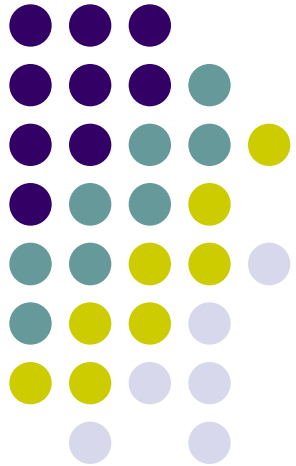
Malware and Protection

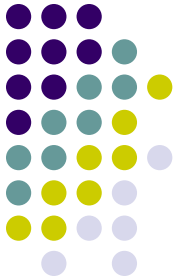
Mr.Jantapong Boodluck

Electronic Computer Technology

King Mongkut's University of Technology North Bangkok



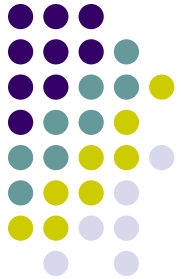
Outline



- Intro Malware and Protection
- มัลแวร์ (Malware)
- โปรแกรมที่ไม่จัดเป็นมัลแวร์
- คุณสมบัติของมัลแวร์
- เทคนิคการตรวจจับไวรัส
- อาการของเครื่องที่ติดไวรัสหรือมัลแวร์
- สาเหตุที่เครื่องติดไวรัสหรือมัลแวร์
- การป้องกันไวรัส
- สรุป

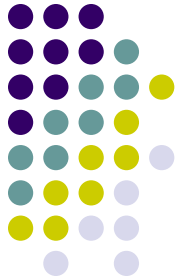
Intro

Malware & Protection



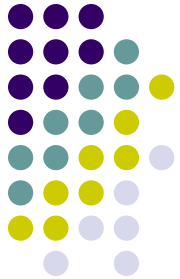
- โปรแกรมที่สามารถสำเนาตัวเองตั้งชื่อว่า "ไวรัส"
- ครั้งแรกในปี พ.ศ.2526 โดย ดร.เฟรดเดอริก โคเฮน
- ไวรัสที่แพร่ระบาดและสร้างความเสียหายครั้งแรกเมื่อปี พ.ศ. 2529
- "เบรน (Brain)" เขียนขึ้น โดยโปรแกรมเมอร์ชาวปากีสถานชื่ออัมจาด (Amjad) และเบซิท (Basit)
- ทำการ Copy Software ขาย พร้อมทั้งแอบปล่อยไวรัส “เบรน”
- ปัจจุบันนี้พบว่ามีมากกว่า 40,000 ชนิด
- เพิ่มขึ้นอีกอยู่ทุกๆ วัน อย่างน้อยวันละ 4-6 ตัว

มัลแวร์ (Malware)



- “Malicious Logic เป็นชุดของคำสั่งที่สร้างปัญหาในการละเมิดนโยบายด้านความปลอดภัยทางเทคโนโลยีสารสนเทศ”
- หรือส่วนใหญ่แล้วเรามักเรียกกันว่า“โปรแกรมประสงค์ร้าย (Malware: Malicious Software)”
- สามารถแบ่งชนิดของโปรแกรมประสงค์ร้ายได้โดยดูจากพฤติกรรม 3 ข้อดังนี้
  - ชุดคำสั่ง(Code) นี้อยู่ได้อิสระหรือไม่ (Need host ?)
  - สามารถเดินทางได้ด้วยตัวเองหรือไม่ (Propagation ?)
  - สามารถสำเนาตัวเองได้หรือไม่ (Self-replicating ?)

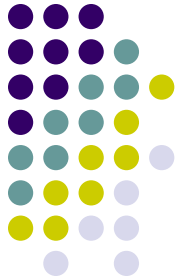
มัลแวร์ (Malware)
ไวรัส (Virus)



- ไวรัส คือ โปรแกรมชนิดหนึ่งที่ถูกเขียนขึ้นให้สามารถจัดการกับตัวมันเอง
  - Need Host –จำเป็นต้องอยู่กับโปรแกรมอื่นหรือชุดคำสั่งอื่น
  - Not Propagation –ต้องใช้ตัวกลางอื่นในการแพร่กระจาย
  - Self-Replicating –จะพยายามทำสำเนาตัวเองกระจายไปยังชุดคำสั่งอื่น

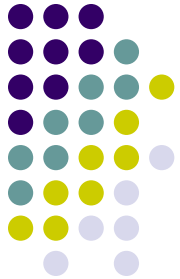
มัลแวร์ (Malware)

หนอน (Worm)



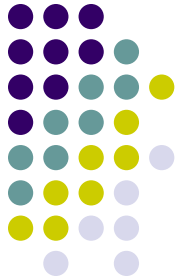
- หนอน (Worm) หมายถึง โปรแกรมที่เป็นอันตรายต่อระบบคอมพิวเตอร์ โดยจะแพร่กระจายตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆที่อยู่ในเครือข่าย
  - *Self-Sub Physical* –สามารถอยู่เป็นโปรแกรมเดียวๆ เองได้
  - *Propagation* –พยายามเคลื่อนที่ไปติดเครื่องอื่น ทั้งไปเองหรือสำเนาตัวเองไป
  - *Not Replicating* –จะไม่ทำสำเนาตัวเองภายในเครื่องเดิม

มัลแวร์ (Malware)
ม้าโทรจัน (Trojan Horse)



