MYSURACHET.COM

# Risk Analysis Process in Cybersecurity


## Instructor :
## Surachet Suchaiya
## PhD. Innovation MGT


www.MySurachet.cmom

# Risk Analysis Process in Cybersecuritysite

MYSURACHET.COM

## Agenda

1. Introduction
2. Steps in Risk Analysis
3. Risk Management Strategies
4. Workshop

# Introduction

MYSURACHET.COM

# 1.Introduction

MYSURACHET.COM

1.1 นิยามของความเสี่ยงด้านไซเบอร์ (Cyber Risk)

1.2 องค์ประกอบของความเสี่ยงด้านไซเบอร์

1.3 ประเภทของความเสี่ยงด้านไซเบอร์

1.4 ความสำคัญของการจัดการความเสี่ยงด้านไซเบอร์

# 1.Introduction

MYSURACHET.COM

1.1 บทนำสู่การวิเคราะห์ความเสี่ยงใน Cybersecurity

- ความหมายและความสำคัญของการวิเคราะห์ความเสี่ยงในด้าน Cybersecurity
- เป้าหมายของการวิเคราะห์ความเสี่ยงในองค์กรด้าน IT
- ตัวอย่างเหตุการณ์ที่เกิดจากการไม่วิเคราะห์ความเสี่ยงใน Cybersecurity

# 1.Introduction

MYSURACHET.COM

1.2 องค์ประกอบของความเสี่ยงด้านไซเบอร์

- ภัยคุกคาม (Threats): สาเหตุที่อาจทำให้เกิดการโจมตี เช่น แฮกเกอร์ มัลแวร์ ฟิชชิง หรือภัยธรรมชาติ
- ช่องโหว่ (Vulnerabilities): จุดอ่อนในระบบหรือซอฟต์แวร์ที่ทำให้สามารถถูกโจมตีได้ เช่น ซอฟต์แวร์ที่ไม่ได้รับการอัปเดต การตั้งค่าที่ไม่ปลอดภัย
- ผลกระทบ (Impact): ผลลัพธ์ที่เกิดขึ้นจากการโจมตี เช่น การสูญเสียข้อมูล การหยุดชะงักของบริการ หรือความเสียหายต่อชื่อเสียงขององค์กร

# 1.Introduction

MYSURACHET.COM

1.3 ประเภทของความเสี่ยงด้านไซเบอร์

- ความเสี่ยงจากการโจมตี (Attack Risks): ความเสี่ยงที่เกิดจากการโจมตีโดยตรง เช่น การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- ความเสี่ยงจากการละเมิดข้อมูล (Data Breach Risks): ความเสี่ยงที่เกิดจากการเปิดเผยข้อมูลที่เป็นความลับหรือข้อมูลส่วนบุคคล
- ความเสี่ยงจากการไม่ปฏิบัติตามกฎหมาย (Compliance Risks): ความเสี่ยงที่เกิดจากการไม่ปฏิบัติตามกฎหมายและข้อบังคับด้านความปลอดภัยไซเบอร์

# 1.Introduction

MYSURACHET.COM

1.4 ความสำคัญของการจัดการความเสี่ยงด้านไซเบอร์

- ช่วยป้องกันและลดผลกระทบจากการโจมตีทางไซเบอร์
- เสริมสร้างความเชื่อมั่นให้กับลูกค้าและผู้มีส่วนได้ส่วนเสีย
- ปกป้องทรัพย์สินทางปัญญาและข้อมูลสำคัญขององค์กร

# 2.Steps in Risk Analysis

MYSURACHET.COM

2.1 การระบุทรัพย์สิน (Asset Identification)

2.2 การระบุความเสี่ยง (Risk Identification)

2.3 ประเมินความเสี่ยง (Risk Assessment)

2.4 การวิเคราะห์ความเสี่ยง (Risk Analysis)

# 2.Steps in Risk Analysis

MYSURACHET.COM

## 2.1 การระบุทรัพย์สิน (Asset Identification)

- การสร้างรายการทรัพย์สินทางเทคโนโลยีสารสนเทศที่สำคัญ
- การทำแผนผังระบบเครือข่ายเพื่อช่วยในการระบุภัยคุกคาม

