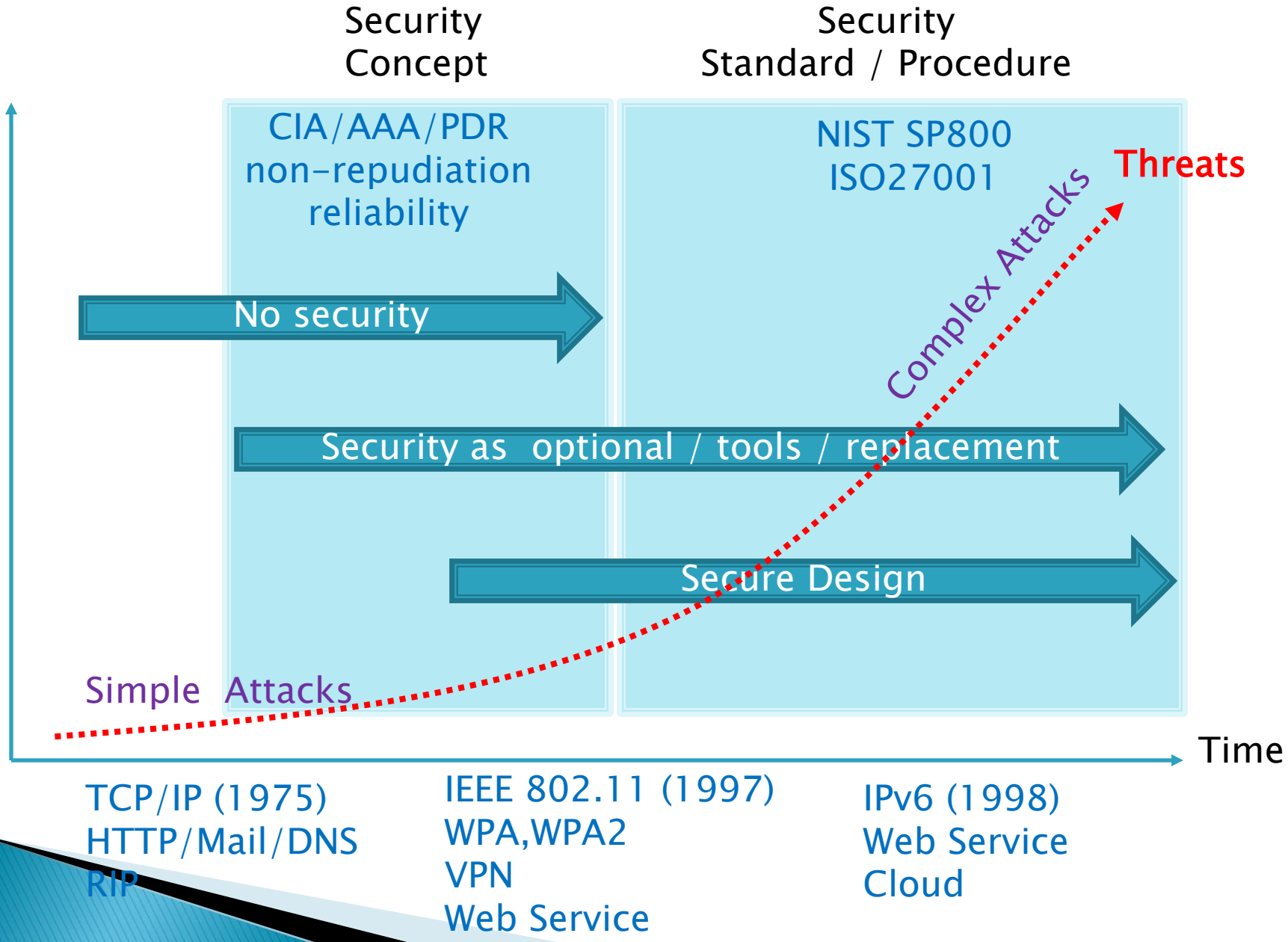
