Thammasat Business School tbs

รส.201 ระบบสารสนเทศเพื่อการจัดการ

หลักสูตร 2552

การรักษาความมั่นคงระบบสารสนเทศ และจริยธรรมเบื้องต้น

Section 06 ผศ.วันชัย ขันดี

หัวข้อ

- ประเภทของบุคคลที่เกี่ยวข้องกับความเสี่ยงของระบบสารสนเทศ
- ประเภทของความเสี่ยงของระบบสารสนเทศ
- การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
- จริยธรรม

ความเสี่ยงของระบบสารสนเทศ

- ความเสี่ยงของระบบสารสนเทศ (Information system risk) หมายถึง เหตุการณ์หรือการกระทำใดๆ ที่ก่อให้เกิดการสูญเสียหรือทำลายฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล สารสนเทศ หรือความสามารถในการประมวลผลข้อมูลของระบบ

ประเภทของบุคคลที่เกี่ยวข้องกับความเสี่ยงของระบบสารสนเทศ

- แฮกเกอร์ (Hacker)
- แครกเกอร์ (Cracker)
- มือใหม่หัดเขียน (Script Kiddie หรือ Skiddie)
- ผู้สอดแนม (Spies)
- เจ้าหน้าที่ขององค์กร (Employees)
- ผู้ก่อการร้ายทางคอมพิวเตอร์ (Cyberterrorist)

ประเภทของความเสี่ยงของระบบสารสนเทศ

- การโจมตีระบบเครือข่าย (Network attack)
  - การโจมตีขั้นพื้นฐาน (Basic Attacks) เช่น กลลวงทางสังคม (Social engineering) และการล้อค้นเอกสารทางคอมพิวเตอร์จากที่ทิ้งขยะ (Dumpster Diving)
  - การโจมตีด้านคุณลักษณะ (Identity Attacks) เช่น DNS Spoofing และ e-mail spoofing
  - การปฏิเสธการให้บริการ (Denial of Service หรือ DoS) เช่น Distributed denial-of-service (DDoS) , DoSHTTP (HTTP Flood Denial of Service)

ประเภทของความเสี่ยงของระบบสารสนเทศ (ต่อ)

- การโจมตีระบบเครือข่าย (ต่อ)
  - การโจมตีด้วยมัลแวร์ (Malware) - โปรแกรมมุ่งร้ายที่โจมตีการปฏิบัติงานของคอมพิวเตอร์ หรือข้อมูลส่วนบุคคล เช่น
    - ไวรัส (Viruses)
    - ตัวหนอน (Worms)
    - ม้าไม้เมืองทรอย (Trojan horse)
    - สปายแวร์ (Spyware)
    - แอดแวร์ (Adware)
    - โปรแกรมแอบเก็บข้อมูลที่คีย์ (Key loggers)
    - พิชชิง (Phishing)

ประเภทของความเสี่ยงของระบบสารสนเทศ (ต่อ)

- การเข้าถึงระบบโดยไม่ได้รับอนุญาต (Unauthorized access) หมายถึงการใช้คอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์โดยไม่มีสิทธิ ซึ่งส่วนมากจะเป็นการใช้คอมพิวเตอร์หรือข้อมูลในเครื่องคอมพิวเตอร์เพื่อทำกิจกรรมบางอย่างที่ผิดกฎระเบียบของกิจการหรือการกระทำที่ผิดกฎหมาย

ประเภทของความเสี่ยงของระบบสารสนเทศ (ต่อ)

- การลักขโมย (Theft)
  - การขโมยฮาร์ดแวร์และการทำลายฮาร์ดแวร์เช่นการตัดสายเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์
  - ขโมยซอฟต์แวร์อาจอยู่ในรูปของการขโมยสื่อจัดเก็บซอฟต์แวร์ การลบโปรแกรมโดยตั้งใจ และการทำสำเนาโปรแกรมอย่างผิดกฎหมาย
  - การขโมยสารสนเทศ เช่นการขโมยข้อมูลที่เป็นข้อมูลปกปิดส่วนบุคคลหรือความลับทางธุรกิจ

ประเภทของความเสี่ยงของระบบสารสนเทศ (ต่อ)

- ความล้มเหลวของระบบสารสนเทศ (System failure) ที่ทำให้ไม่สามารถใช้ระบบได้ตามปกติ อาจมีสาเหตุมาจาก
  - สัญญาณรบกวน(Noise) - ทำให้เครื่องทำงานผิดพลาด
  - แรงดันไฟฟ้าต่ำเกินไป (Undervoltages) - เครื่องทำงานผิดพลาดหรือเครื่องดับ
  - แรงดันไฟฟ้าสูงเกินไป (overvoltages) – ทำให้เครื่องเสียหาย
  - คอมพิวเตอร์เสีย
  - ไฟฟ้าดับ

