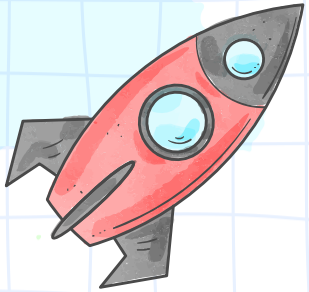
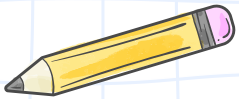


DGA309

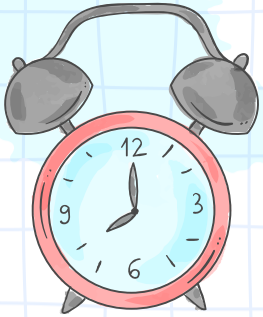
หลักสูตรการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับผู้ปฏิบัติงานด้านเทคโนโลยี



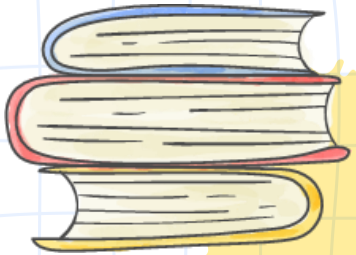
ผู้เข้าอบรม

1. นายกฤตภพ อัครวินทวงศ์
2. นายสุรศักดิ์ แย้มเนตร
3. นายชยารพ บุญมัติ
4. นางสาวสรัณรัตน์ อุษณกรกุล
5. นายกษิดิศ จุฑาภูวดล

CONTENTS



Overview Cyber Security



Overview Cyber Security สถิติอาชญากรรมทางไซเบอร์

Cybercrime Statistics 2024

$10.5 Trillion
projected cost of cybercrimes by 2025.

$30 billion
Cost of Crypto-crime annually by 2025.

$1.5 Trillion
Amount **earned by cybercriminals** for cybercrime activities yearly.

80%
of cybercrimes are **phishing attacks** in the technology sector.

2.7 billion hours
Total time **spent resolving cybercrimes;** average of 6.7 hours daily.

$5.09 Million
Is the highest cost of a data breach in U.S.A. in 2023.

$265 Billion is the estimated annual cost of ransomware to victims by 2031.

astra

Overview Cyber Security สถิติภัยคุกคามทางไซเบอร์ ปี 2567

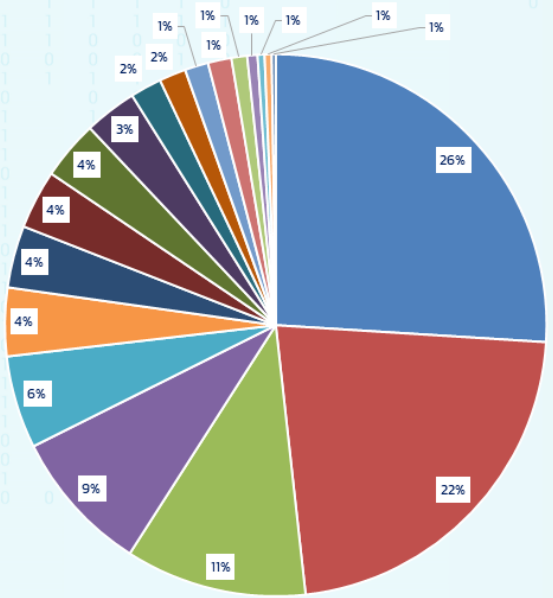
National Cyber Security Agency

สถิติภัยคุกคามทางไซเบอร์ประจำปี พ.ศ. 2567

มกราคม 2567 – ธันวาคม 2567

รวมทั้งสิ้น 2,135 เหตุการณ์

การศึกษา	555
หน่วยงานของรัฐ ด้านอื่นๆ	475
การเงินการธนาคาร	231
ผู้ประกอบการพาณิชย์ที่เป็นบริษัทเอกชน สัญชาติไทย	183
พลังงานและสาธารณูปโภค	118
แจ้งเตือนทุกหน่วยงานภายใต้ พ.ร.บ.ไซเบอร์ฯ	87
ขนส่งและโลจิสติกส์	79
ความมั่นคง	75
สาธารณสุข	75
เทคโนโลยีสารสนเทศและโทรคมนาคม	67
อื่นๆ	40
บริการภาครัฐ	34
ผู้ผลิตซอฟต์แวร์ ระบบ หรืออุปกรณ์ทางเทคโนโลยี	30
ผู้ประกอบการพาณิชต่างประเทศที่มีที่ตั้งในประเทศไทย	30
ผู้ประกอบการธุรกิจอีคอมเมิร์ช	20
ผู้ประกอบกิจการให้เช่าพื้นที่เว็บไซต์หรือที่เป็นดาต้าเซ็นเตอร์	13
กลุ่มจัดตั้ง ชมรม สมาคม	9
ผู้ให้บริการโซเชียลมีเดีย	9
เว็บไซต์ที่มีการสมาชิกหรือใช้เป็นเว็บบอร์ด	5