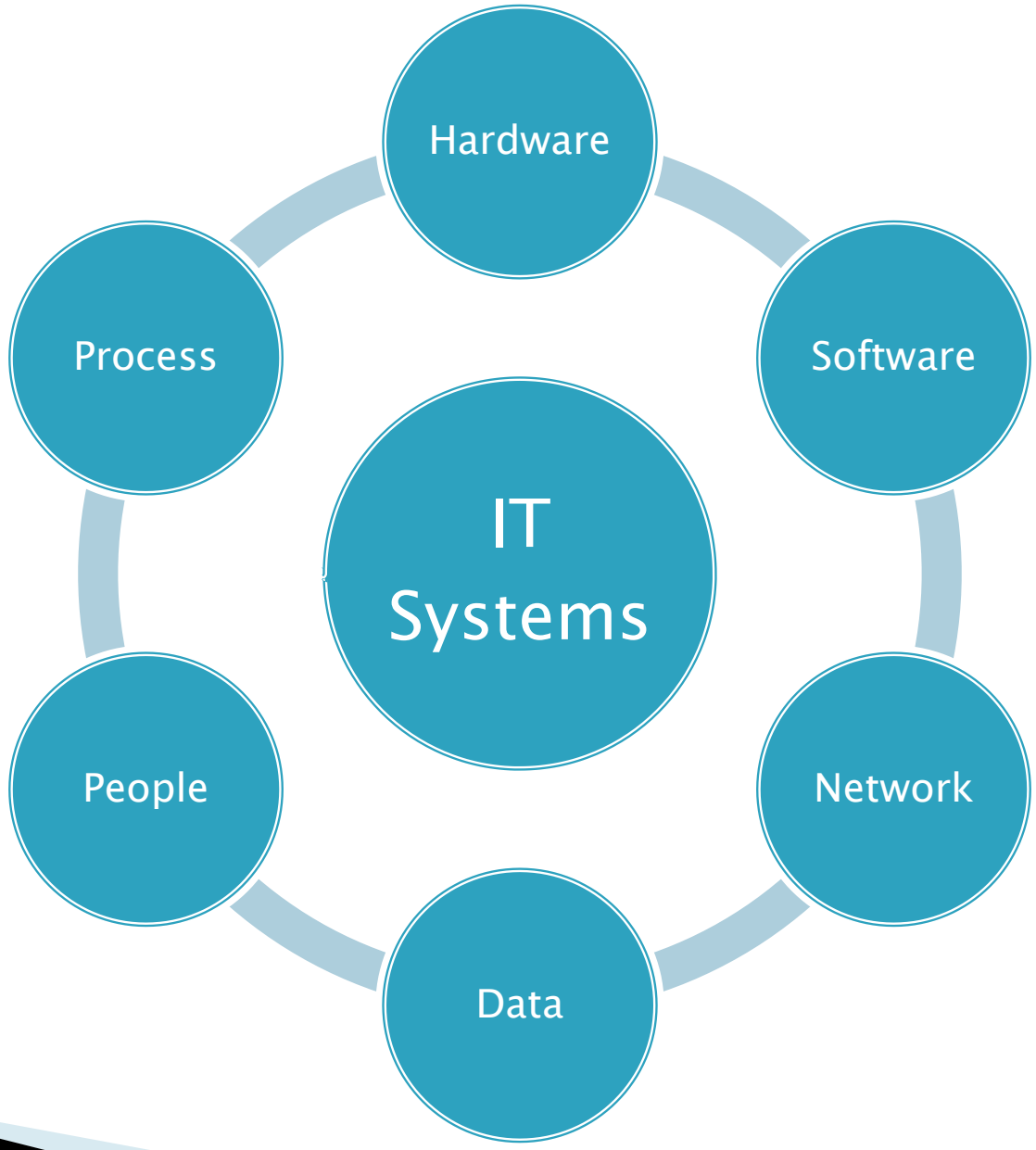
IT Security Concept (Workshop)

