030523114 Network Security

สาขาวิชาเทคโนโลยีอิเล็กทรอนิกส์ (ต่อเนื่อง)

ภาควิชาเทคโนโลยีวิศวกรรมอิเล็กทรอนิกส์

วิทยาลัยเทคโนโลยีอุตสาหกรรม

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

อาจารย์ ดร.เลอสรรค์ กิรสมุทรานนท์

ครั้งที่ 14 “Physical Security”

Physical Security

- **Outline**
  - Intro Physical Security
  - แนวทางความปลอดภัยทางกายภาพของระบบ
  - แนวทางความปลอดภัยทางกายภาพภายใน
  - 10 Physical security Measures
  - ตัวอย่างมาตรฐานการรักษาความปลอดภัยในพื้นที่ IT
  - สรุป

Intro
Physical Security

- ระบบรักษาความปลอดภัยภายนอกระบบงาน (Physical Security)

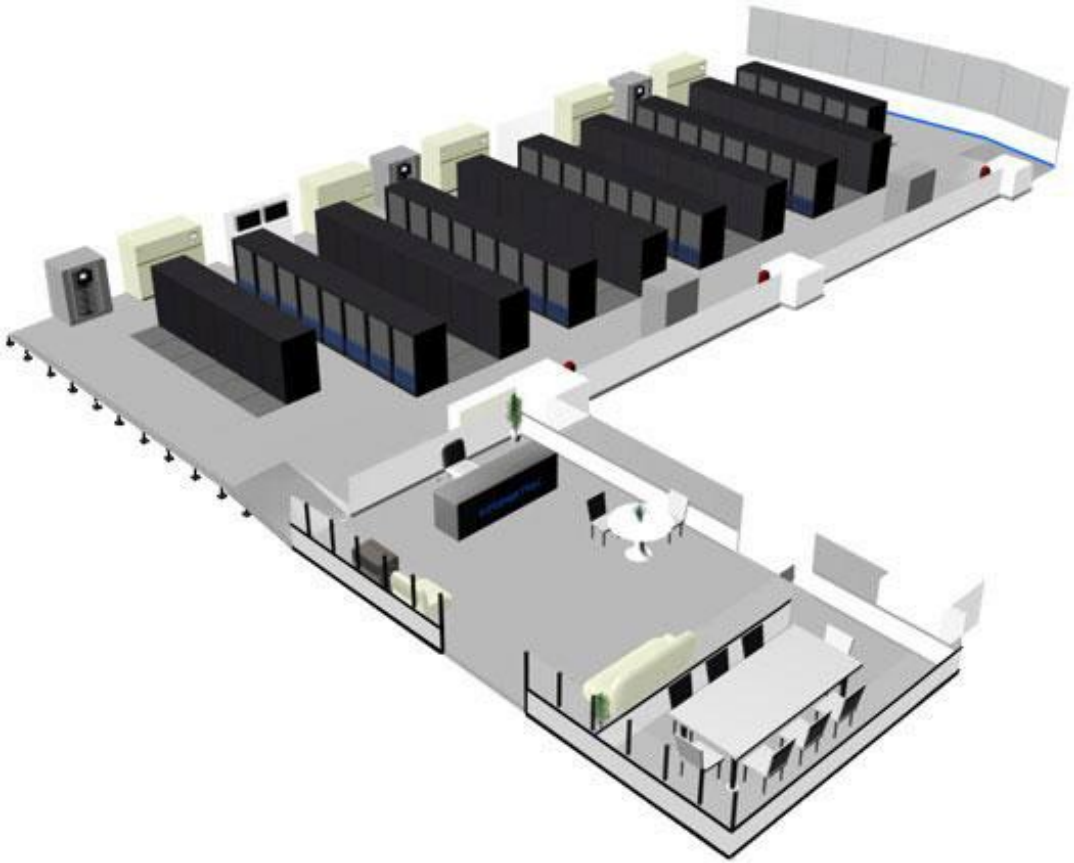
ระบบรักษาความปลอดภัยในส่วนนี้จะกระทากันภายนอกระบบงานคอมพิวเตอร์ ตัวอย่างเช่น การล็อกห้องคอมพิวเตอร์ เป็นต้น