- การศึกษา
- หน่วยงานของรัฐ ด้านอื่นๆ
- การเงินการธนาคาร
- ผู้ประกอบการพาณิชย์ที่เป็นบริษัทเอกชน สัญชาติไทย
- พลังงานและสาธารณูปโภค
- แจ้งเตือนทุกหน่วยงานภายใต้ พ.ร.บ.ไซเบอร์ฯ
- ขนส่งและโลจิสติกส์
- ความมั่นคง
- สาธารณสุข
- เทคโนโลยีสารสนเทศและโทรคมนาคม
- อื่นๆ
- บริการภาครัฐ
- ผู้ผลิตซอฟต์แวร์ ระบบ หรืออุปกรณ์ทางเทคโนโลยี
- ผู้ประกอบการพาณิชต่างประเทศที่มีที่ตั้งในประเทศไทย
- ผู้ประกอบการธุรกิจอีคอมเมิร์ช
- ผู้ประกอบกิจการให้เช่าพื้นที่เว็บไซต์หรือที่เป็นดาต้าเซ็นเตอร์
- กลุ่มจัดตั้ง ชมรม สมาคม
- ผู้ให้บริการโซเชียลมีเดีย
- เว็บไซต์ที่มีการสมาชิกหรือใช้เป็นเว็บบอร์ด

ThaiCERT
Thailand Computer Emergency Response Team
By NCSA Thailand

หมายเหตุ – หน่วยงานการเงินการธนาคารลักษณะภัยคุกคามถูกปลอมแปลงหน้าเว็บไซต์ เพื่อใช้หลอกลวงประชาชน

Overview Cyber Security สถิติภัยคุกคามทางไซเบอร์ ปี 2567

National Cyber Security Agency

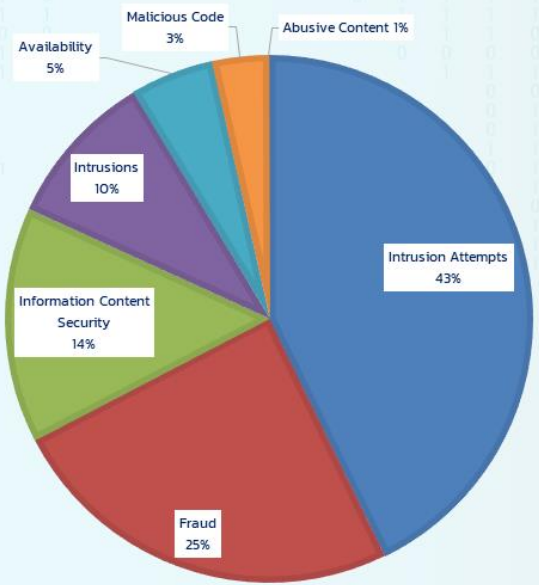
สถิติภัยคุกคามทางไซเบอร์ ประจำปี พ.ศ. 2567

NCSA สกมช

มกราคม 2567 – ธันวาคม 2567

รวมทั้งสิ้น 2,135 เหตุการณ์

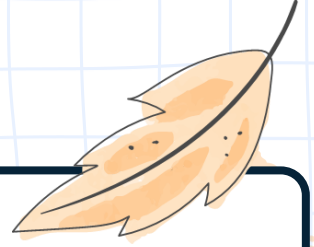
Intrusion Attempts	913
Fraud	525
Information Content Security	309
Intrusions	205
Availability	109
Malicious Code	73
Abusive Content	1



ThaiCERT
By NCSA Thailand

หมายเหตุ – อ้างอิง Incident Class ตาม enisa

Overview Cyber Security



Information Security

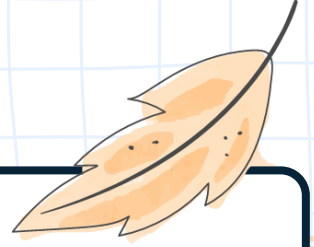
คือ การปกป้องความลับ ความสมบูรณ์ และความพร้อมใช้งาน (CIA) ของข้อมูล ระบบ และสารสนเทศจากภัยคุกคาม การโจมตี และช่องโหว่ต่าง ๆ ซึ่งรวมถึงการปฏิบัติ แนวทาง และเทคโนโลยีต่าง ๆ ที่ออกแบบมาเพื่อปกป้องข้อมูล ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และทำให้ระบบสามารถต้านทานการทำลายหรือการหยุดชะงักได้

Overview Cyber Security

Cyber Security

คือ กระบวนการและมาตรการที่ใช้ในการปกป้องข้อมูล ระบบคอมพิวเตอร์ และเครือข่ายจากการโจมตีและภัยคุกคามทางไซเบอร์

Overview Cyber Security (CIA) 1/4



CIA

ย่อมาจาก “Confidentiality, Integrity และ Availability” ซึ่งเป็นแนวคิดหลักสามประการในด้านความมั่นคงปลอดภัยทางไซเบอร์

Overview Cyber Security (CIA) 2/4

Confidentiality

ความลับ

- การมั่นใจว่าข้อมูลสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

เช่น การเข้ารหัส การควบคุมการเข้าถึง และการใช้ระบบยืนยันตัวตนที่ปลอดภัย

ตัวอย่าง: การใช้รหัสผ่านที่แข็งแรงหรือการยืนยันตัวตนสองขั้นตอน (MFA) เพื่อให้แน่ใจว่าเฉพาะผู้ที่ได้รับอนุญาตสามารถเข้าถึงไฟล์ที่สำคัญได้

