CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

Security Principles for Innovation Management

ดร.สุรเชษฐ์ สุชัยยะ
ผู้อำนวยการสมาคม
ส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ *(CIPAT)*

MYSURACHET.COM

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

MYSURACHET.COM

Surachet Suchaiya, PhD.

ประวัติการศึกษา ประวัติการทำงาน ความเชี่ยวชาญ ประสบการณ์ ประกาศนียบัตรการฝึกอบรมที่ได้รับ และงานวิจัยของอาจารย์

1 Security Principles for Innovation Management

MYSURACHET.COM

ดร.สุรเชษฐ์ สุชัยยะ
ผู้อำนวยการ
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ (CIPAT)

1 การรักษาความมั่นคงปลอดภัยสารสนเทศ

1.1 การจัดการสารสนเทศ (Information Management)

1.2 การจัดการอัตลักษณ์(Identity Management)

1.3 การยืนยันตัวตน (Authentication)

1.4 การควบคุมการเข้าถึง (Access Control)

1.5 การตรวจสอบและการติดตาม (Monitoring and Auditing)

1.6 การรักษาความมั่นคงปลอดภัยของแพลตฟอร์ม (Platform Security)

4 การรักษาความมั่นคงปลอดภัยสารสนเทศ

1.1 การจัดการสารสนเทศ (Information Management)

- การจัดเก็บข้อมูล (Data Storage)
- การป้องกันข้อมูล (Data Protection)
- การจัดการการเข้าถึง (Access Management)
- การบริหารความเสี่ยง (Risk Management)

1 การรักษาความมั่นคงปลอดภัยสารสนเทศ

1.1 การจัดการสารสนเทศ (Information Management)

1 การรักษาความมั่นคงปลอดภัยสารสนเทศ

1.1 การจัดการสารสนเทศ (Information Management)

- การจัดเก็บข้อมูล (Data Storage)
  - การเข้ารหัสข้อมูล (Data Encryption)
  - การสำรองข้อมูล (Data Backup)

1 การรักษาความมั่นคงปลอดภัยสารสนเทศ

1.1 การจัดการสารสนเทศ (Information Management)

- การป้องกันข้อมูล (Data Protection)
  - การควบคุมการเข้าถึง (Access Control)
  - การตรวจสอบและการติดตาม (Monitoring and Auditing)

1 การรักษาความมั่นคงปลอดภัยสารสนเทศ

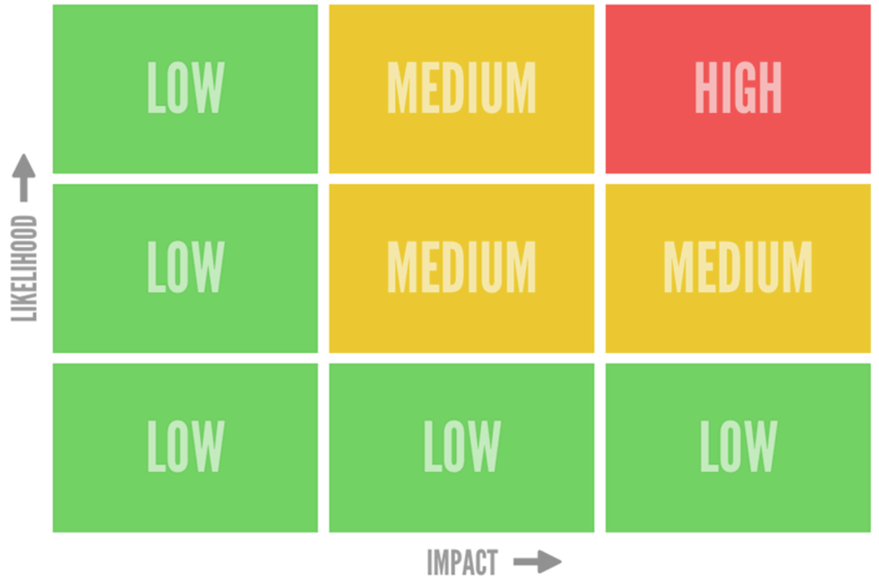
1.1 การจัดการสารสนเทศ (Information Management)

- การจัดการการเข้าถึง (Access Management)
  - การยืนยันตัวตน (Authentication)
  - การกำหนดสิทธิ์ (Authorization)
  - บัญชีรายชื่อผู้ใช้งาน (Account)

