงข้อมูลสำคัญของบริษัทโดยการต่อโมเด็มเข้ามาในบริษัท
ไฟร์วอลล์ (Firewall) ของบริษัทอนุญาตให้มีการ telnet จากนอกองค์กรได้และการอนุญาตให้รหัสผู้ใช้ทั่วไป (Guest ID) เข้าใช้เครื่องเซิร์ฟเวอร์ได้	ผู้ใช้ที่ไม่ได้รับอนุญาต เช่น นักเจาะระบบ, พนักงานที่หมดสภาพการเป็นพนักงานของบริษัท	การ Telnet เข้ามายังเครื่องเซิร์ฟเวอร์และการเข้าใช้ข้อมูลด้วยรหัสผู้ใช้งานทั่วไป
ศูนย์กลางข้อมูลใช้ระบบพ่นน้ำเพื่อป้องกันเพลิงไหม้ แต่ไม่มีอุปกรณ์กันน้ำสำหรับอุปกรณ์ไฟฟ้าและเอกสารข้อมูลต่างๆ	แหล่งกำเนิดเพลิงไหม้, บุคคลที่เพิกเฉยไม่ให้ความใส่ใจ	ระบบน้ำฉีดพ่นทำงานเมื่อเกิดเพลิงไหม้



จากตัวอย่างข้างต้น ด้วยความคิดเชิงเปรียบเทียบตอนนี้องค์กรของคุณตกอยู่ในความเสี่ยงหรือไม่ครับ?

หากผู้อ่านต้องการข้อมูลเพิ่มเติมหรือคำปรึกษาใดๆ โปรดติดต่อได้ที่ฝ่ายบริการวิชาการ คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีไทย-ญี่ปุ่น

แหล่งข้อมูล: National Institute of Standards and Technology
Special Publication 800-30, Risk Management Guide for Information Technology Systems, (2002), PP. 8-26



www.tni.ac.th



สถาบันเทคโนโลยีไทย-ญี่ปุ่น
Thai-Nichi Institute of Technology 泰日工業大学
TNI สอนบัณฑิต ผลิตบัณฑิต

สถาบันเทคโนโลยีไทย-ญี่ปุ่น หรือ TNI เป็นสถาบันระดับอุดมศึกษาแห่งใหม่ มุ่งผลิตบุคลากรที่เชี่ยวชาญเฉพาะทางสนองตอบความต้องการของภาคอุตสาหกรรมไทย เพียบพร้อมด้วยคณาจารย์ผู้ทรงคุณวุฒิ อุปกรณ์เทคโนโลยีการศึกษาอันทันสมัย และมุ่งเน้นการเรียนการสอนภาษาญี่ปุ่นและภาษาอังกฤษ

จุดเด่นของสถาบัน

- ผลิตนักศึกษาที่มีความเชี่ยวชาญทั้งภาคทฤษฎีและภาคปฏิบัติ
- มีงานจริงในสถานประกอบการ เมื่อศึกษาจบแล้วมีโอกาสได้งานทำทันที
- เน้นผลิตนักศึกษาที่สามารถสื่อสารภาษาญี่ปุ่นและภาษาอังกฤษได้ดี
- มีโครงการแลกเปลี่ยนคณาจารย์และนักศึกษากับมหาวิทยาลัยในประเทศญี่ปุ่น
- มีหลักสูตรต่อเนื่องระดับปริญญาตรี และหลักสูตรปริญญาโทเรียนภาคพิเศษวันเสาร์-อาทิตย์

หลักสูตรระดับปริญญาตรี

คณะวิศวกรรมศาสตร์ : - สาขาวิศวกรรมยานยนต์ - สาขาวิศวกรรมการผลิต - สาขาวิศวกรรมคอมพิวเตอร์

คณะเทคโนโลยีสารสนเทศ : - สาขาเทคโนโลยีสารสนเทศ

คณะบริหารธุรกิจ : - สาขาการจัดการอุตสาหกรรม - สาขาบริหารธุรกิจ (ญี่ปุ่น)



หลักสูตรระดับปริญญาโท

หลักสูตรบริหารธุรกิจมหาบัณฑิต : - สาขาการจัดการอุตสาหกรรม - สาขาการจัดการวิสาหกิจสำหรับผู้บริหาร



สอบถามข้อมูลและสมัครเข้าศึกษาต่อได้ที่

สถาบันเทคโนโลยีไทย-ญี่ปุ่น 1771/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทร. 0-2763-2600 E-mail: tniinfo@tni.ac.th Website: www.tni.ac.th