- ระบบรักษาความปลอดภัยภายในระบบงาน (System Security And Integrity) การกระจายอานาจการใช้ข้อมูลออกไป (Distribution System) ของระบบงาน ทาให้ระบบจาเป็นที่จะต้องมีระบบการรักษาความปลอดภัยภายในระบบงานอย่างดีพอ

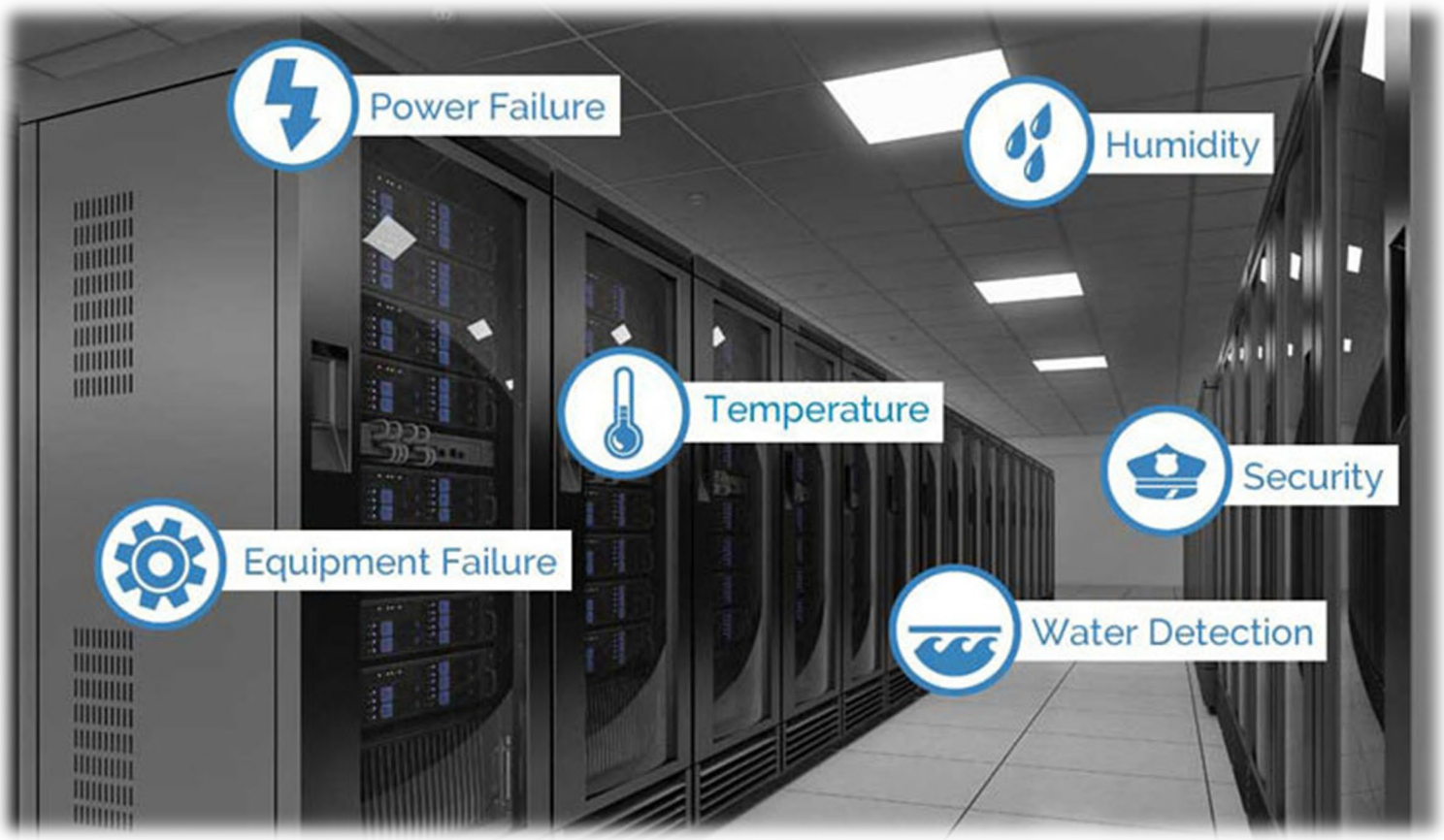
Physical Security
แนวทางความปลอดภัยทางกายภาพของระบบ