1 การรักษาความมั่นคงปลอดภัยสารสนเทศ

1.1 การจัดการสารสนเทศ (Information Management)

- การบริหารความเสี่ยง (Risk Management)
  - การประเมินความเสี่ยง (Risk Assessment)
  - การจัดการความเสี่ยง (Risk Mitigation)

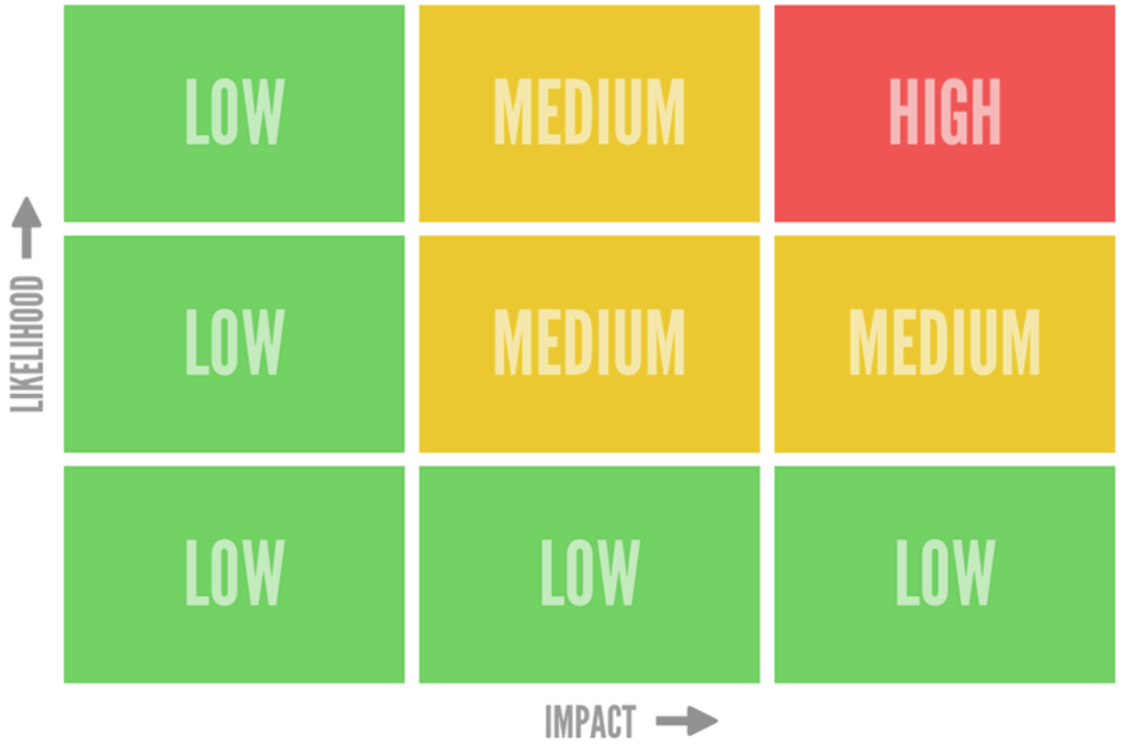


1 การรักษาความมั่นคงปลอดภัยสารสนเทศ

การประเมินความเสี่ยง (Risk Assessment)

พิจารณาระดับความเสี่ยง(Risk) = ผลกระทบ (I) x โอกาสที่จะเกิดภัย (L)

- Impact : ผลกระทบ
- Likelihood : โอกาสที่จะเกิดภัย



1 การรักษาความมั่นคงปลอดภัยสารสนเทศ

การประเมินความเสี่ยง (Risk Assessment)

No	Risk	Level

1 การรักษาความมั่นคงปลอดภัยสารสนเทศ

1.2 การจัดการอัตลักษณ์(Identity Management)

- การระบุอัตลักษณ์ (Identity Identification)
  - การลงทะเบียนผู้ใช้ (User Registration)
  - การจัดเก็บข้อมูลอัตลักษณ์ (Identity Data Storage)

1 การรักษาความมั่นคงปลอดภัยสารสนเทศ

1.3 การยืนยันตัวตน (Authentication)