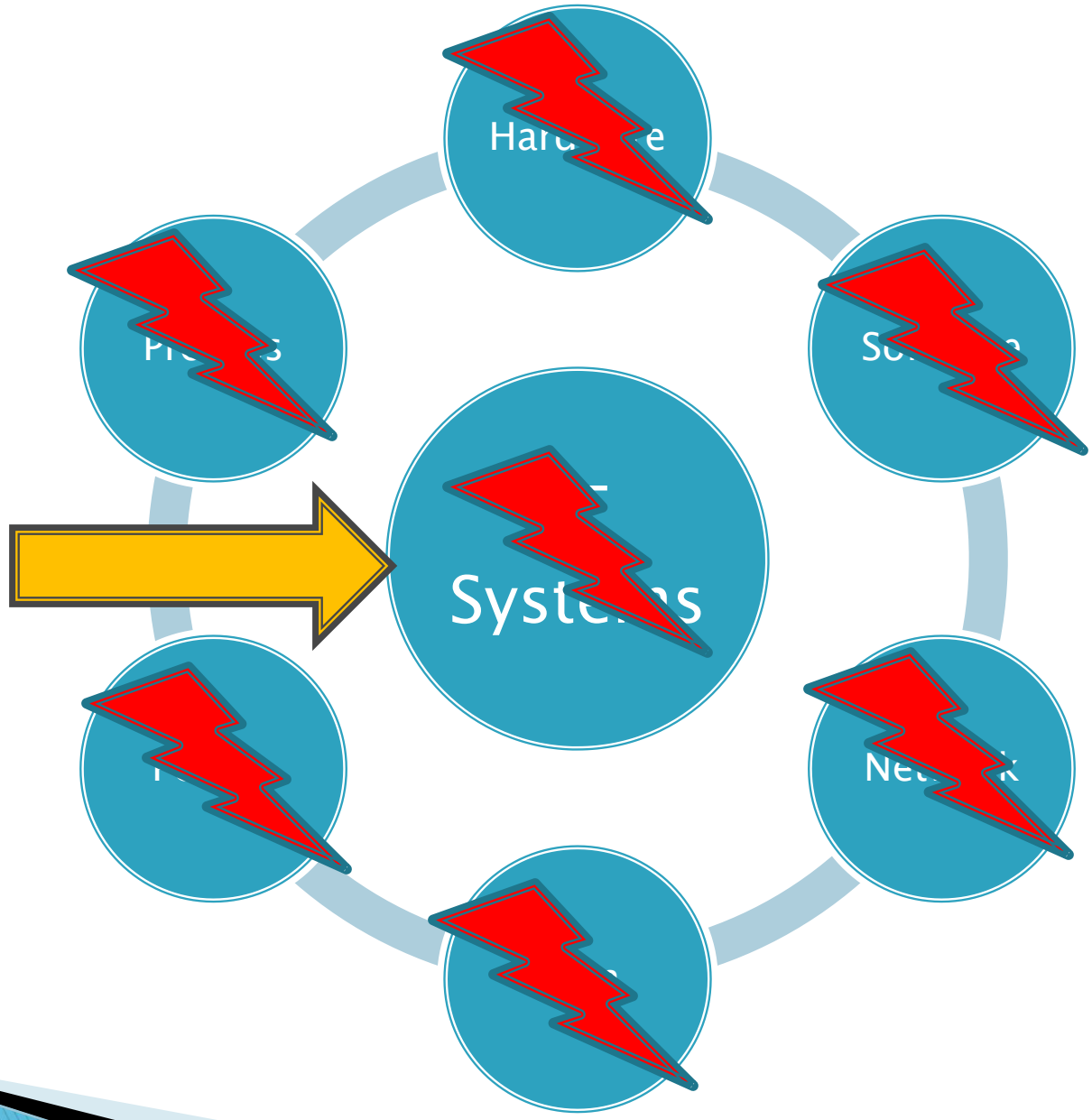
ดร. ธนัญชัย ตรีภาค


Security
Concept
Security
Standard / Procedure
CIA/AAA/PDR
non-repudiation
reliability
NIST SP800
ISO27001
Threats
Complex Attacks
No security
Security as optional / tools / replacement
Secure Design
Simple Attacks
Time
TCP/IP (1975)
HTTP/Mail/DNS
RIP
IEEE 802.11 (1997)
WPA,WPA2
VPN
Web Service
IPv6 (1998)
Web Service
Cloud


Hardware
Software
Network
Data
People
Process
IT Systems

สภาวะที่ระบบสารสนเทศมีความปลอดภัย ??