# 2.Steps in Risk Analysis

MYSURACHET.COM

## 2.2 การระบุความเสี่ยง (Risk Identification)

- วิธีการระบุภัยคุกคามและช่องโหว่
- กระบวนการระบุความเสี่ยง (Risk Identification Process)

# 2.Steps in Risk Analysis

MYSURACHET.COM

## 2.2 การระบุความเสี่ยง (Risk Identification)

### กระบวนการระบุความเสี่ยง (Risk Identification Process)

- ขั้นตอนการระบุความเสี่ยง
  - กำหนดขอบเขตและบริบท: กำหนดขอบเขตของการวิเคราะห์ความเสี่ยงและบริบทที่เกี่ยวข้องกับองค์กรหรือระบบ
  - ระบุทรัพย์สิน: จำแนกและบันทึกทรัพย์สินทุกประเภทขององค์กรที่ต้องการปกป้อง

# 2.Steps in Risk Analysis

MYSURACHET.COM

## 2.2 การระบุความเสี่ยง (Risk Identification)

### กระบวนการระบุความเสี่ยง (Risk Identification Process)

- การระบุภัยคุกคามและจุดอ่อน
  - การระบุภัยคุกคาม: การตรวจสอบภัยคุกคามที่อาจเกิดขึ้น เช่น ไวรัสคอมพิวเตอร์ การโจมตีแบบ phishing, ฯลฯ
  - การระบุจุดอ่อน: ตรวจจับจุดอ่อนภายในระบบหรือกระบวนการที่อาจทำให้เกิดความเสี่ยง

# 2.Steps in Risk Analysis

MYSURACHET.COM

## 2.2 การระบุความเสี่ยง (Risk Identification)

### กระบวนการระบุความเสี่ยง (Risk Identification Process)

- เครื่องมือและเทคนิคการระบุความเสี่ยง
  - เครื่องมือการวิเคราะห์: นำเสนอเครื่องมือที่ใช้ในการระบุความเสี่ยง เช่น ซอฟต์แวร์สแกนเนอร์, การวิเคราะห์ข้อมูลบิ๊กดาต้า
  - เทคนิคการระบุความเสี่ยง: เช่น การสัมภาษณ์ผู้เชี่ยวชาญ, การวิเคราะห์เอกสาร, การทำแบบสำรวจ