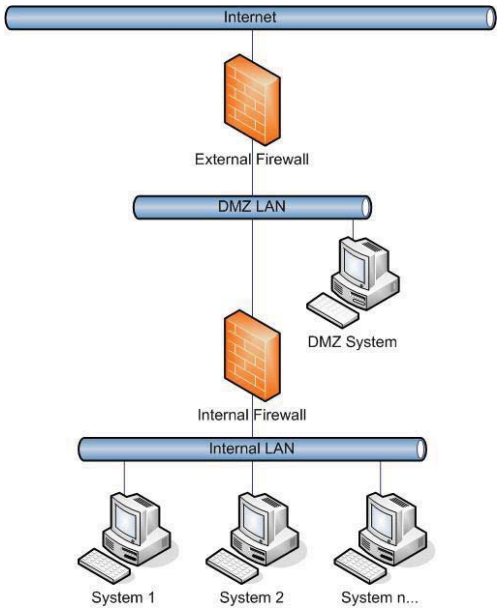
ประเภทของความเสี่ยงของระบบสารสนเทศ (ต่อ)

- ภัยพิบัติ (Disaster) ภัยที่เกิดจากธรรมชาติ
  - แผ่นดินไหว
  - เพลิงไหม้
  - น้ำท่วม
  - ซึนามิ
  - แผ่นดินถล่ม

การรักษาความมั่นคงระบบสารสนเทศ

- การรักษาความมั่นคงปลอดภัยการโจมตีระบบเครือข่าย
  - ติดตั้งโปรแกรมป้องกันไวรัสและปรับปรุง Virus signature หรือ Virus definition
  - ติดตั้งไฟร์วอลล์ (Firewall)
  - ติดตั้งซอฟต์แวร์ตรวจจับการบุกรุก (Intrusion detection software)
  - ติดตั้ง Honeypot

Firewall & Demilitarized Zone (DMZ)



การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (ต่อ)

- การควบคุมการเข้าถึงระบบโดยไม่ได้รับอนุญาต
  - การระบุตัวตน (Identification)
  - การพิสูจน์ตัวจริง (Authentication) เช่น รหัสผ่าน (Password)
    - ข้อมูลที่ทราบเฉพาะบุคคลที่เป็นเจ้าของ (What you know)
    - ใช้บัตรผ่านที่มีลักษณะเป็นบัตรประจำตัว (What you have) เช่น บัตร ATM เป็นต้น
    - ลักษณะทางกายภาพของบุคคล (What you are) เช่น ม่านตา เป็นต้น

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (ต่อ))

- การควบคุมการขโมย
  - ควบคุมการเข้าถึงทางกายภาพ (Physical access control) เช่น การปิดห้องและหน้าต่าง เป็นต้น
  - กิจการบางแห่งนำระบบ Real time location system (RTLS) มาใช้เพื่อระบุสถานที่ที่มีความเสี่ยงสูงโดยนำ RFID tags ติดที่อุปกรณ์คอมพิวเตอร์เพื่อใช้ในการติดตามอุปกรณ์นั้นๆ
  - ปัจจุบันมีการออกแบบเครื่องคอมพิวเตอร์ให้สามารถควบคุมการเปิดเครื่องและการเข้าใช้งานเครื่องด้วยการใช้ลักษณะทางกายภาพของบุคคล เช่น ลายนิ้วมือ เป็นต้น

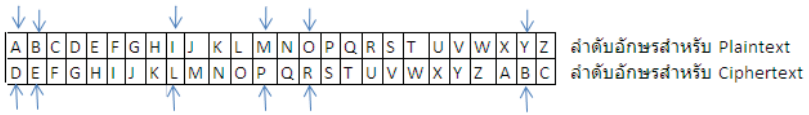
การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (ต่อ)

- การควบคุมการขโมย (ต่อ)
  - การรักษาความปลอดภัยของซอฟต์แวร์ทำโดยเก็บรักษาแผ่นซอฟต์แวร์ในสถานที่มีการรักษาความปลอดภัย
  - ในกรณีที่มีโปรแกรมเมอร์ลาออกหรือถูกให้ออก ต้องควบคุมและติดตามโปรแกรมเมอร์ทันที (Escort)

การรักษาความปลอดภัยของระบบสารสนเทศ (ต่อ)

- การเข้ารหัสลับ (Encryption) คือกระบวนการในการแปลงข้อมูลที่อยู่ในรูปที่คนทั่วไปสามารถอ่านได้ (Plain text) ให้อยู่ในรูปที่อ่านไม่รู้เรื่อง (Cipher text)
- การถอดรหัสลับ (Decryption) เป็นกระบวนการในการแปลงข้อมูลที่ผ่านการเข้ารหัสลับมาแล้ว (cipher text) กลับไปเป็นข้อมูลธรรมดาที่สามารถอ่านได้ (plain text)
- องค์ประกอบของการเข้ารหัส
  - Plain text
  - Algorithm
  - Secure key