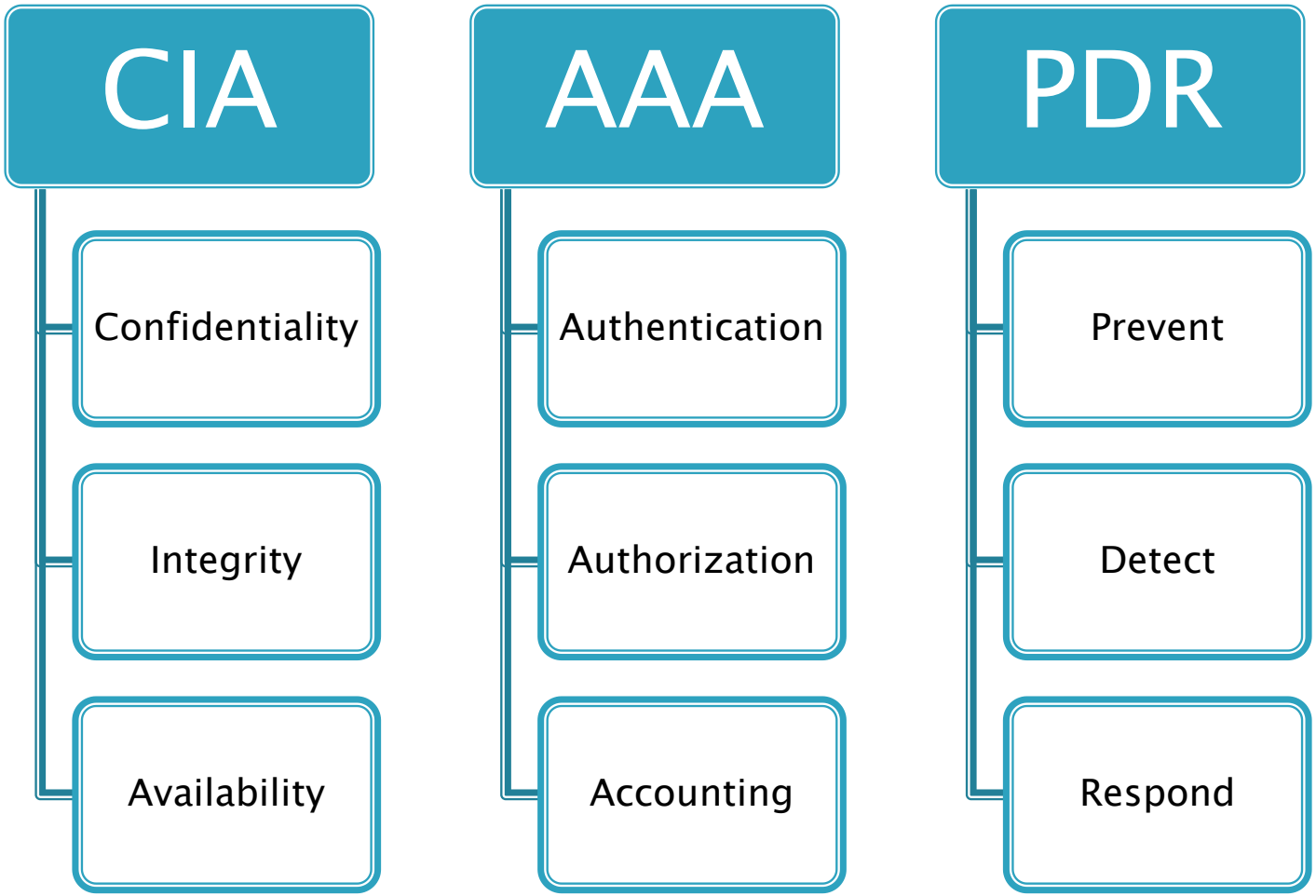
ภัยคุกคาม
สารสนเทศ



ภัยคุกคามสารสนเทศ

- ใช้เอกสาร 1. ตารางแจกแจงผลกระทบจากภัยคุกคาม
- ระบุ ภัยคุกคามสารสนเทศ 10 อันดับ และผลกระทบต่อระบบสารสนเทศ

