CYFENCE
Securing your Business

การสร้างความตระหนักรู้
ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์

วิทยากร
คุณ ศิรินาฏ จินดาวุฒิพันธ์

วิทยากร
คุณ จันทกานต์ ผลพล

AGENDA

1. ทิศทางแนวโน้มด้านความมั่นคงปลอดภัยทางไซเบอร์

- แนวโน้มภัยคุกคามทางไซเบอร์และสถิติอาชญากรรมทางไซเบอร์
- รูปแบบภัยคุกคามทางไซเบอร์

2. แนวทางป้องกันภัยคุกคามทางไซเบอร์

- การป้องกันภัยคุกคามทางไซเบอร์ในรูปแบบต่างๆ
- บทบาทและหน้าที่ความรับผิดชอบของบุคลากรที่เกี่ยวข้อง

3. กฎหมายและมาตรฐานสากลด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง

- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ 2562

4.กิจกรรมตอบคำถาม ถาม-ตอบ

nt CYFENCE
Securing your Business

โลกดิจิทัลที่เชื่อมโยงกันอย่างไร้รอยต่อ

ในปี 2026 เทคโนโลยีไม่ได้ได้แยกส่วนกันอีกต่อไป ทุกระบบตั้งแต่สมาร์ทโฟนในมือคุณ ไปจนถึงเครื่องจักรในโรงงาน ต่างเชื่อมโยงกันบนเครือข่ายเดียว

“เหตุการณ์โจมตีเพียงจุดเดียว สามารถส่งผลกระทบเป็นลูกโซ่ ลุกลามไปทั่วโลกได้อย่างรวดเร็ว”

(WEF Global Cybersecurity Outlook 2026)

GLOBAL CYBERSECURITY OUTLOOK 2026

ทิศทางแนวโน้มความมั่นคงปลอดภัยทางไซเบอร์ระดับโลก 2026

ข้อมูล อ้างอิง: World Economic Forum

5 ทิศทางและแนวโน้มความมั่นคงปลอดภัยทางไซเบอร์ระดับโลก

CYFENCE

1

1	2	3	4	5
				
AI เป็นตัวขับเคลื่อน (The AI Catalyst)	ความร้าวฉานทางภูมิรัฐศาสตร์ (Geopolitical Fractures)	ยุคแห่งการฉ้อโกงทางไซเบอร์ (Cyber-Enabled Fraud)	ความท้าทายด้านความยืดหยุ่น (Cyber Resilience)	ภัยคุกคามรูปแบบใหม่ (Emerging Threats 2030)

1. AI คือ ตัวขับเคลื่อนการเปลี่ยนแปลงที่ยิ่งใหญ่ที่สุด

ปัญญาประดิษฐ์: ดาบสองคมแห่งโลกไซเบอร์

94%
ของผู้บริหารระดับสูงมองว่า AI คือปัจจัยหลักที่จะเปลี่ยนโฉมความมั่นคงปลอดภัย

ดาบเชิงรุก (Offensive)
สร้างการโจมตีที่ซับซ้อน มีขนาดใหญ่ และแม่นยำขึ้นอย่างที่ไม่เคยมีมาก่อน

โล่เชิงรับ (Defensive)
เพิ่มขีดความสามารถในการตรวจจับภัยคุกคามล่วงหน้า และตอบสนองต่อเหตุการณ์ฉุกเฉินได้โดยอัตโนมัติ

จุดเปลี่ยนสำคัญ: ความกังวลหลักเกี่ยวกับ Generative AI ได้เปลี่ยนจากการสร้างเนื้อหาปลอม มาเป็นวิกฤต การรั่วไหลของข้อมูล (Data Leakage)

2. ภูมิรัฐศาสตร์: ปัจจัยอันดับหนึ่งที่กำหนดความเสี่ยง

การโจมตีที่มีแรงจูงใจทางการเมือง
เป้าหมายไม่ได้หยุดแค่การรบกวนระบบ แต่ยกระดับสู่การทำลายโครงสร้างพื้นฐานระดับชาติ และการจารกรรมข้อมูลขั้นสูง

วิกฤตความเชื่อมั่น
ความแตกแยกส่งผลให้ความเชื่อมั่นในความพร้อมระดับชาติต่อการรับมือเหตุการณ์ไซเบอร์ลดลงอย่างมีนัยสำคัญ

ผลกระทบเชิงยุทธศาสตร์
ภูมิรัฐศาสตร์ยังคงเป็นปัจจัยอันดับหนึ่งที่ส่งผลต่อการวางกลยุทธ์ลดความเสี่ยงขององค์กรในระดับบอร์ดบริหาร

เมื่อความขัดแย้งระดับชาติ ขยายผลสู่โลกไซเบอร์

การโจมตีทางไซเบอร์กลายเป็นอาวุธยุคใหม่ที่ใช้ทำลายเศรษฐกิจและโครงสร้างพื้นฐานของประเทศคู่แข่ง