Overview Cyber Security (CIA) 3/4

Integrity
ความสมบูรณ์

- การมั่นใจว่าข้อมูลยังคงมีความถูกต้องและไม่ได้ถูกแก้ไขเว้นแต่จะได้รับอนุญาต
- การปกป้องข้อมูลจากการเปลี่ยนแปลง การเสียหาย หรือการทำลาย

เช่น การใช้แฮช (hashing), การตรวจสอบข้อมูล (checksums) และลายเซ็นดิจิทัลช่วยตรวจสอบความสมบูรณ์ของข้อมูล

ตัวอย่าง: บันทึกธุรกรรมทางการเงิน ข้อมูลจะไม่สามารถถูกเปลี่ยนแปลงโดยผู้ที่ไม่ได้รับอนุญาต

Overview Cyber Security (CIA) 4/4

Availability
ความพร้อมใช้งาน

- การมั่นใจว่าข้อมูลและระบบสามารถเข้าถึงและใช้งานได้เมื่อมีความจำเป็น
- การปกป้องจากการหยุดชะงักของการเข้าถึงข้อมูลหรือการหยุดทำงานของระบบ ซึ่งอาจเกิดจาก การโจมตีไซเบอร์ หรือภัยธรรมชาติ

เช่น การสำรองข้อมูล (backup), ระบบสำรอง (redundancy) และแผนการกู้คืนจากภัยพิบัติ (disaster recovery)

ตัวอย่าง: การมั่นใจว่าระบบอีเมลทำงานอย่างต่อเนื่องเพื่อให้ผู้ใช้สามารถเข้าถึงกล่องจดหมายได้ตลอดเวลา

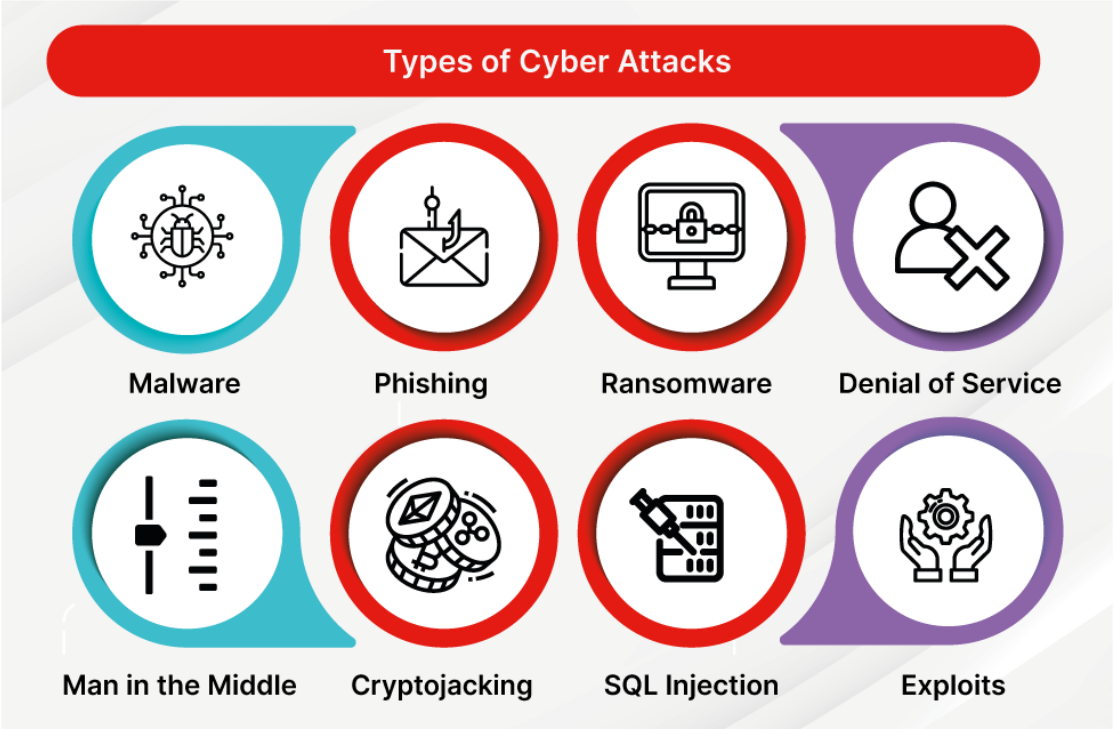
Overview Cyber Security (AAA Model)

AAA Model

คือ กรอบการทำงานด้านความปลอดภัย (Security Framework) ที่ใช้ควบคุมการเข้าถึงระบบหรือเครือข่าย ประกอบด้วย 3 ส่วนหลัก คือ การยืนยันตัวตน(Authentication) การมอบสิทธิ์(Authorization) และการบันทึกข้อมูล (Accounting) เพื่อตรวจสอบว่าใครเข้าถึงระบบได้ สิทธิ์ที่ผู้ใช้มีคืออะไร และมีการใช้งานอย่างไรบ้าง เพื่อให้มั่นใจว่าการเข้าถึงเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

1. **Authentication**
   การยืนยันตัวตน
2. **Authorization**
   การมอบสิทธิ์
3. **Accounting**
   การบันทึกข้อมูล