Security Concept



Confidentiality

- “ข้อมูลใดที่เป็นความลับ จะต้องไม่ถูกเปิดเผยให้กับบุคคลอื่นที่ไม่มีสิทธิในการอ่านข้อมูลดังกล่าว”
- แนวทางการดำเนินการคือการเข้ารหัสข้อมูล (Encryption) แล้วให้เฉพาะบุคคลที่มี key/password เท่านั้นที่สามารถถอดรหัสข้อมูลดังกล่าวได้ (Decryption)

ตัวอย่าง Algorithm / เครื่องมือ / กลไกการทำงาน
ที่สร้าง confidentiality มีอะไรบ้าง ??

หลักการของ Confidentiality จะใช้รับมือกับภัยคุกคามลักษณะใดบ้าง ??

Integrity

- “ข้อมูลต้องมีความถูกต้อง สมบูรณ์ ไม่ถูกเปลี่ยนแปลง แก้ไข”
- แนวทางการคงไว้ซึ่ง Integrity คือการเพิ่มข้อมูล/กลไก ในการตรวจสอบความถูกต้องของข้อมูล

ตัวอย่าง Algorithm / เครื่องมือ / กลไกการทำงาน
ที่สร้าง Integrity มีอะไรบ้าง ??

หลักการของ Integrity จะใช้รับมือกับภัยคุกคามลักษณะใดบ้าง ??

Availability

- “ระบบงาน / ข้อมูล ต้องสามารถเรียกใช้งานได้ตามข้อกำหนดในการให้บริการ (SLA)”
- แนวทางการรักษา Availability คือการออกแบบระบบให้สามารถรองรับกับ
  - การเพิ่มขึ้นของ load
  - การโจมตีระบบ
  - อุบัติเหตุ ภัยพิบัติต่างๆ

ตัวอย่าง Algorithm / เครื่องมือ / กลไกการทำงาน
ที่เสริมสร้าง Availability มีอะไรบ้าง ??

หลักการของ Availability จะใช้รับมือกับภัยคุกคามลักษณะใดบ้าง ??

Authentication

- “การเข้าใช้งานระบบ / ทรัพยากรใดๆ จะต้องเป็นผู้ที่มีสิทธิในการเข้าใช้งานระบบ/ทรัพยากรนั้นๆ”
- แนวทางของ Authentication คือการให้แสดง
  - What you know / What you have / What you are
- สามารถให้แสดง 2 อย่างร่วมกันได้ (2-factors authentication) เพื่อเพิ่มความปลอดภัย

ตัวอย่าง Algorithm / เครื่องมือ / กลไกการทำงาน
ที่เสริมสร้าง Authentication มีอะไรบ้าง ??

หลักการของ Authentication จะใช้รับมือกับภัยคุกคามลักษณะใดบ้าง ??

Authorization

- “ระบบหรือทรัพยากรใด จะต้องระบุสิทธิในการเข้าถึง และมอบสิทธิในการเข้าถึงนั้นกับผู้ใช้งาน”
- แนวทางของ Authorization คือการจัดทำรายการของการใช้งานระบบ / ทรัพยากร , ทำการกำหนด Role ให้กับผู้ใช้งานแต่ละคน แล้วระบุว่าอนุญาตให้ Role ใดทำรายการใด / ใช้ทรัพยากรใดได้บ้าง

ตัวอย่าง Algorithm / เครื่องมือ / กลไกการทำงาน
ที่เสริมสร้าง Authorization มีอะไรบ้าง ??