วิธีการเข้ารหัสแบบสลับตำแหน่ง



ถ้า Plaintext เป็น I am a boy

Ciphertext จะเป็น L dp d erb

การรักษาความปลอดภัยของระบบสารสนเทศ (ต่อ)

- การรักษาความมั่นคงปลอดภัยอื่นๆ
  - Secure sockets layer (SSL) โดยเว็บเพจที่ใช้ SSL จะขึ้นต้นด้วย https แทนที่จะเป็น http
  - Secure HTTP (S-HTTP) เช่น ระบบธนาคารออนไลน์จะใช้ S-HTTP
  - Virtual private network (VPN)
- การควบคุมความล้มเหลวของระบบสารสนเทศ
  - การป้องกันแรงดันไฟฟ้าใช้ Surge protector หรือ Surge suppressor
  - ไฟฟ้าดับใช้ Uninterruptible power supply (UPS)
  - กรณีระบบสารสนเทศถูกทำลายจนไม่สามารถให้บริการได้ การควบคุมทำโดยการจัดทำแผนการทำให้กลับคืนสู่สภาพเดิมจากภัยพิบัติ (Disaster Recovery – DR) หรือ Business continuity planning (BCP)

การรักษาความปลอดภัยของระบบสารสนเทศ (ต่อ)

การสำรองข้อมูล (Data Backup) เป็นการทำสำเนาข้อมูลจากเครื่องที่ใช้งานไปเก็บไว้ในที่ปลอดภัย เผื่อว่า hard disk หรือคอมพิวเตอร์ได้รับความเสียหาย หรือข้อมูลถูกลบหรือได้รับความเสียหายด้วยเหตุใดก็ตาม จะได้นำข้อมูลที่เก็บสำรองไว้มาใส่กลับลงไปในคอมพิวเตอร์ให้ใช้งานได้อีกครั้ง

การรักษาความปลอดภัยของระบบสารสนเทศ (ต่อ)

สิ่งที่ต้องตัดสินใจเกี่ยวกับการสำรองข้อมูลประกอบด้วย

1. เลือกสื่อบันทึก (Media) ที่จะทำการสำรองข้อมูล เช่น CD DVD หรือ Portable Hard disk s หรือเทปเป็นต้น
2. ระยะเวลาที่ใช้ในการเก็บข้อมูลสำรอง
3. ความถี่ในการสำรองข้อมูล ขึ้นอยู่กับระยะเวลาสูงสุดที่ระบบจะไม่สามารถให้บริการได้โดยไม่ส่งผลต่อการดำเนินงานปกติขององค์กร
4. สถานที่จัดเก็บสื่อบันทึกที่สำรองข้อมูล ซึ่งสามารถจัดเก็บไว้สถานที่เดียวกับที่ติดตั้งคอมพิวเตอร์ (On Site) หรือ นำไปเก็บสถานที่อื่น (Offsite) ซึ่งแต่ละประเภทมีข้อดีและข้อเสียแตกต่างกันออกไป
5. สำรองข้อมูลโดยอัตโนมัติ หรือ ต้องใช้คนคอยสั่งและควบคุมการสำรอง

การรักษาความปลอดภัยของระบบสารสนเทศ (ต่อ)

- การรักษาความปลอดภัยของแลนไร้สาย (Wireless LAN)
  - ควบคุมการเชื่อมโยงเข้าสู่แลนไร้สายด้วย Service Set Identifier (SSID)
  - กลั่นกรองผู้ใช้งานด้วยการกรองหมายเลขการ์ดเน็ตเวิร์ก (MAC Addressing Filtering)
  - การเข้ารหัสและถอดรหัสด้วยวิธีการ Wired Equivalency Privacy (WEP)
  - จำกัดขอบเขตพื้นที่ให้บริการด้วยการควบคุมกำลังส่งของแอ็กเซสพอยน์
  - การพิสูจน์สิทธิเข้าใช้งานแลนไร้สายด้วย Radius Server (ไม่กล่าวในรายละเอียด)
  - การสร้าง Virtual Private Network (VPN) บนแลนไร้สาย (ไม่กล่าวในรายละเอียด)
  - การป้องกันด้วยวิธี Wi-Fi Protected Access (WPA) (ไม่กล่าวในรายละเอียด)

จริยธรรม (Ethics)