Something you
KNOW

Password or phrase
PIN

Something you
HAVE

Code from app or SMS
Push notification
USB token

Something you
ARE

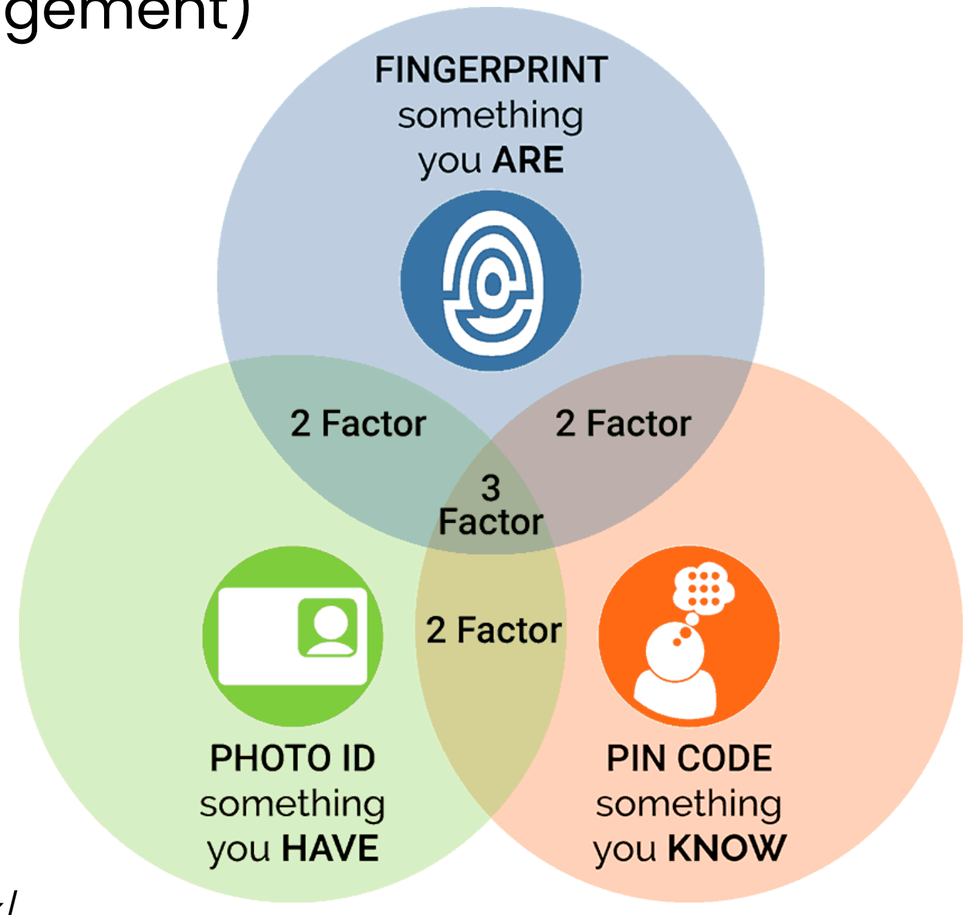
Finger or thumb print
Face scan
Iris scan

ข้อมูลจาก https://www.hsph.harvard.edu

1 การรักษาความมั่นคงปลอดภัยสารสนเทศ

1.3 การยืนยันตัวตน (Authentication)

- การยืนยันตัวตนแบบหลายขั้นตอน (Multi-Factor Authentication - MFA)
- การจัดการรหัสผ่าน (Password Management)



ข้อมูลจาก https://www.borer.co.uk/

1 การรักษาความมั่นคงปลอดภัยสารสนเทศ

1.4 การควบคุมการเข้าถึง (Access Control)

- การกำหนดสิทธิ์ตามบทบาท (Role-Based Access Control - RBAC)
- การควบคุมการเข้าถึงตามคุณลักษณะ (Attribute-Based Access Control - ABAC)
- การควบคุมการเข้าถึงตามลำดับบังคับบัญชา Mandatory Access Control (MAC)

1 การรักษาความมั่นคงปลอดภัยสารสนเทศ

1.4 การควบคุมการเข้าถึง (Access Control)

- การกำหนดสิทธิ์ตามบทบาท (Role-Based Access Control - RBAC)
  - การเข้าถึงตามบทบาทของพนักงาน เช่น ผู้จัดการ, พนักงานขาย, ผู้ดูแลระบบ