หลักการของ Authorization จะใช้รับมือกับภัยคุกคามลักษณะใดบ้าง ??

Accounting

- “การทำงานใดๆ จะต้องสามารถตรวจสอบได้ว่าเกิดขึ้นได้อย่างไร โดยใคร ส่งผลกับอะไร ฯลฯ”
- แนวทางของ Accounting คือการบันทึก log เมื่อมีการเรียกใช้ ฟังก์ชั่น/ข้อมูล

ตัวอย่าง Algorithm / เครื่องมือ / กลไกการทำงาน
ที่เสริมสร้าง Accounting มีอะไรบ้าง ??

หลักการของ Accounting จะใช้รับมือกับภัยคุกคามลักษณะใดบ้าง ??

Prevent

- “ภัยคุกคามที่ทราบว่าจะเกิดขึ้น จะต้องมีการกำหนดการป้องกัน”

ตัวอย่าง Algorithm / เครื่องมือ / กลไกการทำงาน
ที่เสริมสร้าง Prevent มีอะไรบ้าง ??

หลักการของ Prevent จะใช้รับมือกับภัยคุกคามลักษณะใดบ้าง ??

Detect

- “ต้องมีกลไกในการตรวจจับภัยคุกคาม และแจ้งเตือนให้ผู้ดูแลระบบทราบ”

ตัวอย่าง Algorithm / เครื่องมือ / กลไกการทำงาน

ที่เสริมสร้าง Detect มีอะไรบ้าง ??

หลักการของ Detect จะใช้รับมือกับภัยคุกคามลักษณะใดบ้าง ??

Response

- “เมื่อมีการแจ้งเตือนจากขั้นตอนการ detect จะต้องมีการตอบสนองอย่างทันท่วงที”

ตัวอย่าง Algorithm / เครื่องมือ / กลไกการทำงาน

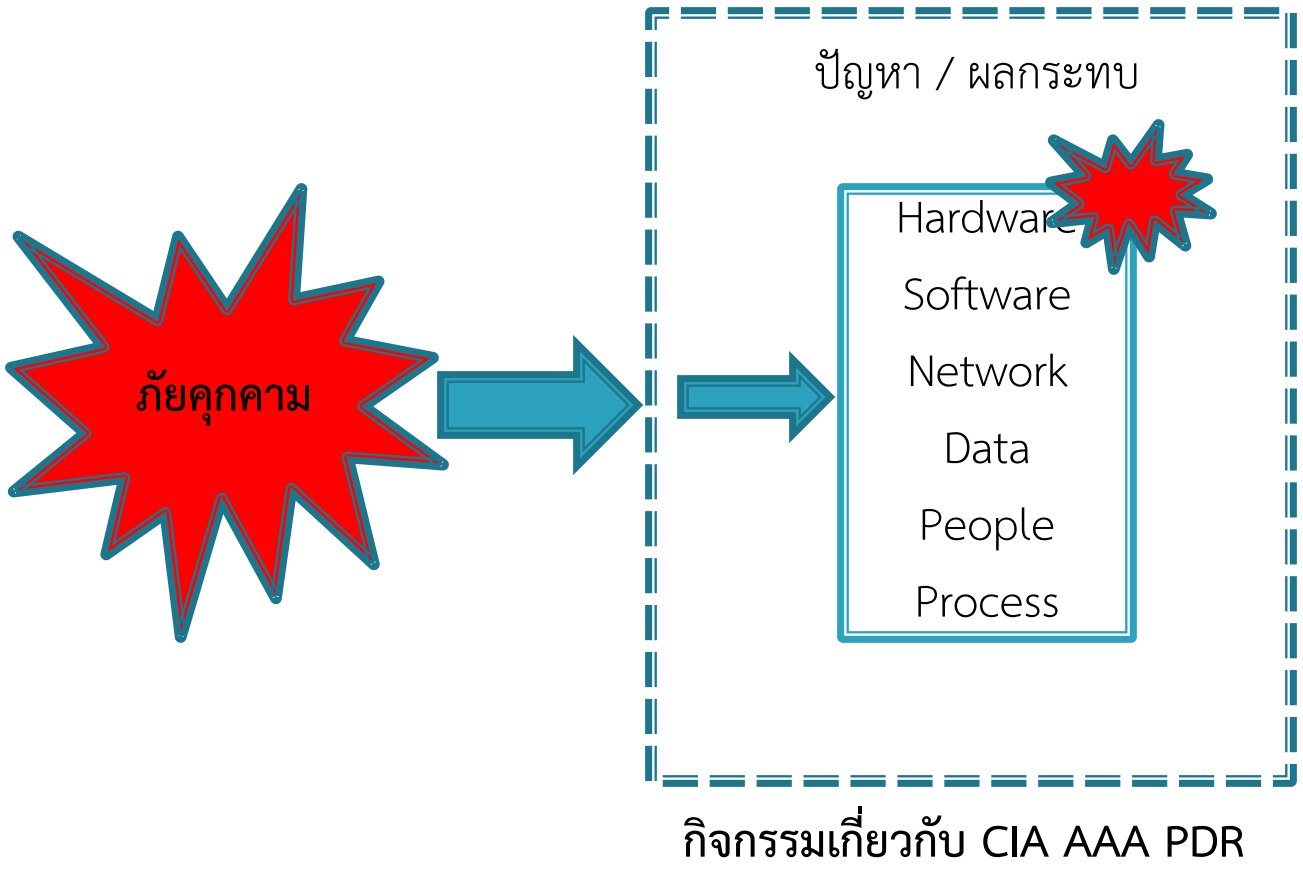
ที่เสริมสร้าง Response มีอะไรบ้าง ??