64%

ขององค์กรทั่วโลก ต้องปรับกลยุทธ์เพื่อรับมือกับการโจมตีที่มีแรงจูงใจทางภูมิรัฐศาสตร์

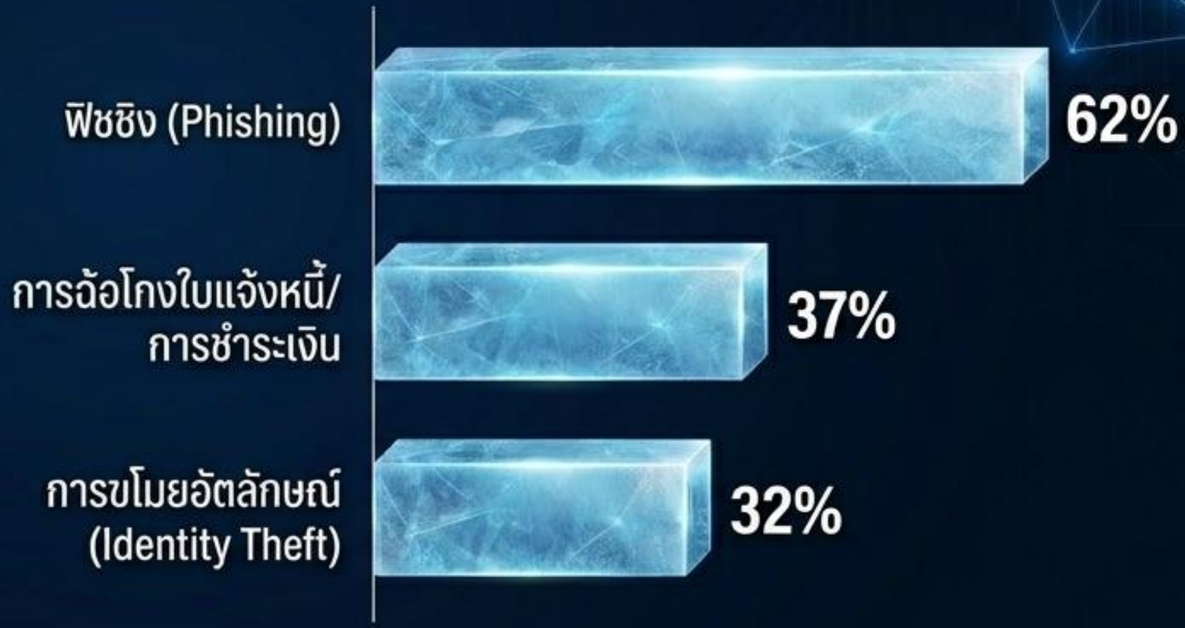
Takeaway

เป้าหมายอาจไม่ใช่รัฐบาลเสมอไป แต่รวมถึงธุรกิจและพนักงานที่เป็นกลไกสำคัญของเศรษฐกิจ

3. ฝันร้ายบทใหม่ของผู้บริหาร: การฉ้อโกงทางไซเบอร์

CEO เปลี่ยนความกังวลสูงสุดจากแรนซัมแวร์มาเป็นการฉ้อโกงทางไซเบอร์และฟิชชิง
เนื่องจากสร้างผลกระทบทางการเงินโดยตรงและรวดเร็ว

สัดส่วนรูปแบบการฉ้อโกงที่พบบ่อยที่สุด (ปี 2025)



ภาพลวงตาแห่งความน่าเชื่อถือ: การติดอาวุธให้ Social Engineering

ความสมจริงขั้นสุด
เทคโนโลยี Deepfake และ AI ขั้นสูง ทำให้การโจมตีแบบ Social Engineering มีความน่าเชื่อถือในระดับที่ตาเปล่าแยกไม่ออก

การโจมตีระดับแมส (Mass-Scale)
ไม่ใช่การหลอกลวงแบบเจาะจงบุคคลอีกต่อไป แต่สามารถทำสำเนาและแพร่กระจายการโจมตีได้ในวงกว้างด้วยต้นทุนที่ต่ำมาก

ผลกระทบเชิงระบบ
บั่นทอนความเชื่อมั่นโดยรวมของสถาบัน และทำลายความรู้สึกปลอดภัยในการทำธุรกรรมของสังคม

มุมมองที่แตกต่าง: เมื่อคณะกรรมการบริหารและผู้ปฏิบัติงานมองมองเห็นความเสี่ยงไม่เหมือนกัน

มุมมอง CEO
(เน้นที่ความสูญเสียทางการเงินและชื่อเสียง)