1 การรักษาความมั่นคงปลอดภัยสารสนเทศ

1.4 การควบคุมการเข้าถึง (Access Control)

- การควบคุมการเข้าถึงตามคุณลักษณะ (Attribute-Based Access Control - ABAC)
  - อนุญาตให้เข้าถึงทรัพยากรเฉพาะในช่วงเวลาทำงานหรือจากที่ตั้งที่เฉพาะเจาะจง

1 การรักษาความมั่นคงปลอดภัยสารสนเทศ

1.4 การควบคุมการเข้าถึง (Access Control)

- การควบคุมการเข้าถึงตามลำดับบังคับบัญชา Mandatory Access Control (MAC)
  - เป็นการควบคุมระบบความมั่นคงปลอดภัยระดับสูง เช่น กองทัพหรือหน่วยงานภาครัฐ ที่มีการกำหนดระดับชั้นความลับและสิทธิ์การเข้าถึงตามระดับความลับตามลำดับตำแหน่งบังคับบัญชา

1 การรักษาความมั่นคงปลอดภัยสารสนเทศ

1.5 การตรวจสอบและการติดตาม (Monitoring and Auditing)

- การตรวจสอบการเข้าถึง (Access Logging)
- การวิเคราะห์และการรายงาน (Analysis and Reporting)

1 การรักษาความมั่นคงปลอดภัยสารสนเทศ

1.6 การรักษาความมั่นคงปลอดภัยของแพลตฟอร์ม (Platform Security)

- การรักษาความมั่นคงปลอดภัยระบบปฏิบัติการ (Operating System Security)
- การรักษาความมั่นคงปลอดภัยซอฟต์แวร์ (Software Security)
- การรักษาความมั่นคงปลอดภัยฮาร์ดแวร์ (Hardware Security)
- การตรวจสอบและการติดตาม (Monitoring and Auditing)
- การบริหารความเสี่ยง (Risk Management)

1 การรักษาความมั่นคงปลอดภัยสารสนเทศ

1.6 การรักษาความมั่นคงปลอดภัยของแพลตฟอร์ม (Platform Security)

- การรักษาความมั่นคงปลอดภัยระบบปฏิบัติการ (Operating System Security)
  - การอัปเดตและแพทช์ระบบ (System Updates and Patches)
  - การกำหนดค่าอย่างปลอดภัย (Secure Configuration)

1 การรักษาความมั่นคงปลอดภัยสารสนเทศ

1.6 การรักษาความมั่นคงปลอดภัยของแพลตฟอร์ม (Platform Security)

- การรักษาความมั่นคงปลอดภัยซอฟต์แวร์ (Software Security)
  - การพัฒนาซอฟต์แวร์อย่างปลอดภัย (Secure Software Development)
  - การตรวจสอบช่องโหว่ (Vulnerability Scanning)

1 การรักษาความมั่นคงปลอดภัยสารสนเทศ

1.6 การรักษาความมั่นคงปลอดภัยของแพลตฟอร์ม (Platform Security)

- การรักษาความมั่นคงปลอดภัยฮาร์ดแวร์ (Hardware Security)
  - การควบคุมการเข้าถึงฮาร์ดแวร์ (Hardware Access Control)
  - การใช้เทคโนโลยีรักษาความมั่นคงปลอดภัย (Security Technologies)

1 การรักษาความมั่นคงปลอดภัยสารสนเทศ

1.6 การรักษาความมั่นคงปลอดภัยของแพลตฟอร์ม (Platform Security)

- การตรวจสอบและการติดตาม (Monitoring and Auditing)
  - การบันทึกเหตุการณ์ (Event Logging)
  - การตรวจสอบเหตุการณ์ (Event Monitoring)

1 การรักษาความมั่นคงปลอดภัยสารสนเทศ

1.6 การรักษาความมั่นคงปลอดภัยของแพลตฟอร์ม (Platform Security)

- การบริหารความเสี่ยง (Risk Management)
  - การประเมินความเสี่ยง (Risk Assessment)
  - การจัดการความเสี่ยง (Risk Mitigation)