- แบ่งแยกพื้นที่ควบคุมความปลอดภัยอย่างชัดเจน
- ใช้ระบบป้องกันและตรวจสอบการเข้าออก
- เก็บรักษาระบบและอุปกรณ์ต่าง ๆ ในพื้นที่รักษาความปลอดภัย
- ใช้เครื่องจ่ายกาลังไฟฟ้าสำรอง
- วางแผนสำหรับการกู้ระบบคืน
- ตรวจสอบข้อมูลของเจ้าหน้าที่จากภายนอกที่เข้ามา

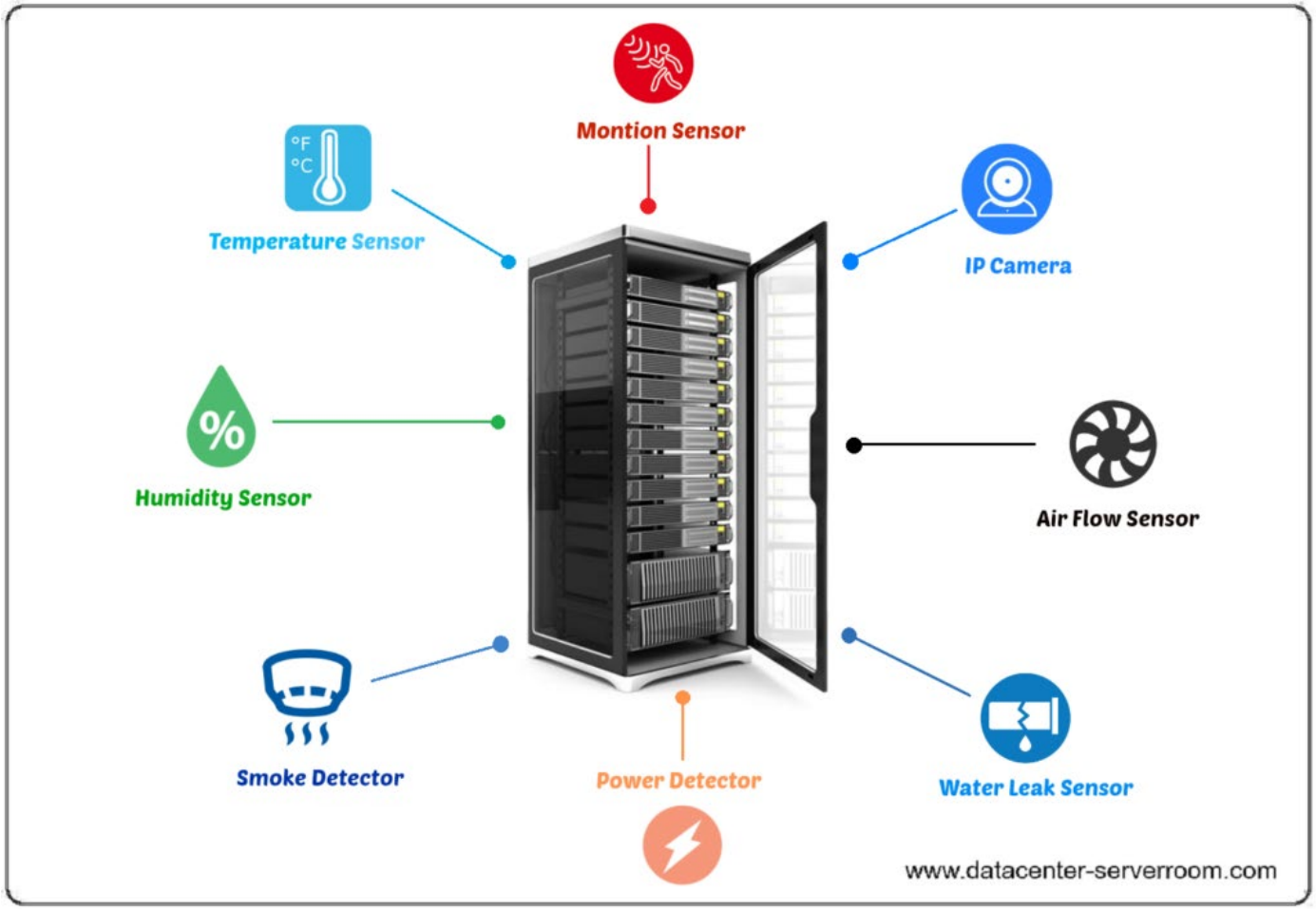
Physical Security
แนวทางความปลอดภัยทางกายภาพของระบบ