หลักการของ Response จะใช้รับมือกับภัยคุกคามลักษณะใดบ้าง ??

Security Concept / IT Component

Security Concept / IT Components	Confidentiality	Integrity	Availability	Authentication	Authorization	Accounting	Prevent	Detect	Respond
Hardware		X	X	X	X	X	X	X	X
Software		X	X	X	X	X	X	X	X
Network		X	X	X	X	X	X	X	X
Data	X	X	X	X	X	X	X	X	X
People		X	X	X	X	X	X	X	X
Process		X	X	X	X	X	X	X	X

Security Activities



กิจกรรมเกี่ยวกับ CIA AAA PDR

ภัยคุกคามกับ Security Concept

- ภัยคุกคามต่างๆ กระทบกับหลักการข้อใดบ้าง
- ยกตัวอย่างเช่น
  - ไฟฟ้าดับ -> ระบบหยุดทำงาน -> Availability
  - การลักลอบใช้งาน -> Authentication
- ใช้ตารางที่ 2 ภัยคุกคามกับการขาดหลักการด้าน Security
- ระบุว่าภัยคุกคาม มีสาเหตุจากการขาดหลักการข้อใด

กิจกรรมเพื่อส่งเสริมความปลอดภัย

- จากหลักการ CIA AAA PDR ใช้ตาราง 4 เพื่อระบุกิจกรรมส่งเสริมความปลอดภัย

กิจกรรมเพื่อรับมือภัยคุกคามที่ระบุ

- ใช้ตาราง 5 กิจกรรมเพื่อส่งเสริมความปลอดภัย เพื่อจัดการกับภัยคุกคามในตารางที่ 1 ตารางภัยคุกคาม

กิจกรรม / โครงการ ทั้งหมดที่ทำให้ระบบสารสนเทศมีความปลอดภัย ??

รายละเอียดสำคัญ ของ ISO27000:2005 (Annex A)

1. Security policy (5)
2. Organization of information security (6)
3. Asset management(7)
4. Human resources security (8)
5. Physical and environmental security (9)
6. Communications and operations management (10)
7. Access control (11)
8. Information systems acquisition, development and maintenance (12)
9. Information security incident management (13)
10. Business continuity management (14)
11. Compliance (15)