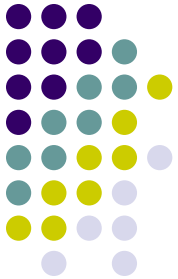
- ม้าโทรจัน (Trojan Horse) หมายถึง โปรแกรมที่ทำลายระบบความปลอดภัยของคอมพิวเตอร์ไม่ทางใดก็ทางหนึ่ง โดยแฝงมากับโปรแกรมอื่นๆ
  - *Self-Sub Physical* –สามารถอยู่เป็นโปรแกรมเดียวๆเองได้
  - *Not Propagation* –ต้องถูกชักนำเข้ามาจากผู้ถูกโจมตีเองไม่สามารถเคลื่อนที่เองได้
  - *Not Replicating* –จะไม่ทำสำเนาตัวเอง
- รูทคิท(Root Kits) หลอกให้ผู้ใช้เชื่อว่าจำเป็นต่อการทำงานของระบบ
- Remote Access Trojan (RAT) สร้างประตูหลัง (Back Door)
- Data Sending and Password Sending Trojan ขโมยรหัสผ่านต่างๆ แล้วส่งไปให้ผู้ไม่ประสงค์ดี
- ฯลฯ

มัลแวร์ (Malware)
โปรแกรมที่ไม่จัดเป็นมัลแวร์



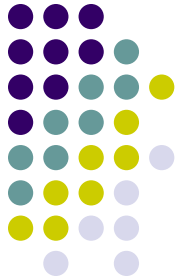
- โจ๊กแอพพลิเคชัน
- โฮแอคซ์(Hoaxes)
- สแปม(Spam)
- สปายแวร์(Spyware)
- แอดแวร์ (Adware)
- อินเทอร์เน็ตคุกกี้ (Internet Cookies)

มัลแวร์ (Malware)
คุณสมบัติของมัลแวร์



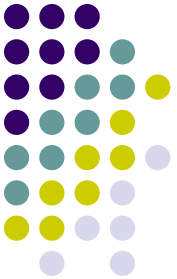
- **คุณสมบัติของเป้าหมาย** *ประเภทของอุปกรณ์, ระบบปฏิบัติการ, แอพพลิเคชัน*
- **พาหะนำมัลแวร์** *Executable File, Script, Boot Sector*
- **กลไกการแพร่กระจาย** *Removable Media, Network Shares*
- **การจุดชนวน** *Manual Execution, Automatic Execution*
- **กลไกการป้องกันตัวเอง** *Stealth, Encryption*

มัลแวร์ (Malware)
เทคนิคการตรวจจับไวรัส



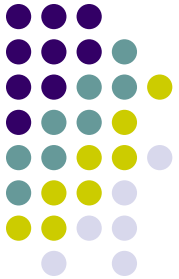
- *การสแกนหาซิกเนเจอร์ (Signature Scanning)* เปรียบเทียบฐานข้อมูลกับไฟล์ที่กำลังสแกนเพื่อจะตัดสินว่าไฟล์นั้นติดไวรัสหรือไม่
- *การสแกนหาคุณลักษณะเฉพาะ* เทคนิคประเภทนี้จะตรวจพบทั้งมัลแวร์เก่าและใหม่โดยการค้นหาคุณลักษณะทั่วไปของมัลแวร์
  - *การแจ้งเตือนผิดๆ (False Positive)*
  - *การสแกนที่ช้า*
- *การมอนิเตอร์พฤติกรรม* เทคนิคประเภทนี้จะเน้นที่พฤติกรรมของการโจมตี

มัลแวร์ (Malware)
อาการของเครื่องที่ติดไวรัสหรือมัลแวร์



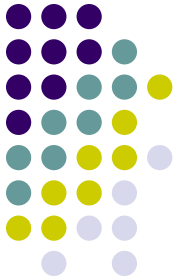
- เครื่องทำงานช้าลง
- เครื่องแฮ้งค้าง หรือหยุดทำงานโดยไม่ทราบสาเหตุ
- ขนาดของหน่วยความจำที่เหลืออยู่ลดน้อยกว่าปกติ โดยหาเหตุผลไม่ได้
- ซีพียูถูกเรียกใช้งานมากเกินกว่า 90 เปอร์เซ็นต์ขึ้นไปตลอดเวลา
- แป้นพิมพ์ทำงานผิดปกติหรือไม่ทำงานเลย
- ไฟล์ข้อมูลหรือโปรแกรมที่เคยใช้อยู่หายไปเฉยๆ
- พบไฟล์มีชื่อแปลกๆที่ไม่เคยพบมาก่อนอยู่ในโฟลเดอร์ต่างๆ
- ขนาดของไฟล์โปรแกรมหรือไฟล์งานใหญ่ขึ้น

มัลแวร์ (Malware)
สาเหตุที่เครื่องติดไวรัสหรือมัลแวร์



- *จากทางแผ่นดิสก์หรือแฟลชไดร์ฟ*
- *จากทางอีเมล์*
- *จากการเข้าไปเปิดเว็บที่มีสคริปต์มุ่งร้าย* (Malicious Script)
- *จากการดาวโหลดไฟล์*
- *จากช่องโหว่* (Vulnerability)
- *จากการเล่นหรือรับไฟล์*