# 2.Steps in Risk Analysis

MYSURACHET.COM

## 2.2 การระบุความเสี่ยง (Risk Identification)

## กระบวนการระบุความเสี่ยง (Risk Identification Process)

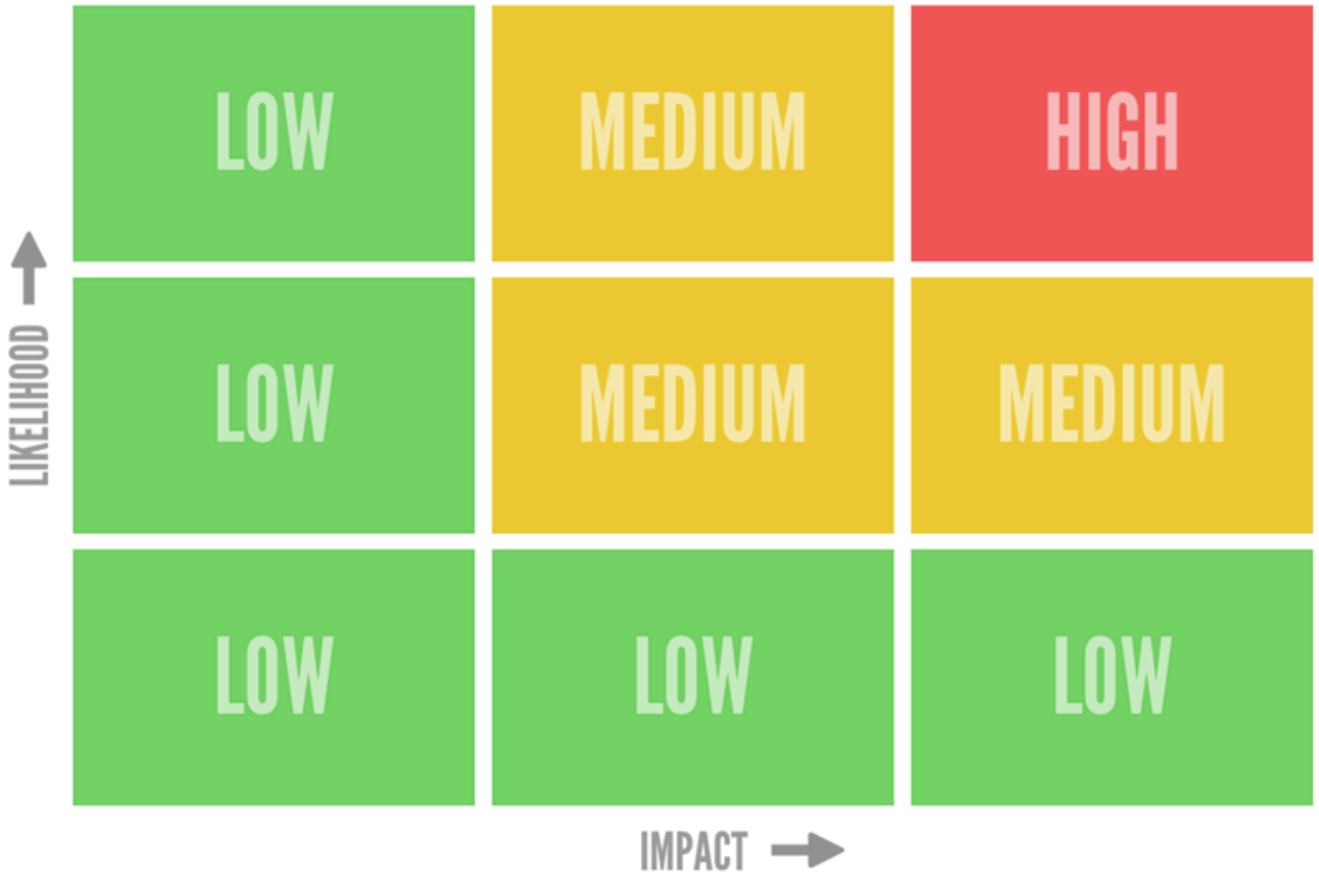
- การวิเคราะห์และการสรุป
  - การวิเคราะห์ข้อมูลที่ได้: วิธีการประมวลผลข้อมูลจากการระบุความเสี่ยงเพื่อกำหนดความสำคัญและความเร่งด่วน
  - การสรุป: ทบทวนเนื้อหาที่ได้กล่าวถึงและเปิดโอกาสให้ผู้เรียนถามคำถามและแสดงความคิดเห็น

# 2.Steps in Risk Analysis

MYSURACHET.COM

2.3 การประเมินความเสี่ยง (Risk Assessment)

- การใช้เครื่องมือในการประเมินความเสี่ยง เช่น Risk Matrix เพื่อจัดลำดับความสำคัญของความเสี่ยง



# 2.Steps in Risk Analysis

MYSURACHET.COM

## 2.4 การวิเคราะห์ความเสี่ยง (Risk Analysis)

- การประเมินผลกระทบที่อาจเกิดขึ้นจากภัยคุกคาม
- การจัดลำดับความเสี่ยงตามระดับของความน่าจะเป็นและผลกระทบ