1 การรักษาความมั่นคงปลอดภัยสารสนเทศ

สรุปบทเรียน : การรักษาความมั่นคงปลอดภัยสารสนเทศ

- การรักษาความลับของข้อมูล (Confidentiality)
- ความถูกต้องของข้อมูล (Integrity)
- ความพร้อมใช้งานของข้อมูล (Availability)
- การจัดการอัตลักษณ์และสิทธิ์การเข้าถึงของผู้ใช้ (Identity Management)
- การยืนยันตัวตน (Authentication)
- การควบคุมการเข้าถึง (Access Control)
- การรักษาความมั่นคงปลอดภัยของแพลตฟอร์ม (Platform Security)

1 การรักษาความมั่นคงปลอดภัยสารสนเทศ

Workshop Question 1

บริบท: บริษัท ABC Technology มีฐานลูกค้ามากมายทั่วโลกและข้อมูลของลูกค้าถูกจัดเก็บไว้ในศูนย์ข้อมูลที่ตั้งอยู่ในหลายประเทศ บริษัทต้องการยกระดับความปลอดภัยของข้อมูลและระบบของตนให้แข็งแกร่งยิ่งขึ้นเพื่อรับมือกับภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้นและเปลี่ยนแปลงอย่างต่อเนื่อง

โจทย์ 1 : การประเมินและปรับปรุงระบบให้เป็นไปตามหลัก CIA Triad

1.วิเคราะห์และประเมินระบบปัจจุบันของบริษัท ABC Technology ในด้านความลับ (Confidentiality), ความสมบูรณ์ (Integrity), และความพร้อมใช้งาน (Availability).

2.สร้างแผนการปรับปรุงระบบที่จะช่วยเพิ่มความปลอดภัยข้อมูลโดยอาศัยหลักการ CIA Triad พร้อมอธิบายถึงผลกระทบและประโยชน์ที่บริษัทจะได้รับจากการปรับปรุงนี้

1 การรักษาความมั่นคงปลอดภัยสารสนเทศ

Workshop Question 2

บริบท: บริษัท ABC Technology มีฐานลูกค้ามากมายทั่วโลกและข้อมูลของลูกค้าถูกจัดเก็บไว้ในศูนย์ข้อมูลที่ตั้งอยู่ในหลายประเทศ บริษัทต้องการยกระดับความปลอดภัยของข้อมูลและระบบของตนให้แข็งแกร่งยิ่งขึ้นเพื่อรับมือกับภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้นและเปลี่ยนแปลงอย่างต่อเนื่อง

โจทย์ 2 : การออกแบบและพัฒนานโยบายความมั่นคงปลอดภัยใหม่

1.ออกแบบนโยบายความมั่นคงปลอดภัยเพื่อรับมือกับภัยคุกคามใหม่ๆ ที่อาจเกิดขึ้น นโยบายควรครอบคลุมทั้งการป้องกัน การตรวจจับ และการตอบสนองต่อเหตุการณ์

2.อธิบายว่านโยบายใหม่นี้จะช่วยให้บริษัทสามารถปกป้องข้อมูลและระบบได้อย่างไร รวมถึงวิธีการที่จะใช้เพื่อประเมินและตรวจสอบประสิทธิภาพของนโยบาย

1 การรักษาความมั่นคงปลอดภัยสารสนเทศ

Workshop Question 3

บริบท: บริษัท ABC Technology มีฐานลูกค้ามากมายทั่วโลกและข้อมูลของลูกค้าถูกจัดเก็บไว้ในศูนย์ข้อมูลที่ตั้งอยู่ในหลายประเทศ บริษัทต้องการยกระดับความปลอดภัยของข้อมูลและระบบของตนให้แข็งแกร่งยิ่งขึ้นเพื่อรับมือกับภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้นและเปลี่ยนแปลงอย่างต่อเนื่อง

โจทย์ 3 : การออกแบบและพัฒนานโยบายความมั่นคงปลอดภัยใหม่

1.จัดทำการวิเคราะห์ความเสี่ยงของระบบสารสนเทศของบริษัท ABC Technology พิจารณาถึงทั้งภัยคุกคามภายในและภายนอก

2.ออกแบบแผนการจัดการความเสี่ยงที่จะใช้ป้องกันและบรรเทาความเสี่ยงที่ระบุได้ แผนควรรวมถึงวิธีการตรวจสอบและปรับปรุงแผนการจัดการความเสี่ยงอย่างต่อเนื่อง