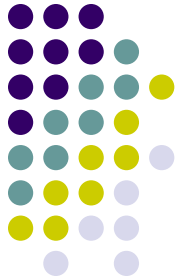
มัลแวร์ (Malware)
การป้องกันไวรัส



- ***การป้องกันไวรัสที่เครื่องไคลเอนท์***
  - *การลบโปรแกรมที่ไม่ได้ใช้งาน, การอัพเดตแพตซ์*
  - *การติดตั้งโฮสต์เบสไฟร์วอลล์, การติดตั้งซอฟต์แวร์ป้องกันไวรัส*
- ***การป้องกันไวรัสที่เซิร์ฟเวอร์***
  - *อัพเดตซีเคียวริตี้แพตซ์, ไม่ติดตั้งโปรแกรมหรือเซอร์วิสที่ไม่จำเป็น*
  - *การป้องกันไวรัสเมล์เซิร์ฟเวอร์, การป้องกันไวรัสที่ดาต้าเบสเซิร์ฟเวอร์*
- ***การป้องกันไวรัสระดับเครือข่าย***
  - *การติดตั้ง IDS, การกรองข้อมูลในระดับแอพพลิเคชัน*
  - *การบล๊อคเว็บไซต์, การสร้างเครือข่ายกักกันเฉพาะ*

มัลแวร์ (Malware)

สรุป



การป้องกันไวรัสที่จะให้ได้ผลนั้นไม่ใช่แค่การติดตั้งโปรแกรมป้องกันไวรัสเท่านั้น จากตัวอย่างของเหตุการณ์ในการโจมตีหลายเหตุการณ์ล่าสุดนั้นได้พิสูจน์ให้เห็นแล้วการป้องกันไวรัสนั้นต้องทำแบบเป็นระบบและต่อเนื่อง คอมพิวเตอร์ไวรัสนั้นมีการพัฒนาตัวเองและปรับเปลี่ยนเทคนิคในการโจมตีเรื่อยๆ

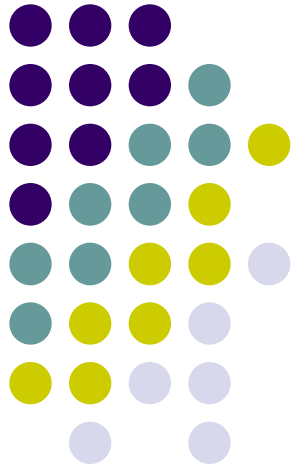
องค์กรควรทบทวนมาตรการป้องกันไวรัสเป็นประจำและปรับปรุงและปรับเปลี่ยนเมื่อจำเป็น การป้องกันไวรัสทุกๆ ด้านมีความสำคัญทั้งหมด

System Restore

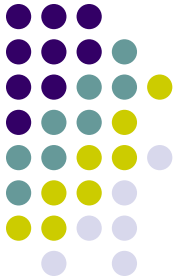
Mr.Jantapong Boodluck

Electronic Computer Technology

King Mongkut's University of Technology North Bangkok



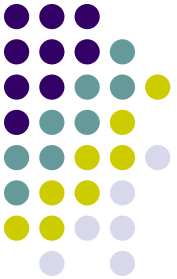
Outline



- Intro System Restore
- การเตรียมการสำหรับการกู้คืนระบบ
- การวิเคราะห์การถูกโจมตี
- การกู้คืนระบบ (System Recovery)
- ขั้นตอนหลังจากการกู้คืนระบบ
- สรุป

Intro

System Restore

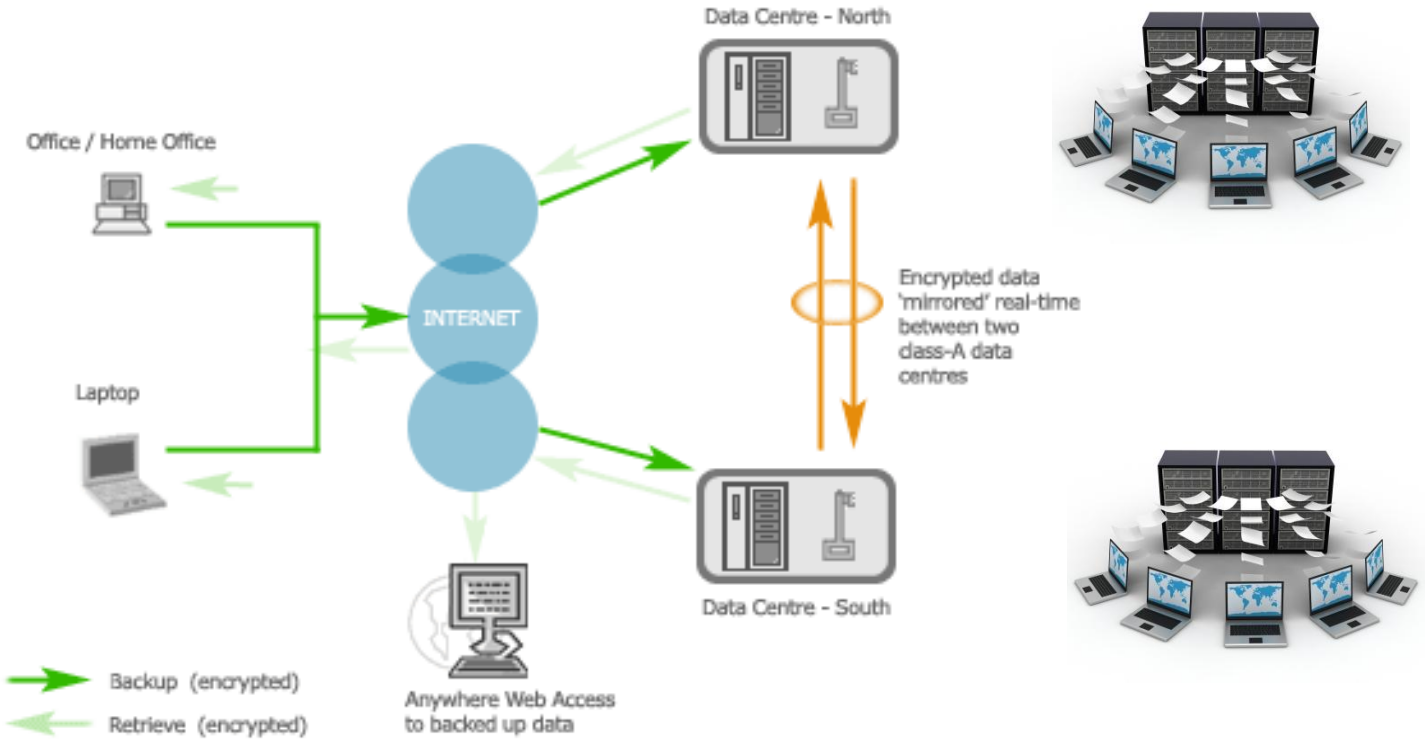


ในปัจจุบันระบบสารสนเทศกลายเป็นหัวใจหลักของระบบธุรกิจส่วนใหญ่ทั้งภาครัฐและเอกชนล้วนนำระบบสารสนเทศมาใช้ในองค์กรอย่างกว้างขวาง

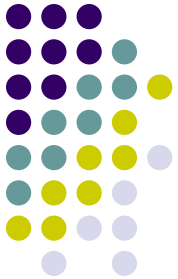
ปัญหาที่หลายองค์กรกำลังเผชิญอยู่ คือ *ปัญหาระบบสารสนเทศไม่สามารถทำงานตามปกติหรือปัญหาระบบสารสนเทศล่ม* ทำให้องค์กรไม่สามารถดำเนินธุรกิจธุรกรรมต่างๆได้ตามปกติ ส่งผลให้องค์กรเกิดความเสียหายได้

System Restore

Example : System Infrastructure

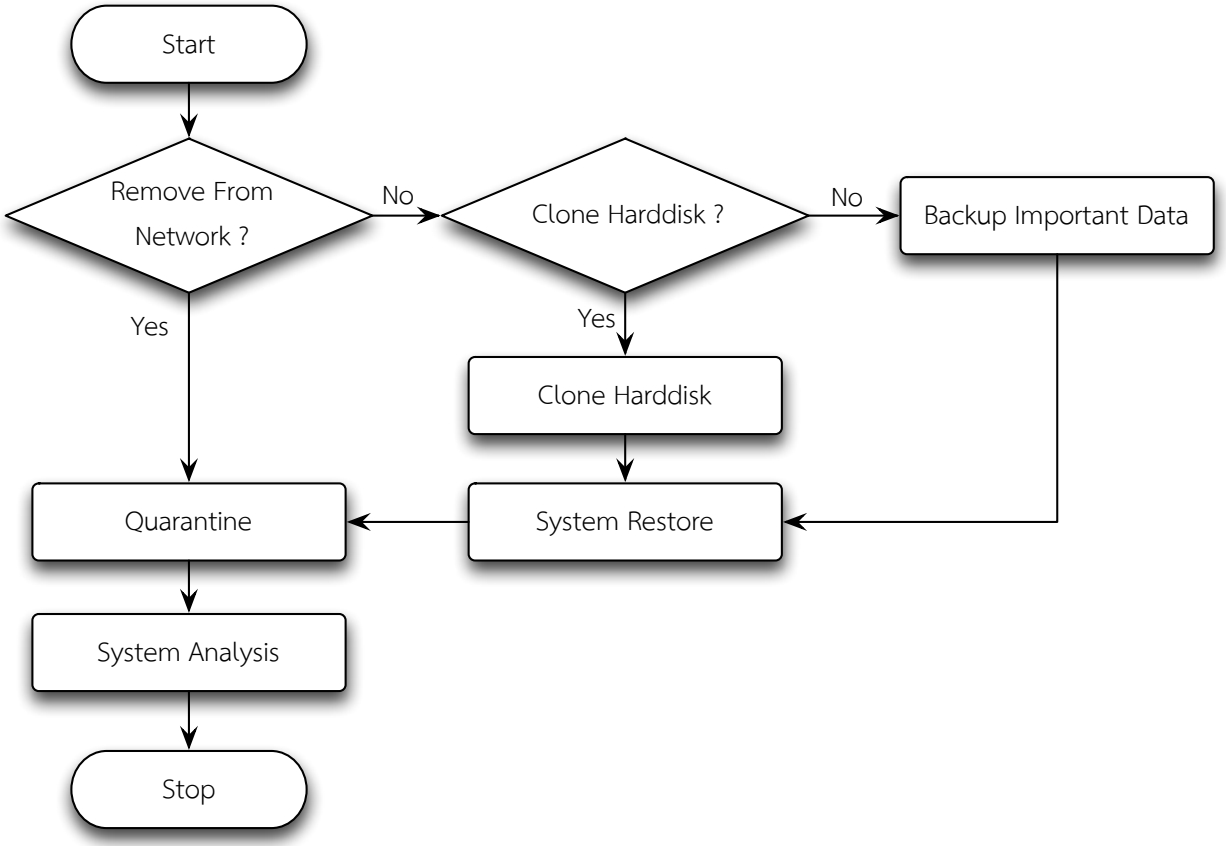


System Restore
การเตรียมการสำหรับการกู้คืนระบบ



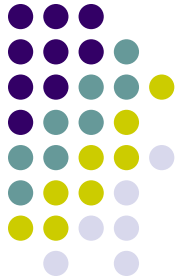
- มีผลกระทบต่อการใช้งานขององค์กรน้อยที่สุด
- ใช้เวลาในการกู้คืนระบบให้เร็วที่สุด
- เก็บข้อมูลหรือหลักฐานเพื่อไว้สำหรับดำเนินการในทางกฎหมาย
- เก็บข้อมูลเพื่อสำหรับการติดตั้งระบบป้องกันและรักษาความปลอดภัยเพิ่มเติม
- ป้องกันการโจมตีแบบเดิมกับระบบที่ถูกกู้คืนเรียบร้อยแล้ว

System Restore
การเตรียมการสำหรับการกู้คืนระบบ



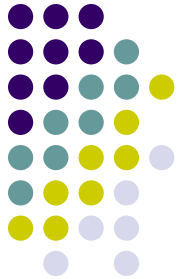
รูปแสดงขั้นตอนการกู้คืนระบบก่อนการวิเคราะห์

System Restore
การวิเคราะห์การถูกโจมตี



- *การตรวจเช็คโพรเซสและเซอร์วิสที่กำลังทำงานอยู่*
- *การตรวจเช็คสตาร์อัพโฟลเดอร์*
- *การตรวจเช็ค Scheduled Applications*
- *การวิเคราะห์ Local Registry*
- *การตรวจค้นหามัลแวร์และคอร์รัพต์ไฟล์*
- *การตรวจสอบบัญชีผู้ใช้และบัญชีกลุ่มผู้ใช้*
- *การตรวจสอบแชร์โฟลเดอร์*
- *การตรวจสอบพอร์ตที่เปิดไว้*
- *การตรวจสอบอีเวนต์ล็อกของระบบ ฯลฯ*

System Restore
การกู้คืนระบบ (System Recovery)



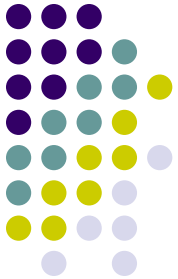
ควรกำจัดมัลแวร์ออกจากระบบหรือติดตั้งระบบใหม่

การคลีนระบบ	การติดตั้งระบบใหม่
เป็นวิธีที่ง่าย ถ้ามีเครื่องมือกำจัดไวรัสที่พร้อมใช้งาน	ขั้นตอนซับซ้อนกว่า โดยเฉพาะถ้าไม่มีเครื่องมือสำหรับแบ็คอัพและกู้คืนระบบก่อนที่จะมีไวรัส
ขั้นตอนน้อยกว่า	ขั้นตอนมากกว่า เพราะต้องเก็บข้อมูล แบ็คอัพ การกำจัดไวรัส สแกน และการกู้คืนระบบ
ใช้รีซอร์สน้อยกว่าในการกำจัดไวรัส	การติดตั้งระบบใหม่ส่วนใหญ่จะใช้เวลาและรีซอร์สมากกว่าในการทำให้ระบบสมบูรณ์
ความเสี่ยงเกี่ยวกับว่าระบบนั้นยังมีมัลแวร์หรือไวรัสอยู่	ความเสี่ยงในการที่มัลแวร์ยังคงอยู่นั้นน้อย

System Restore
การกู้คืนระบบ (System Recovery)

- **การกำจัดมัลแวร์ออกจากระบบ** ควรเลือกที่จะกำจัดมัลแวร์ออกจากระบบ เฉพาะกรณีที่เราเข้าใจพฤติกรรมของมัลแวร์ และแน่ใจว่าขบวนการกำจัดไวรัสนั้นได้ผลจริง
- **การแบ็คอัพไฟล์หรือระบบ**
- **การกู้คืนข้อมูลจากระบบที่ติดไวรัส** *ข้อมูลค่าคอนฟิกของระบบปฏิบัติการ, ข้อมูลของแอพพลิเคชัน, ข้อมูลของผู้ใช้*
- **การติดตั้งระบบใหม่** ติดตั้งจากแบ็คอัพของระบบล่าสุดที่แน่ใจว่าไม่มีไวรัสแน่นอน

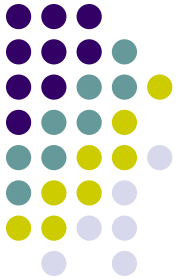
System Restore
ขั้นตอนหลังจากการกู้คืนระบบ



- ***การประชุมเพื่อสรุปสถานการณ์***
  - การดำเนินการทางกฎหมายกับผู้ที่บุกรุก
  - รายงานความเสียหาย
  - วิเคราะห์ว่าจุดอ่อนหรือช่องโหว่
  - ข้อเสนอในการปรับเปลี่ยนนโยบายการรักษาความปลอดภัย

System Restore

สรุป

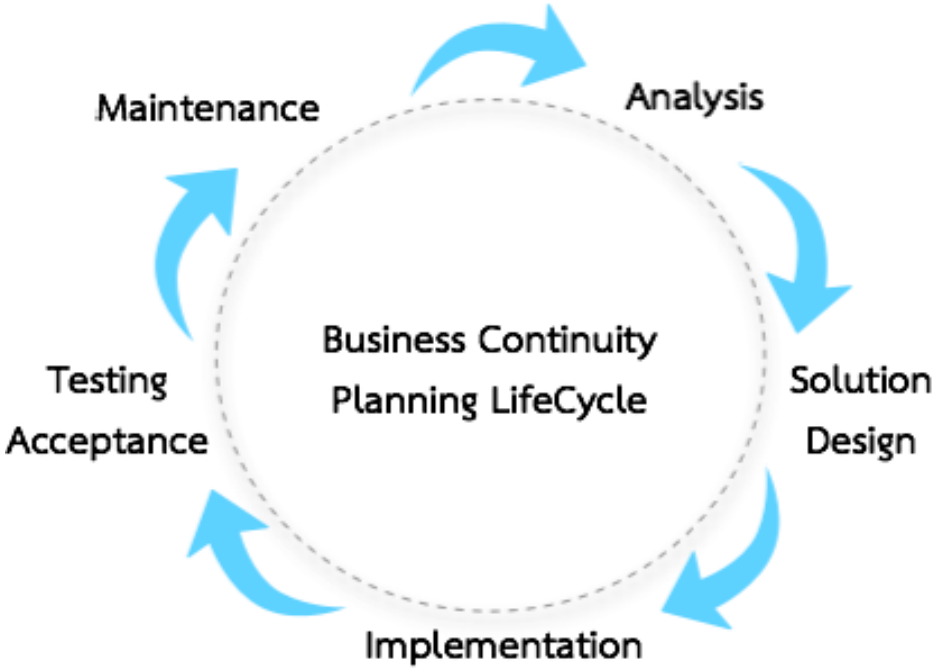


ถ้าองศ์กรมีมาตรการป้องกันที่ดีและมีประสิทธิภาพมากแล้ว โอกาศที่จะถูกโจมตีและที่ต้องกู้คืนระบบนั้นก็น้อยลง อย่างไรก็ตามการไม่ได้วางแผนรับมือกับเหตุการณ์ที่เลวร้ายที่สุดก็อาจเป็นการเพิ่มความเป็นไปได้ที่องศ์กรอาจเผชิญกับความเสียหายขั้นรุนแรงก็ได้ถ้าหากการโจมตีนั้นสำเร็จ

System Restore

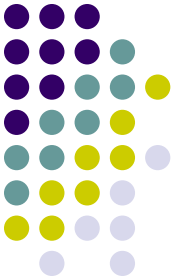
Business Continuity Management (BCM)

- องค์ความรู้ทางด้านการบริหารจัดการให้องค์กรสามารถดำเนินธุรกิจได้อย่างต่อเนื่องภายใต้ภาวะวิกฤติ



System Restore

Business Continuity Management (BCM)



ขั้นตอนที่ 1 : Analysis Phase การวิเคราะห์ปัจจัยเสี่ยงและผลกระทบ

ขั้นตอนที่ 2 : Solution Design Phase ออกแบบยุทธศาสตร์ในการกู้ข้อมูล

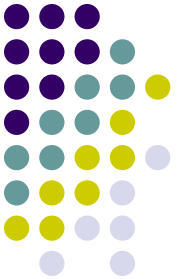
ขั้นตอนที่ 3 : Implementation Phase นำยุทธศาสตร์ที่ออกแบบไว้ทำเป็นแผนปฏิบัติการ

ขั้นตอนที่ 4 : Testing and Organization Acceptance Phase การทดสอบแผน

ขั้นตอนที่ 5 : Maintenance Phase เป็นขั้นตอนในการปรับปรุงแผน BCP ในคู่มือ BCP ให้เป็นปัจจุบัน

System Restore

สรุป



ถ้าองศ์กรมีมาตรการป้องกันที่ดีและมีประสิทธิภาพมากแล้ว โอกาศที่จะถูกโจมตีและที่ต้องกู้คืนระบบนั้นก็น้อยลง อย่างไรก็ตามการไม่ได้วางแผนรับมือกับเหตุการณ์ที่เลวร้ายที่สุดก็อาจเป็นการเพิ่มความเป็นไปได้ที่องศ์กรอาจเผชิญกับความเสียหายขั้นรุนแรงก็ได้ถ้าหากการโจมตีนั้นสำเร็จ

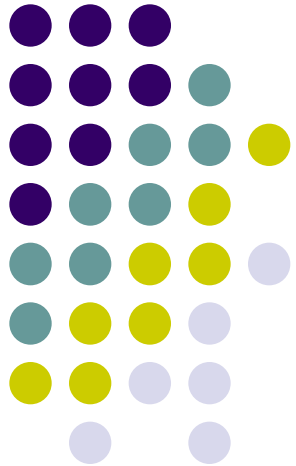
ทิศทางของการประยุกต์ใช้มาตรฐาน BS 25999 ในเรื่องการจัดทำ BCM และการรับรองผู้เชี่ยวชาญด้าน BCM ของสถาบัน BCI ตามกระแสความต้องการบุคลากรด้าน BCM นั้นมีแนวโน้มที่จะได้รับความนิยมมากขึ้นในอนาคตอันใกล้นี้

Physical Security

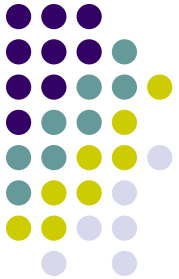
Mr.Jantapong Boodluck

Electronic Computer Technology

King Mongkut's University of Technology North Bangkok



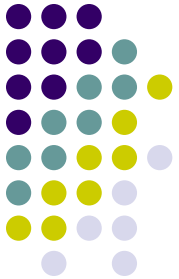
Outline



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

Intro

Physical Security



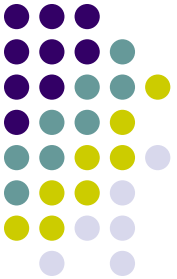
- **ระบบรักษาความปลอดภัยภายนอกระบบงาน (Physical Security)**

ระบบรักษาความปลอดภัยในส่วนนี้จะกระทำกันภายนอกระบบงานคอมพิวเตอร์ ตัวอย่างเช่น การล็อกห้องคอมพิวเตอร์ เป็นต้น

- **ระบบรักษาความปลอดภัยภายในระบบงาน (System Security And Integrity)** การกระจายอำนาจการใช้ข้อมูลออกไป (Distribution System) ของระบบงาน ทำให้ระบบจำเป็นที่จะต้องมีระบบการรักษาความปลอดภัยภายในระบบงานอย่างดีพอ

Physical Security

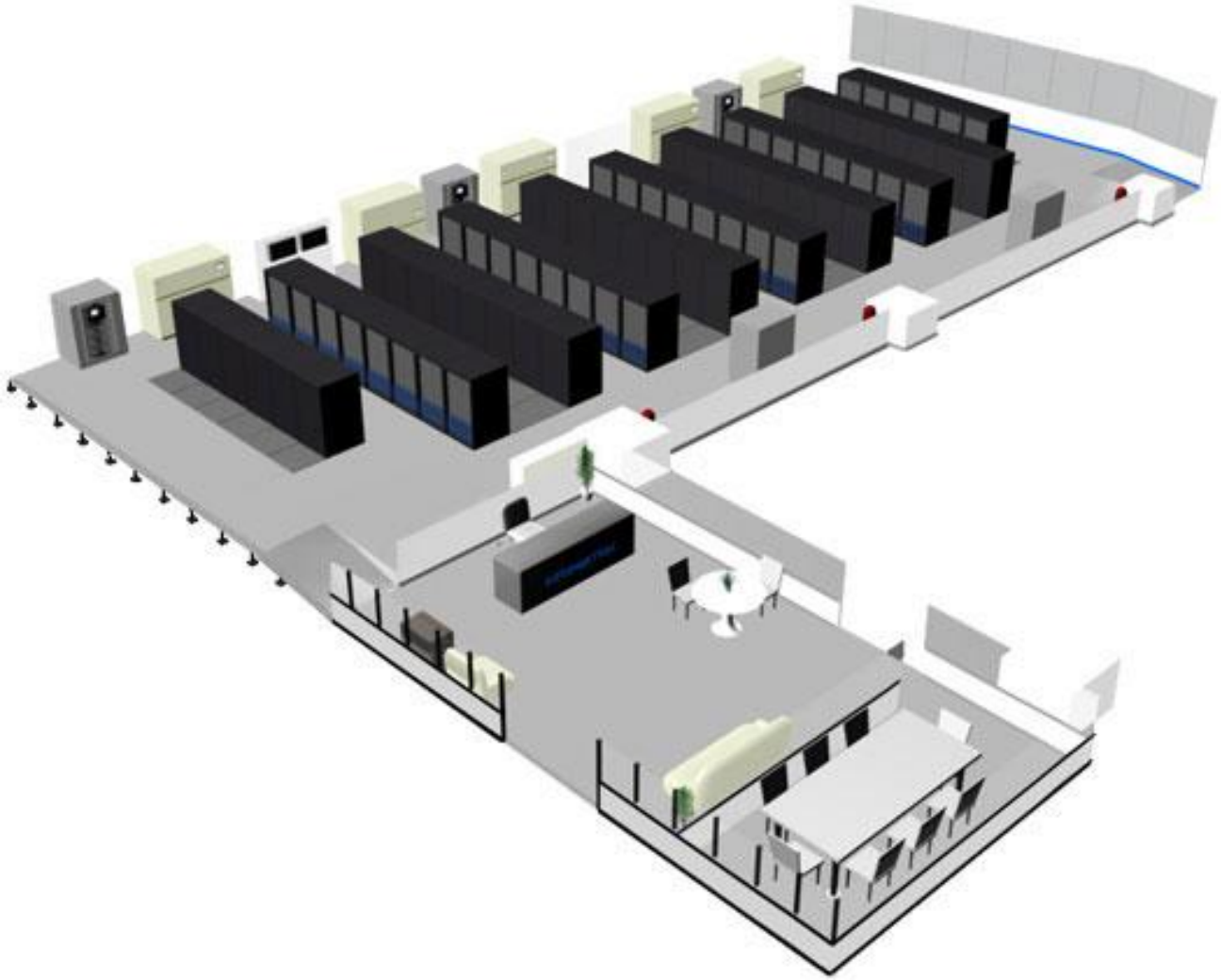
แนวทางความปลอดภัยทางกายภาพของระบบ



- แบ่งแยกพื้นที่ควบคุมความปลอดภัยอย่างชัดเจน
- ใช้ระบบป้องกันและตรวจสอบการเข้าออก
- เก็บรักษาระบบและอุปกรณ์ต่างๆ ในพื้นที่รักษาความปลอดภัย
- ใช้เครื่องจ่ายกำลังไฟฟ้าสำรอง
- วางแผนสำหรับการกู้ระบบคืน
- ตรวจสอบข้อมูลของเจ้าหน้าที่จากภายนอกที่เข้ามา

Physical Security

แนวทางความปลอดภัยทางกายภาพของระบบ

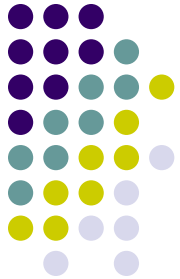


Physical Security

แนวทางความปลอดภัยทางกายภาพของระบบ

Physical Security

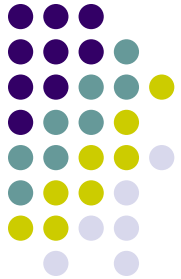
แนวทางความปลอดภัยทางกายภาพภายใน



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

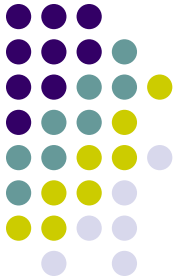
Physical Security

10 Physical security Measures



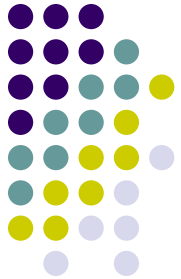
- *ล็อคห้องเก็บเซิร์ฟเวอร์ (Server)*
- *มีการเฝ้าระวังการเข้า-ออกอย่างเข้มงวด*
- *อุปกรณ์ที่เป็นจุดอ่อนต้องเก็บไว้ในห้องที่ปิดล็อค*
- *ตั้ง Server ไว้บน Rack*
- *อย่าลืมเวิร์คสเตชั่น*
- *ไม่ให้ผู้บุกรุกหรือบุคคลภายนอกเปิดตู้ได้*
- ป้องกันคอมพิวเตอร์ Lap Top หรือ Note Book
- ป้องกันคอมพิวเตอร์ Lap Top หรือ Note Book
- *ทำให้หน่วยขับเคลื่อนความจำไม่ทำงาน*
- *ป้องกันปริ้นเตอร์*

Physical Security
ตัวอย่างมาตรฐานการรักษาความปลอดภัย



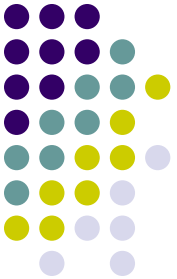
- **กระทรวงเกษตรของสหรัฐอเมริกา** (United State Department of Agriculture = USDA)
  - เก็บข้อมูลส่วนตัวของประชากรสหรัฐ
  - ทั้งรายได้และธุรกรรมทางการเงิน
- ***นโยบาย (Policy)*** รักษาความปลอดภัยแหล่งข้อมูล
- ***กระบวนการ (Procedures)*** รักษาความปลอดภัย คอมพิวเตอร์ อุปกรณ์โทรคมนาคมและระบบเครือข่าย

Physical Security
สำหรับพื้นที่ควบคุมเพื่อความปลอดภัย



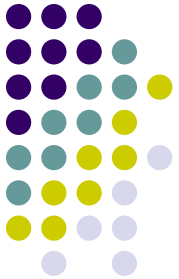
- *ข้อบังคับทั่วไปเพื่อความปลอดภัย*
  - ลานจอดรถ (Parking)
  - มีโทรทัศน์วงจรปิด (Close Circuit TV)
  - มีแสงสว่างพอเพียงและมีระบบไฟฟ้าสำรอง
  - ล็อคทางเข้า (Entrance) และทางออก (Exit)
  - ผู้มาติดต่อต้องแสดงบัตร
  - อนุญาตให้ใช้อุปกรณ์หรือเครื่องมือบางอย่างเฉพาะเจ้าหน้าที่เท่านั้น
  - แผนการทดสอบฉุกเฉิน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

Physical Security
สำหรับพื้นที่ควบคุมเพื่อความปลอดภัย



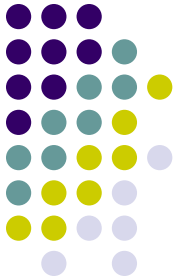
- *มาตรฐานการรักษาความปลอดภัยในเขตควบคุมระบบ IT*
  - อยู่ในอาคารห่างจากหน้าต่าง
  - Floor Plan ไม่ระบุจุดที่ตั้งของทรัพย์สินที่สำคัญ
  - Sound Transmission Class 40
  - มีระบบป้องกันไฟระบบท่อแบบแห้ง
  - รักษาทางเข้าเขตควบคุม
  - ผู้มาติดต่อ ห่างจากเขตควบคุมไม่ต่ำกว่า 50 ฟุต
  - ข้อมูล Back up ที่สำคัญหรืออ่อนไหวมากให้เก็บภานนอกห้องนี้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

Physical Security
สำหรับพื้นที่ควบคุมเพื่อความปลอดภัย



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

Physical Security
สำหรับพื้นที่ควบคุมเพื่อความปลอดภัย

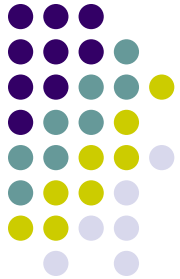


- *หัวหน้าแผนก IT*
- *รองหัวหน้า (CIO)*
- *หัวหน้าเจ้าหน้าที่ข้อมูลในหน่วยงาน*
- *ผู้จัดการหน่วยงานสำหรับเขตควบคุมระบบ IT และระบบ*
- *ผู้จัดการโปรแกรมรักษาความปลอดภัยระบบข้อมูล*

มีการประสานงานและทำงานร่วมกัน เช่นร่วมกันร่าง ข้อบังคับ หรือนโยบายต่างๆ เป็นต้น

Physical Security

สรุป



การป้องกันความปลอดภัยทางกายภาพนั้นจะให้ได้ผลมากที่สุด ต้องทำตามคำแนะนำดังกล่าวให้ครบ ถึงแม้ว่าคำแนะนำดังกล่าวอาจจะไม่สามารถป้องกันผู้บุกรุกได้ 100 เปอร์เซ็นต์ แต่อย่างน้อยก็สามารถชะลอให้ผู้บุกรุกเข้าถึงระบบได้ช้าลงได้ การป้องกันความปลอดภัยให้แก่ระบบเครือข่ายหรือ Network ทางด้านกายภาพ (Physical) หรือ Hardware ก่อน ผลที่ตามมาก็คือ ซอฟท์แวร์จะได้รับการป้องกันด้วย

References

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 การจำแนกลักษณะภัยคุกคามและการโจมตีที่มีต่อระบบคอมพิวเตอร์

(Computer Threats Analysis and Risk Management) โดย อ.พงศ์ตะวัน แสงสว่าง