Physical Security
แนวทางความปลอดภัยทางกายภาพของระบบ



Physical Security
แนวทางความปลอดภัยทางกายภาพของระบบ



Physical Security
แนวทางความปลอดภัยทางกายภาพของระบบ

Physical Security
แนวทางความปลอดภัยทางกายภาพภายใน

- การล็อคเครื่องคอมพิวเตอร์
- การรักษาความปลอดภัยใน BIOS
- การรักษาความปลอดภัยที่ Boot Loader
- การล็อคหน้าจอมอนิเตอร์
- การตรวจสอบการเปลี่ยนแปลงของความปลอดภัยทางกายภาพ
- ล็อกไฟล์ที่ไม่สมบูรณ์หรือที่มีข้อมูลขาดหายไป
- ฯลฯ

Physical Security

10 Physical security Measures

- ล็อคห้องเก็บเซิร์ฟเวอร์ (Server)
- มีการเฝ้าระวังการเข้า-ออกอย่างเข้มงวด
- อุปกรณ์ที่เป็นจุดอ่อนต้องเก็บไว้ในห้องที่ปิดล็อค
- ตั้ง Server ไว้บน Rack
- อย่าลืมเวิร์คสเตชั่น (นำเครื่องที่ไม่ได้ใช้งานออกจากระบบ)
- ไม่ให้ผู้บุกรุกหรือบุคคลภายนอกเปิดตู้ได้
- ป้องกันคอมพิวเตอร์ Lap Top หรือ Note Book (ขโมยง่าย มีข้อมูลภายใน ล๊อคโดยคล้องห่วง)
- สำรองข้อมูล
- ทำให้หน่วยขับเคลื่อนความจำไม่ทำงาน (USB port, ect.) ถอดสาย ใช้โปรแกรม
- ป้องกันปริ้นเตอร์ (หน่วยความจำชั่วคราว และช่องทางเชื่อมต่อ)

Summary

Remember that network security starts at the physical level. All the firewalls in the world won’t stop an intruder who is able to gain physical access to your network and computers, so lock up as well as lock down.

Physical Security
สำหรับพื้นที่ควบคุมเพื่อความปลอดภัย

- ข้อบังคับทั่วไปเพื่อความปลอดภัย
- ลานจอดรถ (Parking)
- มีโทรทัศน์วงจรปิด (Close Circuit TV)
- มีแสงสว่างพอเพียงและมีระบบไฟฟ้าสำรอง
- ล็อคทางเข้า (Entrance) และทางออก (Exit)
- ผู้มาติดต่อต้องแสดงบัตร
- อนุญาตให้ใช้อุปกรณ์หรือเครื่องมือบางอย่างเฉพาะเจ้าหน้าที่เท่านั้น
- แผนการทดสอบฉุกเฉิน
- การฝึกอบรม

Physical Security
สำหรับพื้นที่ควบคุมเพื่อความปลอดภัย

- มาตรฐานการรักษาความปลอดภัยในเขตควบคุมระบบ IT
- อยู่ในอาคารห่างจากหน้าต่าง
- Floor Plan ไม่ระบุจุดที่ตั้งของทรัพย์สินที่สำคัญ
- Sound Transmission Class 40
- มีระบบป้องกันไฟระบบท่อแบบแห้ง
- รักษาทางเข้าเขตควบคุม
- ผู้มาติดต่อ ห่างจากเขตควบคุมไม่ต่ำกว่า 50 ฟุต
- ข้อมูล Back up ที่สำคัญหรืออ่อนไหวมากให้เก็บภานนอกห้องนี้
- ฯลฯ