Overview Cyber Security การโจมตีไซเบอร์ที่พบโดยทั่วไป



รูปภาพจาก : https://www.fortinet.com/resources/cyberglossary/what-is-cyber-attack

Overview Cyber Security (Security Awareness)

- การเรียนรู้ถึงความเสียหายที่เกิดขึ้นจากภัยคุกคามไซเบอร์

เช่น พาสเวิร์ดหายจะเข้าระบบไม่ได้ รหัสATMหลุดเงินในบัญชีอาจโดนขโมย ข้อมูลลูกค้าหลุดทำให้บริษัทเสียชื่อเสียงลูกค้าหาย ข้อมูลอ่อนไหวหลุดจะโดนดำเนินคดี

Overview Cyber Security (Security Awareness)

- การรู้เท่าทันการโจมตีและความมั่นคงปลอดภัยทางไซเบอร์

เช่น ล็อคหน้าจอ ใช้โปรแกรม Anti-Malware ไม่ติดตั้งโปรแกรมที่ไม่มีความน่าเชื่อถือ สำรองข้อมูล ตั้งรหัสผ่านที่ซับซ้อน ไม่บันทึก Password ไว้กับเครื่องสาธารณะ ระวังในการใช้งาน Public Wi-Fi

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

วัตถุประสงค์

- เพื่อปกป้องระบบคอมพิวเตอร์และโครงข่าย IT ของโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ
- เพื่อให้บริการที่สำคัญของประเทศมีความมั่นคงปลอดภัยสามารถให้บริการได้เป็นปกติ
- เพื่อให้หน่วยงานสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที

หน่วยงานหลักที่เกี่ยวข้อง

- หน่วยงานควบคุมหรือกำกับดูแล
- สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

Overview Cyber Security กฎหมาย

ภาพรวม

หมวด 1

- ม.5-11 : คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ (กมช.)
- ม.12-19 : คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.)

หมวด 2

- ม.20-40 : สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

ภาพรวม

หมวด 3 การรักษาความมั่นคงปลอดภัยไซเบอร์

- ม.41-44 : นโยบายและแผน
- ม.45-47 : การบริหารจัดการ
- ม.48-57 : โครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- ม.58-69 : การรับมือกับภัยคุกคามไซเบอร์

โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (ม.48)

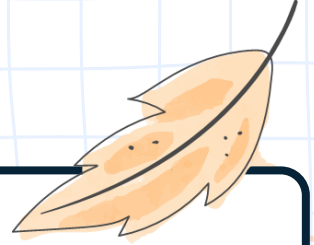
- ความมั่นคงของรัฐ
- ความมั่นคงทางทหาร
- ความมั่นคงทางเศรษฐกิจ
- ความสงบเรียบร้อยภายในประเทศ

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)

- ด้านความมั่นคงของรัฐ
- ด้านบริการภาครัฐที่สำคัญ
- ด้านการเงินการธนาคาร
- ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม
- ด้านการขนส่งและโลจิสติกส์
- ด้านพลังงานและสาธารณูปโภค
- ด้านสาธารณสุข
- ด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม

สิ่งที่หน่วยงานต้องปฏิบัติตาม

- แจ้งรายชื่อและข้อมูลการติดต่อ
- ดำเนินการตามมาตรฐาน
- ประเมินความเสี่ยงและส่งผลให้สำนักงาน
- ต้องมีกลไกหรือขั้นตอนเฝ้าระวังภัยคุกคามไซเบอร์
- เมื่อมีเหตุภัยคุกคาม ต้องรายงานต่อสำนักงานและหน่วยงานควบคุมหรือกำกับ



การรับมือภัยคุกคามทางไซเบอร์

- กรณีคาดว่าจะเกิดภัยคุกคาม ให้ตรวจสอบเพื่อประเมินว่ามีภัยคุกคามเกิดขึ้นจริงหรือไม่ หากพบว่าเกิดให้ดำเนินการป้องกัน รับมือ ลดความเสี่ยง และแจ้งไปยังสำนักงาน

- เมื่อได้รับแจ้ง ให้หน่วยงานควบคุมหรือกำกับดูแล ดำเนินการรวบรวมข้อมูลตรวจสอบวิเคราะห์สถานการณ์ ประเมินผลกระทบ และต้องสนับสนุนให้ความช่วยเหลือ ต้องแจ้งเตือนหน่วยงานภายใต้การดูแลของตน

ระดับภัยคุกคามไซเบอร์

ระดับไม่ร้ายแรง - ทำให้ระบบคอมพิวเตอร์หน่วยงานพื้นฐานของประเทศหรือการให้บริการของรัฐด้อยประสิทธิภาพลง

ระดับร้ายแรง - ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์

ระดับวิกฤต - ผลกระทบรุนแรงจนไม่สามารถควบคุมหรือแก้ไขได้ อาจกระทบต่อความสงบเรียบร้อยของประชาชนหรือเป็นภัยความมั่นคง

บทกำหนดโทษ (1/2)