# 3.Risk Management Strategies

MYSURACHET.COM

3.1 แนวทางในการจัดการความเสี่ยง

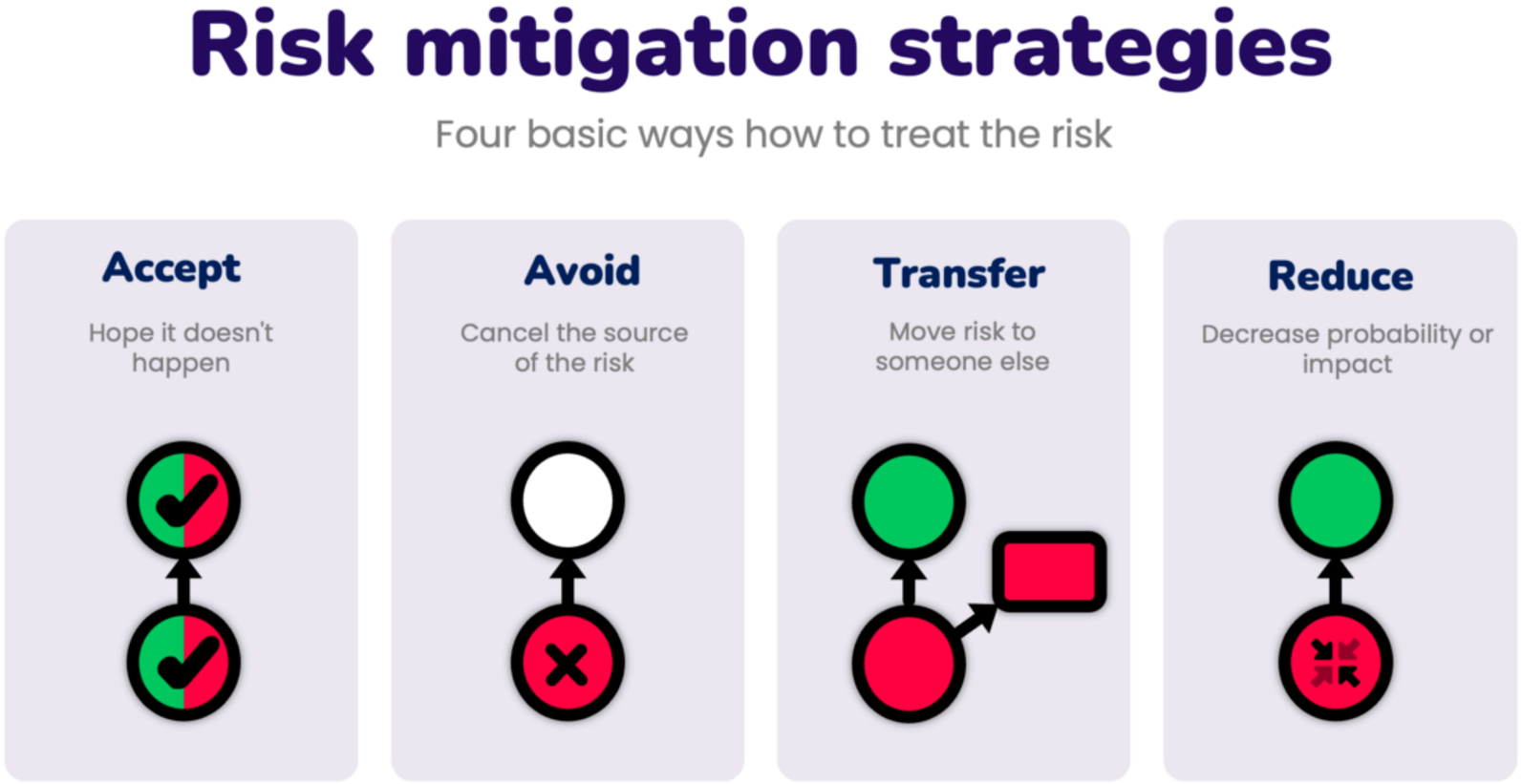
3.2 การติดตามและตรวจสอบสถานะของความเสี่ยง

# 3.Risk Management Strategies

MYSURACHET.COM

## 3.1 แนวทางในการจัดการความเสี่ยง

- การพัฒนาแผนตอบสนองต่อเหตุการณ์เพื่อเตรียมพร้อมสำหรับภัยคุกคาม



# 3.Risk Management Strategies

MYSURACHET.COM

## 3.2 การติดตามและตรวจสอบสถานะของความเสี่ยง

- ความสำคัญของการติดตามเพื่อปรับปรุงกลยุทธ์การจัดการความเสี่ยง
- วิธีการใช้เครื่องมือในการติดตามสถานะของความเสี่ยง

# 4.Workshop


TRAINING
GOAL
IDEA
SKILLS
WORKSHOP
TEAM
PRACTICE
RESULTS
TREND

# 4.Workshop

MYSURACHET.COM

กิจกรรมกลุ่ม: ให้ผู้เรียนร่วมกันระบุและประเมินความเสี่ยงในสถานการณ์สมมติ

**Case Study** : การโจมตีทางไซเบอร์ต่อองค์กรด้านโครงสร้างพื้นฐาน

**Background** : ในช่วงปีที่ผ่านมา หน่วยงานโครงสร้างพื้นฐานสำคัญในประเทศไทย เช่น โรงไฟฟ้าและระบบการขนส่งสาธารณะ ถูกโจมตีทางไซเบอร์อย่างรุนแรง โดยเฉพาะในช่วงที่มีการทำงานจากที่บ้าน (Work from Home) เนื่องจากสถานการณ์ COVID-19 ส่งผลให้การรักษาความปลอดภัยไซเบอร์มีความซับซ้อนมากขึ้น ข้อมูลจากกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีระบุว่ามีการแจ้งความเกี่ยวกับการโจมตีทางไซเบอร์กว่า 44,000 คดีในช่วง 4 เดือนที่ผ่านมา

# 4.Workshop

MYSURACHET.COM

กิจกรรมกลุ่ม: ให้ผู้เรียนร่วมกันระบุและประเมินความเสี่ยงในสถานการณ์สมมติ

**Case Study** : การโจมตีทางไซเบอร์ต่อองค์กรด้านโครงสร้างพื้นฐาน

**Event** : องค์กรหนึ่งในภาคการขนส่งสาธารณะได้รับผลกระทบจากการโจมตีในรูปแบบ Ransomware Attack ที่เรียกว่า "Triple Extortion Ransomware" ซึ่งแฮกเกอร์ได้เข้าถึงระบบข้อมูลขององค์กรและเข้ารหัสข้อมูลสำคัญ ทำให้ไม่สามารถเข้าถึงข้อมูลได้ โดยแฮกเกอร์เรียกค่าไถ่ในการปลดล็อกข้อมูล หลังจากนั้นยังขู่ว่าจะเผยแพร่ข้อมูลลูกค้าบน Dark Web หากองค์กรไม่จ่ายเงินตามที่เรียกร้อง

# 4.Workshop

MYSURACHET.COM

กิจกรรมกลุ่ม: ให้ผู้เรียนร่วมกันระบุและประเมินความเสี่ยงในสถานการณ์สมมติ

**Case Study** : การโจมตีทางไซเบอร์ต่อองค์กรด้านโครงสร้างพื้นฐาน

**Questions for Analysis** :

4.1 **การระบุความเสี่ยง** : นักศึกษาโปรดระบุและวิเคราะห์ความเสี่ยงที่องค์กรนี้เผชิญอยู่ รวมถึงช่องโหว่ที่ทำให้เกิดการโจมตี

4.2 **กลยุทธ์การตอบสนอง** : องค์กรควรมีแนวทางใดในการจัดการกับเหตุการณ์นี้? โปรดเสนอแผนการตอบสนองต่อเหตุการณ์และวิธีการฟื้นฟูระบบ

4.3 **ผลกระทบต่อผู้มีส่วนได้ส่วนเสีย** : วิเคราะห์ผลกระทบที่เกิดขึ้นต่อผู้มีส่วนได้ส่วนเสีย เช่น ลูกค้า พนักงาน และสังคมโดยรวม

4.4 **มาตรการป้องกันในอนาคต** : เสนอแนวทางในการปรับปรุงระบบรักษาความปลอดภัยไซเบอร์ขององค์กรเพื่อป้องกันเหตุการณ์ในลักษณะเดียวกันในอนาคต

4.5 **บทเรียนที่ได้** : นักศึกษาโปรดสรุปบทเรียนที่องค์กรสามารถเรียนรู้จากเหตุการณ์นี้เพื่อปรับปรุงกระบวนการบริหารจัดการความเสี่ยงทางไซเบอร์

MYSURACHET.COM

# Thank You

## Let’s Connect with Us!

www.MySurachet.com

Biz Card Contact