SOUND TRANSMISSION CLASS

STC	Performance	Description
50 - 60	Excellent	Loud sounds heard faintly or not at all
45 - 50	Very Good	Loud speech heard faintly
35 - 40	Good	Loud speech heard by hardly intelligible
30 - 35	Fair	Loud speech understood fairly well
25 - 30	Poor	Normal speech understood easily
20 - 25	Very Poor	Low speech audible

Physical Security
สำหรับพื้นที่ควบคุมเพื่อความปลอดภัย

- ความต้องการที่เกี่ยวกับความปลอดภัยของบุคคล
  - เฉพาะเจ้าหน้าที่ทำงานโดยไม่มีคนประกบ
  - ทำธุระเสร็จแล้วจะต้องออกนอกห้องทันที
  - ต้องลงชื่ออละเซ็นชื่อเข้า-ออก
  - บุคคลภายนอกจะต้องมีเจ้าหน้าที่เป็นผู้พาเข้า
- ความต้องการในการควบคุมความปลอดภัยของ Web Farm
  - มาตรฐานการรักษาความปลอดภัยของ Web Farm
  - ในห้องจะต้องมีชั้น (Cabinet) แข็งแรงปลอดภัย

Physical Security
สำหรับพื้นที่ควบคุมเพื่อความปลอดภัย

- หัวหน้าแผนก IT
- รองหัวหน้า (CIO)
- หัวหน้าเจ้าหน้าที่ข้อมูลในหน่วยงาน
- ผู้จัดการหน่วยงานสาหรับเขตควบคุมระบบ IT และระบบ
- ผู้จัดการโปรแกรมรักษาความปลอดภัยระบบข้อมูล

มีการประสานงานและทางานร่วมกัน เช่นร่วมกันร่าง ข้อบังคับ หรือนโยบายต่าง ๆ เป็นต้น

สรุป

การป้องกันความปลอดภัยทางกายภาพนั้นจะให้ได้ผลมากที่สุด ต้องทาตามคำแนะนาดังกล่าวให้ครบ ถึงแม้ว่าคาแนะนาดังกล่าวอาจจะไม่สามารถป้องกันผู้บุกรุกได้ 100 เปอร์เซ็นต์ แต่อย่างน้อยก็สามารถชะลอให้ผู้บุกรุกเข้าถึงระบบได้ช้าลงได้ การป้องกันความปลอดภัยให้แก่ระบบเครือข่ายหรือ Network ทางด้านกายภาพ (Physical) หรือ Hardware ก่อนผลที่ตามมาก็คือ ซอฟท์แวร์จะได้รับการป้องกันด้วย

Reference

- 1. 10 physical security measures every organization should take ผู้เขียน: Debra Littlejohn Shinder
- http://blogs.techrepublic.com.com/10things/?p=106
- 2. บทเรียนมาตรฐานการรักษาความปลอดภัยในพื้นที่ IT กระทรวงเกษตรของสหรัฐอเมริกา (United State Department of Agriculture = USDA) http://www.ocio.usda.gov/directives/doc/DM3510-001.htm
- 3. ระบบรักษาความปลอดภัยและความถูกต้องของระบบงานhttp://www.bcoms.net/system_analysis/lesson77.asp
- 4. Physical Security (การรักษาความปลอดภัยทางกายภาพ) เรียบเรียงโดย : กิติศักดิ์จิรวรรณกูล http://www.thaicert.org/paper/basic/physical_security.php
- 5. สไลด์การสอน บทที่ 2 การจาแนกลักษณะภัยคุกคามและการโจมตีที่มีต่อระบบคอมพิวเตอร์
- (Computer Threats Analysis and Risk Management) โดย อ.พงศ์ตะวัน แสงสว่าง
- 6. https://www.techrepublic.com/article/10-physical-security-measures-every-organization-should-take/