- ห้ามพนักงานเปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ที่ได้มาตาม พ.ร.บ. นี้ แก่ผู้อื่นระวางโทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 6 หมื่นบาท
- ผู้ใดกระทำโดยประมาทเป็นเหตุให้มีผู้ล่วงรู้ข้อมูลคอมพิวเตอร์ ต้องระวางโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 2 หมื่นบาท
- ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาและนำไปเปิดเผยต่อ ระวางโทษจำคุกไม่เกิน 2 ปี หรือปรับไม่เกิน 4 หมื่นบาท หรือทั้งจำทั้งปรับ
- หน่วยงานโครงสร้างพื้นฐานฯ ใดไม่รายงานเหตุภัยคุกคาม ต้องระวางโทษปรับไม่เกิน 2 แสนบาท
- ผู้ใดไม่ปฏิบัติตามหนังสือเรียกหรือไม่ส่งข้อมูลให้พนักงานเจ้าหน้าที่ ต้องระวางโทษปรับไม่เกิน 1 แสนบาท

บทกำหนดโทษ (2/2)

ผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามคำสั่งของ กกม.

- ไม่เฝ้าระวังหรือตรวจสอบ ต้องระวางโทษปรับไม่เกิน 3 แสนบาท + ปรับอีกไม่เกินวันละ 1 หมื่นบาทนับตั้งแต่วันออกคำสั่งจนกว่าจะปฏิบัติให้ถูกต้อง
- ไม่ดำเนินมาตรการแก้ไขเพื่อจัดการข้อบกพร่อง รักษาสถานะของข้อมูลหรือเข้าถึงข้อมูลเฉพาะเท่าที่จำเป็น ต้องระวางโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 2 หมื่นบาท
- ผู้ใดขัดขวางหรือไม่ปฏิบัติตามคำสั่งของ กกม. ในการรับมือและบรรเทาความเสียหายของภัยระดับร้ายแรง ต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 6 หมื่นบาท
- กรณีที่ผู้กระทำผิดเป็นนิติบุคคล ซึ่งเกิดจากการสั่งการหรือการกระทำของ กมช. ผู้จัดการหรือบุคคลที่รับผิดชอบในการดำเนินงานของนิติบุคคลคนนั้น ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย

Overview Cyber Security (CSF)

NIST Cybersecurity Framework 2.0

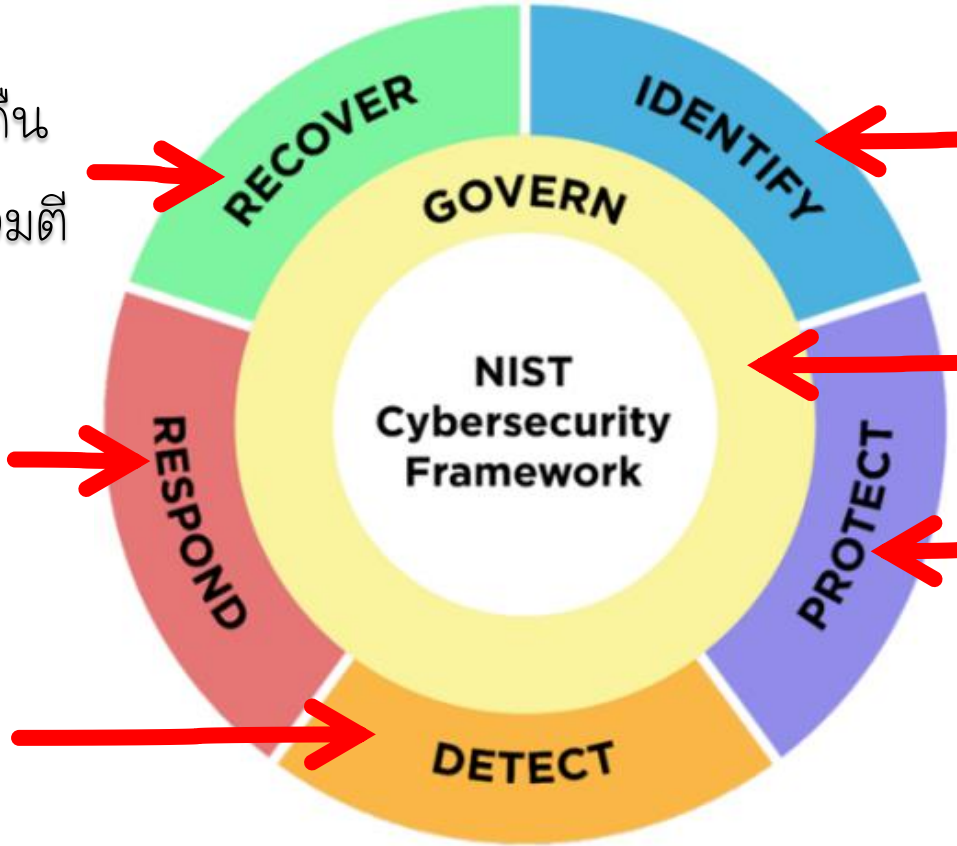
เป็นกรอบการทำงานด้านการบริหารจัดการความเสี่ยงทางไซเบอร์ที่กำหนดโดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (NIST) ที่บังคับใช้สำหรับหน่วยงานรัฐบาลกลางของสหรัฐอเมริกา เพื่อเป็นแนวทางการสร้างความปลอดภัยในการดำเนินงานสำหรับองค์กรต่างๆ รวมถึงหน่วยงานด้านสาธารณสุข การเงิน พลังงาน และโทรคมนาคม ซึ่งเป็นหน่วยงานที่มีการบริหารจัดการข้อมูลที่มีความละเอียดอ่อน และต้องปฏิบัติตามข้อกำหนดที่เข้มงวด

Overview Cyber Security (CFS)

กระบวนการกู้คืน
ระบบหากถูกโจมตี

การรับมือ
กับภัยคุกคาม

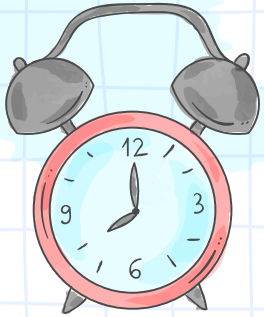
การตรวจจับ



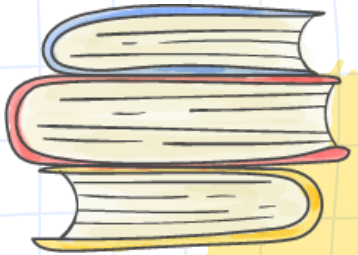
การระบุ
ความเสี่ยง

การกำกับดูแล

การป้องกัน



Identify



Identify

Identify 1/3

คือ การทำความเข้าใจสภาพแวดล้อมทางไซเบอร์ขององค์กร เพื่อระบุความเสี่ยงและความจำเป็นในการปรับปรุง การดำเนินการนี้ครอบคลุมการจัดการสินทรัพย์ การประเมินความเสี่ยง และการปรับปรุง โดยเน้นที่การระบุสินทรัพย์สำคัญ จุดอ่อน และบริบททางธุรกิจ เพื่อจัดลำดับความสำคัญของการรักษาความปลอดภัยทางไซเบอร์อย่างมีประสิทธิภาพ

Identify 2/3

วัตถุประสงค์

- เข้าใจสภาพแวดล้อม : องค์กรจำเป็นต้องรู้ว่ามีอะไรบ้าง มีการทำงานอย่างไร และมีความเสี่ยงอะไรบ้างในสภาพแวดล้อมทางไซเบอร์

- ระบุสินทรัพย์สำคัญ : ค้นหาและจัดลำดับความสำคัญของฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล และบริการที่สำคัญต่อการดำเนินงานขององค์กร

Identify 3/3

- ประเมินความเสี่ยง : วิเคราะห์ความเสี่ยงที่เกี่ยวข้องกับสินทรัพย์และระบบต่างๆ เพื่อทำความเข้าใจช่องโหว่และภัยคุกคามที่อาจเกิดขึ้น

- จัดลำดับความสำคัญ : กำหนดเป้าหมายและลำดับความสำคัญของการรักษาความปลอดภัยทางไซเบอร์ตามระดับความเสี่ยงและผลกระทบทางธุรกิจ

Identify ตัวอย่าง บัญชีทรัพย์สิน

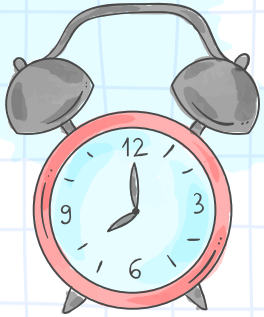
Host	Product	Function	Internet Protocol Address	Operating System
Demilitazied Zone				
Oreo1	Oreo1	Network Monitor	10.10.1.253	Ubuntu 22.04
IT Systems				
AD-STD1	Active Directory	Directory, DNS	10.10.1.1	Windows Server 2022

เลขทะเบียนทรัพย์สินสารสนเทศ	ประเภทฮาร์ดแวร์	ลักษณะการใช้งาน	ระดับความมั่นคงปลอดภัย (สูง/ปานกลาง/ต่ำ)	ผู้เป็นเจ้าของฮาร์ดแวร์	ผู้ใช้งาน	ที่ตั้ง	วันที่เริ่มสัญญาบำรุงรักษา
IT-618291928484	Nas Storage	Backup Data	สูง	นายณรงค์ ศักดิ์ศรี	นายณรงค์ ศักดิ์ศรี	DC Rack A2 - U20	1 Jan 2561

เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อซอฟต์แวร์	ชื่อบริษัทผู้พัฒนา	จำนวนลิขสิทธิ์	ประเภทซอฟต์แวร์	ระดับความมั่นคงปลอดภัย (สูง/ปานกลาง/ต่ำ)	ผู้เป็นเจ้าของซอฟต์แวร์	สถานที่จัดเก็บซอฟต์แวร์	วันที่ลงทะเบียนซอฟต์แวร์
IT-649912231234	Veeam Backup	Veeam	1	Backup Software	ปานกลาง	นายณรงค์ ศักดิ์ศรี	IT Dept	1 Jan 2564

เลขทะเบียนทรัพย์สินสารสนเทศ	ประเภทข้อมูล	รายละเอียดของสารสนเทศ	ระดับความลับ	ระดับความมั่นคงปลอดภัย (สูง/ปานกลาง/ต่ำ)	ผู้เป็นเจ้าของสารสนเทศ	ที่จัดเก็บ (ชื่อสถานที่)	เลขทะเบียน ทรัพย์สินซอฟต์แวร์ (เพื่อใช้อ้างอิง)
IT-64192981746756	Information	ข้อมูล Backup VM	Confidential	สูง	นายณรงค์ ศักดิ์ศรี	DC Rack A2 - U20	IT-649912231234

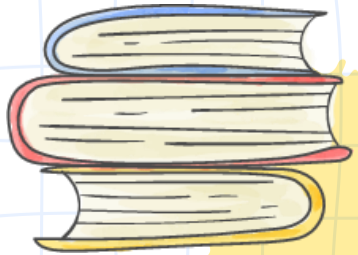
รูปภาพจาก : เอกสารการอบรม หลักสูตรการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับผู้ปฏิบัติงานด้านเทคโนโลยี 3 มี.ค. 2025 โดย Ittipon (Art) Rassameeroj, Ph.D.



Protection

NO GLYPH

Detection



Protection & Detection

Protection 1/3

กิจกรรมและการจัดการเพื่อป้องกันระบบ ข้อมูล และการดำเนินงาน จากการถูกคุกคามทางไซเบอร์โดยมุ่งเน้นการดำเนินการตามมาตรการที่ช่วยจำกัดผลกระทบของการโจมตีให้เหลือน้อยที่สุด

เป้าหมาย เพื่อให้แน่ใจว่าองค์กรสามารถดำเนินการตามขั้นตอนที่จำเป็นเพื่อเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์และจำกัดความเสี่ยงจากการถูกโจมตี

Protection & Detection

Protection 2/3

- การบริหารจัดการช่องโหว่ : ระบุและแก้ไขช่องโหว่ที่อาจเป็นอันตรายต่อระบบ

- การรักษาความปลอดภัยของข้อมูล : การจัดการและปกป้องข้อมูลสำคัญ

- การป้องกันเครือข่ายและระบบ : การติดตั้งและบำรุงรักษาเครื่องมือและมาตรการป้องกัน เช่น ไฟร์วอลล์ และระบบตรวจจับการบุกรุก

Protection & Detection

Protection 3/3

- การรักษาความปลอดภัยของบุคลากร : การให้ความรู้และความตระหนักแก่พนักงานเกี่ยวกับภัยคุกคามทางไซเบอร์และการปฏิบัติตามนโยบายความปลอดภัย

- การจัดการการเข้าถึง : การควบคุมการเข้าถึงระบบและข้อมูล เพื่อให้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงได้

- การป้องกันการสูญเสียข้อมูล : การสำรองข้อมูลและการรักษาความสมบูรณ์ของข้อมูลเพื่อป้องกันการสูญหายจากการโจมตี

Protection & Detection

Detection 1/2

กระบวนการในการติดตามสินทรัพย์ต่างๆ อย่างต่อเนื่อง เพื่อตรวจจับสิ่งผิดปกติ และสัญญาณที่บ่งชี้ถึงภัยคุกคาม รวมถึงความสามารถในการวิเคราะห์เหตุการณ์ที่น่าสงสัย หรืออาจก่อให้เกิดอันตรายอย่างรวดเร็ว เพื่อระบุลักษณะและตรวจพบพฤติกรรมหรือสถานการณ์ที่ผิดปกติของระบบ ซึ่งอาจเป็นสัญญาณบ่งชี้ถึงการถูกคุกคามทางด้านความมั่นคงปลอดภัยไซเบอร์

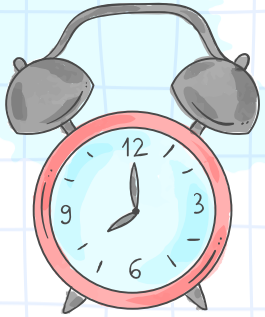
Protection & Detection

Detection 2/2

- การเฝ้าระวังอย่างต่อเนื่อง(Continuous Monitoring) : องค์กรจะดำเนินการตรวจสอบระบบและเครือข่ายอย่างสม่ำเสมอเพื่อหาภัยคุกคามหรือพฤติกรรมที่น่าสงสัย

- การระบุภัยคุกคาม (Threat Identification) : เมื่อตรวจพบกิจกรรมที่ผิดปกติ ฟังก์ชันนี้จะช่วยระบุชนิดของภัยคุกคามและแหล่งที่มาของภัย

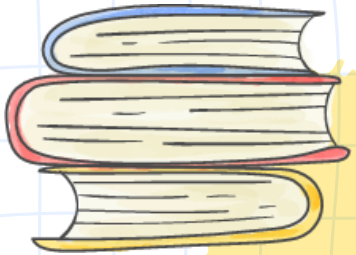
- การแจ้งเตือน (Alerting) : การแจ้งเตือนเมื่อตรวจพบเหตุการณ์ด้านความปลอดภัย เพื่อให้ทีมที่เกี่ยวข้องสามารถดำเนินการตอบสนองได้อย่างรวดเร็ว



Response

NO GLYPH

Govern



Response &Govern

Response 1/4

กระบวนการในการรับมือกับเหตุการณ์ที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์อย่างทันท่วงทีและมีประสิทธิภาพ เพื่อลดความเสียหายและผลกระทบให้น้อยที่สุด โดยต้องมีการวางแผนนโยบายและขั้นตอนที่ชัดเจน กำหนดผู้รับผิดชอบ และมีการฝึกซ้อมอย่างสม่ำเสมอเพื่อให้องค์กรสามารถดำเนินการได้ตามแผน