- จริยธรรมทางคอมพิวเตอร์ คือหลักปฏิบัติที่แสดงให้เห็นถึงความรู้สึกผิดชอบเกี่ยวกับการใช้ระบบสารสนเทศ ซึ่งประกอบด้วย
  - การใช้คอมพิวเตอร์และเครือข่ายโดยไม่ได้รับอนุญาต
  - การขโมยซอฟต์แวร์ (การละเมิดลิขสิทธิ์)
  - ความถูกต้องของสารสนเทศ เช่น การตกแต่งรูปภาพ เป็นต้น
  - สิทธิ์ต่อทรัพย์สินทางปัญญา (Intellectual property rights)
  - จรรยาบรรณ (Code of conduct)
  - การปกปิดข้อมูลส่วนบุคคล (Information privacy)

จริยธรรม(ต่อ)

- คำถามอย่างกว้างขวางเกี่ยวกับลิขสิทธิ์ดังนี้
  - บุคคลสามารถ Download ส่วนประกอบของเว็บไซต์ ต่อจากนั้นปรับปรุง แล้วนำไปแสดงบนเว็บในนามของตนเองได้หรือไม่
  - เจ้าหน้าที่ของมหาวิทยาลัยสามารถพิมพ์เอกสารบนเว็บและกระจายให้นักศึกษาเพื่อใช้สำหรับการเรียนการสอนได้หรือไม่
  - บุคคลสามารถสแกนรูปภาพหรือหนังสือ ต่อจากนั้นนำไปลงในเว็บซึ่งอนุญาตให้คน Download ได้หรือไม่
  - บุคคลสามารถสามารถนำเพลงใส่ในเว็บได้หรือไม่
  - นักศึกษาสามารถนำข้อสอบหรือโครงการต่าง ๆ ที่อาจารย์กำหนดในชั้นเรียนเข้าไปใส่ในเว็บเพื่อให้นักศึกษาคนอื่น ๆ ลอกโครงการนั้นแล้วส่งอาจารย์ว่าเป็นงานของตนได้หรือไม่

จริยธรรม (ต่อ)

- จรรยาบรรณคือสิ่งที่เขียนเป็นลายลักษณ์อักษรเพื่อเป็นแนวทางในการตัดสินใจว่าการกระทำใดที่เกี่ยวข้องกับคอมพิวเตอร์เป็นสิ่งที่มีหรือไม่มีจริยธรรม หลักปฏิบัติมีดังนี้
  - ต้องไม่ใช้คอมพิวเตอร์ในการทำอันตรายบุคคลอื่น
  - ต้องไม่รบกวนการทำงานทางคอมพิวเตอร์ของคนอื่น
  - ต้องไม่เข้าไปยุ่งเกี่ยวกับแฟ้มข้อมูลของคนอื่น
  - ต้องไม่ใช้คอมพิวเตอร์ในการขโมย
  - ต้องไม่ใช้คอมพิวเตอร์เพื่อให้หลักฐานที่เป็นเท็จ
  - ต้องไม่สำเนาหรือใช้ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์
  - ต้องไม่ใช้ทรัพยากรทางคอมพิวเตอร์ของผู้อื่นโดยไม่ได้รับอนุญาต

จริยธรรม (ต่อ)

- จรรยาบรรณ (ต่อ)
  - ต้องไม่ใช้ทรัพสินทางปัญญาของผู้อื่นเหมือนเป็นของตน
  - ต้องคำนึงถึงผลกระทบทางสังคมของโปรแกรมที่ออกแบบ
  - ต้องใช้คอมพิวเตอร์ในทางที่แสดงให้เห็นถึงความเคารพในมนุษย์แต่ละคน

จริยธรรม (ต่อ)

- การปกปิดข้อมูลส่วนบุคคล เป็นการรักษาความลับเกี่ยวกับข้อมูลที่เกี่ยวกับตัวบุคคล ไม่ว่าจะเป็นข้อมูลพนักงานขององค์กรหรือข้อมูลเกี่ยวกับลูกค้า
- ตัวอย่างแนวปฏิบัติที่ระมัดระวังไม่ให้ข้อมูลส่วนบุคคลรั่วไหล
  - เก็บข้อมูลในที่ปลอดภัย มีการควบคุมการเข้าถึง ให้เข้าถึงได้เฉพาะบุคคลที่มีอำนาจหน้าที่ที่เกี่ยวข้องเท่านั้น
  - ยกเลิกการเปิดบริการแบ่งปันข้อมูล (File sharing) หรือเครื่องพิมพ์ก่อนการเชื่อมต่ออินเทอร์เน็ต
  - ติดตั้งไฟร์วอลล์ส่วนบุคคล
  - ติดตั้งโปรแกรม Anti-spam

กฎหมายของไทยที่เกี่ยวข้องระบบสารสนเทศ

- **พรบ.ลิขสิทธิ์ พ.ศ.๒๕๓๗**
- **พรบ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔**
- **พรบ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐**