บทที่ 2 : การรักษาความปลอดภัยข้อมูล Part1

สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยศ

apipong.ping@gmail.com

Outline

- กระบวนการรักษาความปลอดภัยข้อมูล
- การบริหารความเสี่ยง
- การประเมินความเสี่ยง

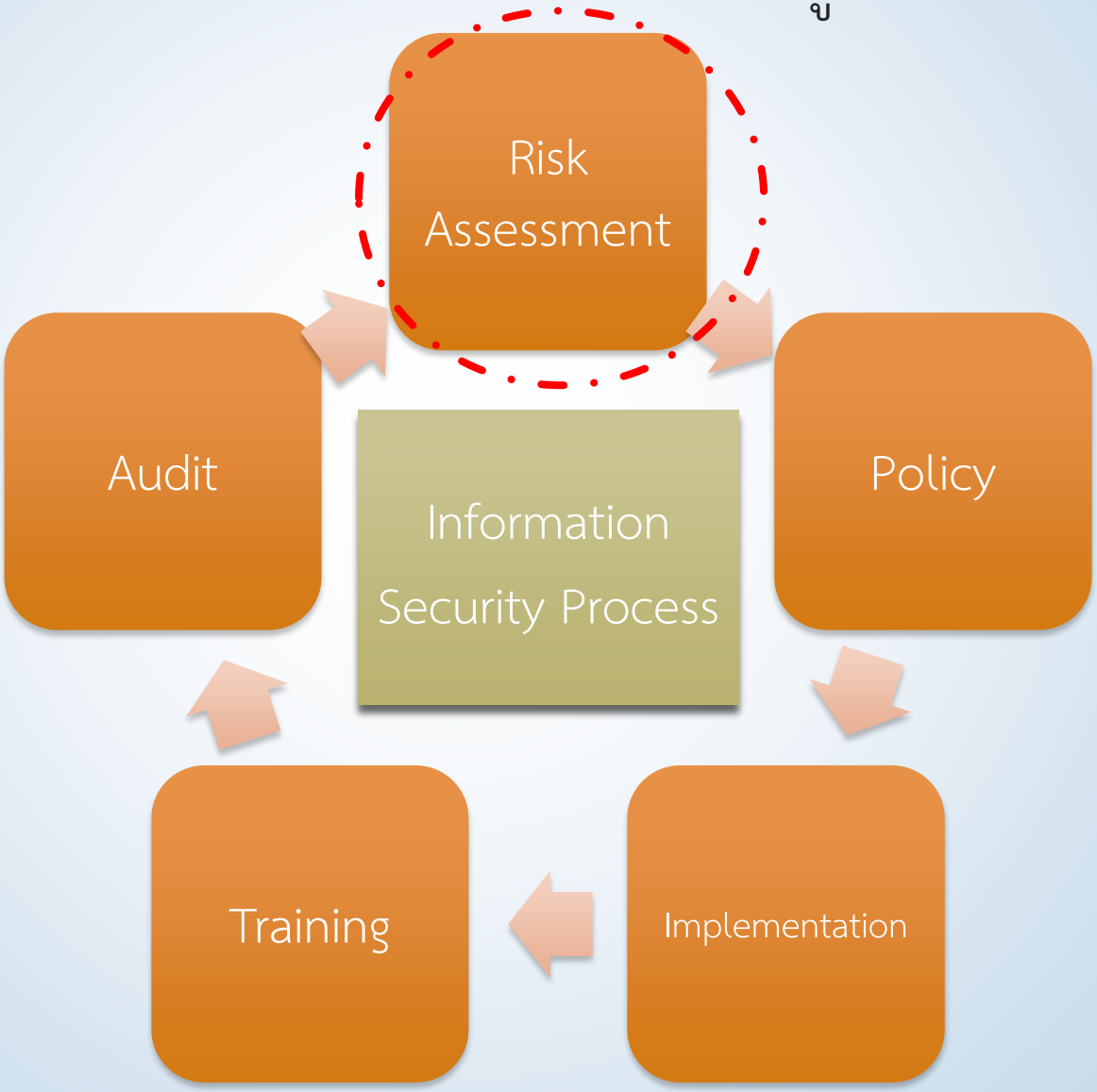
กระบวนการรักษาความปลอดภัยข้อมูล

- การรักษาความปลอดภัยของข้อมูลเป็นกระบวนการใน**เชิงรุก**เพื่อบริหารความเสี่ยง (Risk Management)
- แต่โดยส่วนใหญ่การรักษาความปลอดภัยกลับเป็น**เชิงรับ** คือองค์กรจะรอให้เกิดเหตุการณ์ขึ้นก่อนแล้วค่อยหาวิธีป้องกัน ตรงกับสุภาษิต **“วัวหายล้อมคอก”**
- *ค่าใช้จ่ายในการรักษาความปลอดภัย = ค่าความเสียหายเมื่อเกิดเหตุการณ์ + ค่าใช้จ่ายในการติดตั้งระบบป้องกัน*

กระบวนการรักษาความปลอดภัยข้อมูล [2]

- การวางแผนเพื่อเตรียมรับเหตุการณ์และการบริหารความเสี่ยงอย่างดี ทำให้ค่าความเสียหายเมื่อเกิดเหตุการณ์ลดลงได้
- *ค่าใช้จ่ายในการรักษาความปลอดภัย = ค่าใช้จ่ายในการติดตั้งระบบป้องกัน*

กระบวนการรักษาความปลอดภัยข้อมูล



การบริหารความเสี่ยง (Risk Management)

- การรักษาความปลอดภัยเกี่ยวข้องกับการบริหารความเสี่ยงอย่างใกล้ชิด
- หากไม่เข้าใจความเสี่ยงขององค์กร อาจใช้ทรัพยากรเพื่อการรักษาความปลอดภัยมากเกินความจำเป็นหรือน้อยกว่าที่ควร

การบริหารความเสี่ยง (Risk Management)

: ความเสี่ยงคืออะไร?

- **ความเสี่ยง (Risk)** คือความเป็นไปได้ที่อาจจะสูญเสียบางสิ่งที่ปกป้องอยู่ ความเสี่ยงยังเป็นพื้นฐานที่ทำให้ต้องมีการรักษาความปลอดภัย
- เช่น การซื้อประกันภัยรถยนต์เป็นการช่วยลดความเสี่ยง ซึ่งการคำนวณเบี้ยประกันก็มาจากจำนวนเงินที่อาจต้องใช้ในการซ่อมรถยนต์และความน่าจะเป็นที่จะเกิดอุบัติเหตุ
- จากตัวอย่างข้างต้น **ความเสี่ยงจะประกอบด้วย 2 ส่วน** ส่วนแรกคือเงินที่ใช้ในการซ่อมรถที่บริษัทประกันภัยจะต้องจ่าย ถือเป็น**ช่องโหว่ (Vulnerability)** ส่วนที่สองคือความน่าจะเป็นที่จะเกิดอุบัติเหตุ ถือเป็น**ภัยคุกคาม (Threat)** ที่จะใช้ประโยชน์จากช่องโหว่นั้น

การบริหารความเสี่ยง (Risk Management)

: ความเสี่ยงคืออะไร? [2]

- <u>สรุป</u> เมื่อรวมช่องโหว่และภัยคุกคามเข้าด้วยกัน จะกลายเป็นความเสี่ยง
- หากไม่มีช่องโหว่ก็จะไม่มีความเสี่ยง หรือหากไม่มีภัยคุกคามก็จะไม่มีความเสี่ยงเช่นกัน

การบริหารความเสี่ยง (Risk Management)

: ช่องโหว่หรือจุดอ่อน (Vulnerability)

- คือช่องทางที่อาจใช้สำหรับการโจมตีได้
- จุดอ่อนมีหลายระดับขึ้นอยู่กับความยากง่าย, ระดับความชำนาญทางด้านเทคนิคที่สามารถใช้ประโยชน์จากจุดอ่อนได้ และผลกระทบที่เกิดจากการใช้ประโยชน์จากจุดอ่อนดังกล่าว
- จุดอ่อนไม่ได้มีเฉพาะระบบคอมพิวเตอร์และเครือข่ายเท่านั้น แต่รวมถึงด้านกายภาพ พนักงาน ข้อมูล หรือทรัพย์สินที่ไม่ได้อยู่ในรูปแบบอิเล็กทรอนิกส์ด้วย

การบริหารความเสี่ยง (Risk Management)

: ภัยคุกคาม (Threat)

- คือ สิ่งที่อาจจะเกิดขึ้นและมีอันตรายต่อทรัพย์สินขององค์กร ประกอบด้วย 3 ส่วน
  - **เป้าหมาย (Target)**
  - **ผู้โจมตี (Agent)**
  - **เหตุการณ์ (Event)**

การบริหารความเสี่ยง (Risk Management)

: ภัยคุกคาม (Threat) : เป้าหมาย (Target)

- หมายถึง*องค์ประกอบ*ด้านต่างๆ ของการรักษาความปลอดภัย
  - **ความลับ (Confidentiality)** จะเป็นเป้าหมายก็ต่อเมื่อความลับของข้อมูลถูกเปิดเผยต่อผู้ที่ไม่ได้รับอนุญาต
  - **ความคงสภาพ (Integrity)** จะเป็นเป้าหมายเมื่อภัยคุกคามนั้นพยายามที่จะเปลี่ยนแปลงข้อมูล
  - **ความพร้อมใช้งาน (Availability)** จะเป็นเป้าหมายเมื่อมีการโจมตีแบบปฏิเสธการให้บริการ (DoS)

การบริหารความเสี่ยง (Risk Management)

: ภัยคุกคาม (Threat) : ผู้โจมตี (Agent)

- หมายถึง *ผู้ที่กระทำการ*ใดๆ ที่ก่อให้เกิดผลทางด้านลบกับองค์กร โดยมีคุณสมบัติ 3 ข้อ
  - **การเข้าถึง (Access)** : ผู้โจมตีต้องสามารถเข้าถึงเป้าหมายได้
  - **ความรู้ (Knowledge)** : ความรู้หรือข้อมูลของเป้าหมาย
  - **แรงจูงใจ (Motivation)** : เหตุผลที่ผู้โจมตีมีสำหรับการโจมตี

การบริหารความเสี่ยง (Risk Management)

: ภัยคุกคาม (Threat) : ผู้โจมตี (Agent) >การเข้าถึง

- **การเข้าถึง (Access)** : ผู้โจมตีต้องสามารถเข้าถึงระบบ เครือข่าย สถานที่ หรือข้อมูลที่ต้องการ
- **ทางตรง** เช่น การเจาะเข้าระบบบัญชี
- **ทางอ้อม** เช่น ผู้โจมตีเข้าถึงสถานที่ใดๆผ่านทางช่องทางพิเศษ
- องค์ประกอบสำคัญของการเข้าถึงคือ **โอกาส**
- ผู้โจมตีอาจเป็น 1) พนักงาน 2) พนักงานเก่า 3) แฮคเกอร์ 4) ศัตรูหรือคู่แข่ง

การบริหารความเสี่ยง (Risk Management)

: ภัยคุกคาม (Threat) : ผู้โจมตี (Agent) > ความรู้

- ความรู้ (Knowledge) : ผู้โจมตีต้องมีความรู้หรือข้อมูลเกี่ยวกับเป้าหมาย เช่น บัญชีผู้ใช้ รหัสผ่าน ที่อยู่ IP address ระบบรักษาความปลอดภัย
- ยิ่งผู้โจมตีมีข้อมูลของเป้าหมายมากเท่าใด ยิ่งรู้จุดอ่อนมากขึ้นเท่านั้น และยิ่งมีโอกาสรู้วิธีการใช้ประโยชน์จากจุดอ่อนนั้นได้ง่าย

การบริหารความเสี่ยง (Risk Management)

: ภัยคุกคาม (Threat) : ผู้โจมตี (Agent) > แรงจูงใจ

- พิจารณาได้จาก
- ความท้าทาย : เป็นความพยายามพิสูจน์ว่าเขาสามารถทำอะไรบางอย่างได้
- ความอยากได้ : ความต้องการอยากได้อะไรบางอย่าง เช่น เงิน สิ่งของ บริการ หรือข้อมูล
- ความตั้งใจ : ตั้งใจที่จะทำอันตรายต่อองค์กร หรือบุคคลใดบุคคลหนึ่ง

การบริหารความเสี่ยง (Risk Management)

: ภัยคุกคาม (Threat) : เหตุการณ์ (Event)

- หมายถึง *วิธีการ*ที่ผู้โจมตีอาจทำอันตรายต่อองค์กร ยกตัวอย่างเช่น
  - การใช้บัญชีผู้ใช้ในทางผิดหรือเกินกว่าได้รับอนุญาต
  - การแก้ไขข้อมูลที่สำคัญ
  - การเจาะเข้าระบบโดยไม่ได้รับอนุญาต
  - การทำลายระบบโดยไม่ได้ตั้งใจ
  - การรบกวนระบบสื่อสารข้อมูลทั้งภายในและภายนอก
  - การบุกรุกเข้าห้องควบคุมโดยไม่ได้รับอนุญาต

การประเมินความเสี่ยง (Risk Assessment)

- เครื่องมือต่างๆที่ใช้ในการประเมินความเสี่ยงถูกใช้งานเพื่อตอบคำถามดังนี้
  - เราต้องการจะปกป้องอะไร?
  - ใครหรืออะไรที่เป็นภัยคุกคาม หรือช่องโหว่
  - จะเกิดความเสียหายมากน้อยเท่าใดเมื่อถูกโจมตี
  - มูลค่าทรัพย์สินขององค์กรมีอะไรบ้างและเท่าไร
  - เราจะป้องกันหรือแก้ไขช่องโหว่ได้อย่างไร
- ผลจากการประเมินความเสี่ยงคือข้อแนะนำเกี่ยวกับวิธีป้องกันที่ดีที่สุด เพื่อปกป้องความลับ ความคงสภาพ และความพร้อมใช้งาน

การประเมินความเสี่ยง (Risk Assessment)

- ขั้นตอนสำคัญของการประเมินความเสี่ยงคือ
  - 1) กำหนดขอบเขต
  - 2) เก็บรวบรวมข้อมูล
  - 3) วิเคราะห์นโยบายและระเบียบปฏิบัติ
  - 4) วิเคราะห์ภัยคุกคาม
  - 5) วิเคราะห์จุดอ่อนหรือช่องโหว่
  - 6) ประเมินความเสี่ยง

การประเมินความเสี่ยง (Risk Assessment)

: 1) กำหนดขอบเขต

- เป็นขั้นตอนที่สำคัญที่สุดของกระบวนการ เนื่องจากเป็นตัวกำหนดว่าอะไรที่จะทำหรือไม่ทำในระหว่างการประเมิน และเป็นการระบุว่าอะไรที่เราจะปกป้อง ความสำคัญของสิ่งที่จะปกป้อง จะปกป้องถึงระดับไหน

การประเมินความเสี่ยง (Risk Assessment)

: 2) เก็บรวบรวมข้อมูล

- เป็นการรวบรวมนโยบาย ระเบียบปฏิบัติในปัจจุบัน
- การสัมภาษณ์หรือสนทนากับบุคคลหลักๆขององค์กร จะช่วยทำให้ได้ข้อมูลได้
- การเก็บรวบรวมข้อมูลควรทำสิ่งต่อไปนี้ เช่น แพตช์ที่ติดตั้งแต่ละเครื่อง เซอร์วิสที่ให้บริการ ประเภทและเวอร์ชันของระบบปฏิบัติการ แอพพลิเคชันที่รันผ่านเครือข่าย สิทธิ์ในการเข้าออกห้องคอมพิวเตอร์ สแกนพอร์ตที่เปิด การให้บริการไวร์เลสแลน ทดสอบระบบIDSและไฟร์วอลล์ เป็นต้น

การประเมินความเสี่ยง (Risk Assessment)

: 2) เก็บรวบรวมข้อมูล [2]

- เว็บไซต์ที่ให้ข้อมูลเกี่ยวกับช่องโหว่ เช่น
- www.securityfocus.com
- www.incidents.org
- www.packetstormsecurity.org
- www.sans.org
- www.cert.org

การประเมินความเสี่ยง (Risk Assessment)

: 3) วิเคราะห์นโยบายและระเบียบปฏิบัติ

- เป็นการตรวจสอบดูว่าองค์กรนั้นจัดอยู่ในระดับมาตรฐานใด มาตรฐานความปลอดภัยที่นิยมคือ ISO17799 ISO15504
- หากส่วนใดขององค์กรไม่ได้มาตรฐาน ควรวิเคราะห์ดูว่ามีความจำเป็นที่จะต้องทำให้ได้ตามมาตรฐานหรือไม่ เนื่องจากมาตรฐานด้านความปลอดภัยนั้นมีค่อนข้างมาก

การประเมินความเสี่ยง (Risk Assessment)

: 5) วิเคราะห์จุดอ่อนหรือช่องโหว่

- จุดประสงค์ในการวิเคราะห์ช่องโหว่ (Vulnerability Analysis) เพื่อเป็นการทดสอบสถานภาพขององค์กรว่าล่อแหลมต่อการถูกโจมตีหรือทำลายมากน้อยแค่ไหน เช่น การทดลองเจาะระบบทั้งจากภายในและภายนอก
- เครื่องมือที่ใช้วิเคราะห์ช่องโหว่ของระบบ เช่น Nessus, GFI LANGuard, Retina, SAINT

ระดับความรุนแรงของช่องโหว่

ระดับความเสี่ยง (Severity)	ระดับ (Rating)	ความเปิดเผย (Exposure)
Minor Severity : การใช้ประโยชน์จากช่องโหว่นี้ต้องใช้ทรัพยากรมาก และความเสียหายที่เกิดมีน้อยมาก	1	**Minor Exposure** : ผลกระทบอยู่ในระดับควบคุมได้และไม่ทำให้เกิดช่องโหว่อื่นๆ
Moderate Severity : การใช้ประโยชน์จากช่องโหว่นี้ต้องใช้ทรัพยากรมาก และความเสียหายที่เกิดมีสูง **หรือ** การใช้ประโยชน์จากช่องโหว่นี้ต้องใช้ทรัพยากรน้อย และความเสียหายที่เกิดปานกลาง	2	**Moderate Exposure** : ช่องโหว่อาจมีผลกระทบมากกว่าหนึ่งระบบ อาจมีการใช้ประโยชน์จากช่องโหว่หนึ่งแล้วเพิ่มโอกาสให้มีช่องโหว่อื่นๆ
High Severity : การใช้ประโยชน์จากช่องโหว่นี้ต้องใช้ทรัพยากรน้อย และความเสียหายที่เกิดมีสูง	3	**High Exposure** : ช่องโหว่มีผลกระทบต่อระบบส่วนใหญ่ มีการใช้ประโยชน์จากช่องโหว่หนึ่งแล้วเพิ่มโอกาสให้มีช่องโหว่อื่นๆ

การประเมินความเสี่ยง (Risk Assessment)

: 6) ประเมินความเสี่ยง

- เมื่อทำตามขั้นตอนการบริหารความเสี่ยงแล้ว จะสามารถระบุความเสี่ยง และค่าความเสียหายจากภัยได้ เพื่อสามารถเลือกใช้เครื่องมือหรือระบบป้องกันที่เหมาะสม และมีประสิทธิภาพเพื่อป้องกันภัยเหล่านั้นได้

การประเมินความเสี่ยง (Risk Assessment)

: 6) ประเมินความเสี่ยง [2]

- การประเมินความเสี่ยงขององค์กร แบ่งออกเป็น 5 ระดับ
  - ระดับระบบ (System-Level)
  - ระดับเครือข่าย (Network-Level)
  - ระดับองค์กร (Organization-Level)
  - การตรวจสอบ (Audit)
  - ทดสอบเจาะเข้าระบบ (Penetration Test)