Response 2/4

องค์ประกอบ

- การจัดทำแผนรับมือเหตุการณ์ (Incident Response Plan) : องค์กรต้องมีแผนที่กำหนดขั้นตอนการรับมือเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ไว้อย่างเป็นระบบ

- การกำหนดนโยบายและขั้นตอน : แผนดังกล่าวควรกำหนดนโยบายและขั้นตอนการดำเนินการที่ชัดเจนสำหรับสถานการณ์ต่างๆ

Response &Govern

Response 3/4

- การกำหนดหน้าที่ความรับผิดชอบ : ต้องระบุหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในการตอบสนองต่อเหตุการณ์อย่างชัดเจน

- การสื่อสาร : การสื่อสารภายในและภายนอกองค์กรระหว่างการเกิดเหตุการณ์เป็นสิ่งสำคัญ เพื่อให้ทุกฝ่ายรับทราบข้อมูลและประสานงานกันได้อย่างมีประสิทธิภาพ

Response &Govern

Response 4/4

- การวิเคราะห์หลังเกิดเหตุ (Post-Incident Activity) : การวิเคราะห์สาเหตุและผลกระทบหลังเหตุการณ์ รวมถึงการทบทวนและปรับปรุงแผนรับมือ เพื่อป้องกันไม่ให้เกิดเหตุการณ์ซ้ำ

Response & Govern

Govern 1/3

เพิ่มเข้ามาในกรอบงานความปลอดภัยทางไซเบอร์ (Cyber Security Framework) เวอร์ชัน 2.0 โดยเน้นความสำคัญของการสร้างโครงสร้างการกำกับดูแลที่มีประสิทธิภาพ เพื่อให้องค์กรสามารถบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างสอดคล้องกับวัตถุประสงค์ทางธุรกิจและข้อกำหนดทางกฎหมาย

Govern 2/3

รายละเอียด

- การวางนโยบายควบคุม : การกำหนดนโยบายและแนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
- การบริหารความเสี่ยง : การกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้, การจัดลำดับความสำคัญ, และการกำหนดสมมติฐานเพื่อใช้ในการตัดสินใจเกี่ยวกับความเสี่ยง

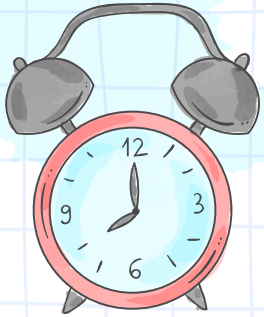
Response & Govern

Govern 3/3

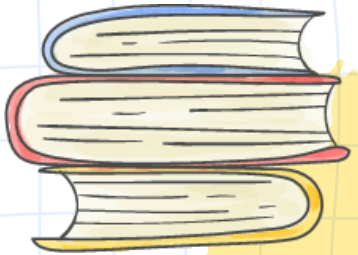
- การกำหนดบทบาทและความรับผิดชอบ : การกำหนดผู้รับผิดชอบและอำนาจหน้าที่ที่ชัดเจนในด้านความมั่นคงปลอดภัยไซเบอร์

- การกำกับดูแลในห่วงโซ่อุปทาน : การจัดการความเสี่ยงในห่วงโซ่อุปทานความปลอดภัยทางไซเบอร์

- การเชื่อมโยงกับวัตถุประสงค์ทางธุรกิจ : การทำให้การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์สอดคล้องกับเป้าหมายทางธุรกิจขององค์กร



Recovery



Recovery

Recovery 1/3

การดำเนินกิจกรรมเพื่อฟื้นฟูความสามารถหรือบริการที่เสียหายจากเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยมีเป้าหมายเพื่อให้การดำเนินงานกลับสู่ภาวะปกติได้อย่างทันท่วงที และปรับปรุงความสามารถในการรับมือกับเหตุการณ์ในอนาคต

Recovery 2/3

กระบวนการ

- ปฏิบัติตามแผน : ดำเนินการตามแผนการกู้คืนระบบที่เตรียมไว้

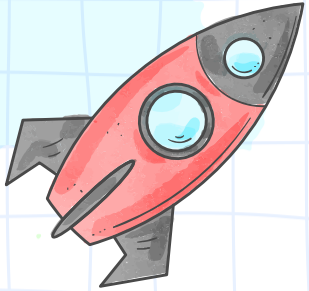
- ตรวจสอบข้อมูลสำรอง: ตรวจสอบความครบถ้วนสมบูรณ์ของข้อมูลสำรองที่จะใช้ในการกู้คืน

Recovery

Recovery 3/3

- การสื่อสาร : จัดทำแผนการสื่อสารเพื่อแจ้งความคืบหน้าให้ผู้เกี่ยวข้องทราบ เพื่อให้การดำเนินงานต่อเนื่อง

- จัดทำเอกสาร : บันทึกรายละเอียดเหตุการณ์ ปัญหาและขั้นตอนการแก้ไข เพื่อนำมาวิเคราะห์



THE END