- อันดับ 1: การฉ้อโกงที่ใช้ไซเบอร์เป็นเครื่องมือ (Cyber-enabled fraud)
- อันดับ 2: ช่องโหว่จาก AI (AI vulnerabilities)

มุมมอง CISO
(เน้นที่ความต่อเนื่องในการดำเนินงาน)

- อันดับ 1: การโจมตีด้วย Ransomware
- อันดับ 2: การหยุดชะงักของห่วงโซ่อุปทาน (Supply chain disruption)

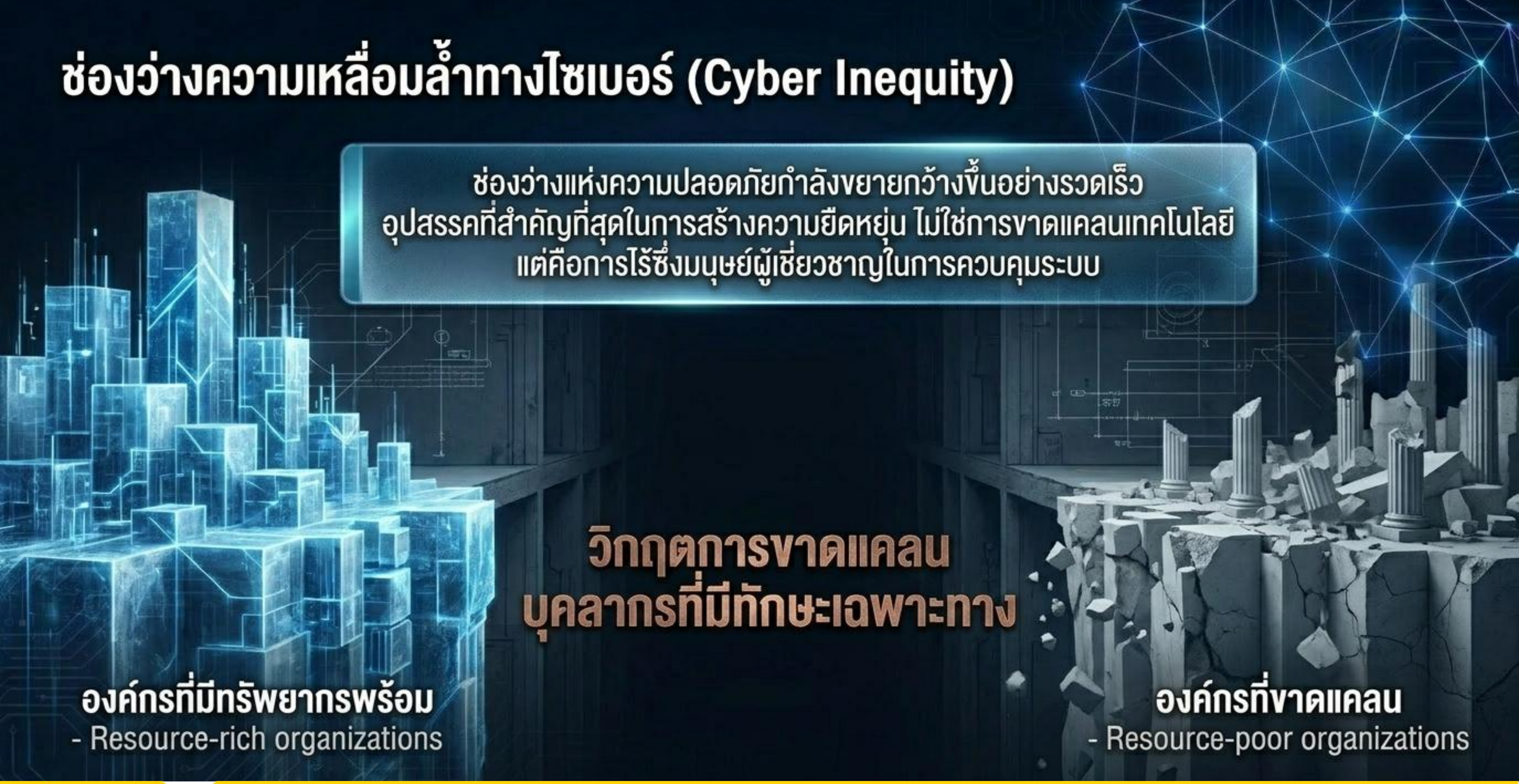
ความท้าท้ายสูงสุดในปี 2026 คือ การผสานมุมมองทั้งสองนี้ให้เป็นกลยุทธ์หนึ่งเดียว

4. ความยืดหยุ่นทางไซเบอร์ (Cyber Resilience): ไม่ใช่วาระของฝ่ายไอทีอีกต่อไป

กรอบความคิดเดิม (The Old Paradigm)		กรอบความคิดปี 2026 (The 2026 Paradigm)
สถานะ	เป็นเพียงปัญหาทางเทคนิค (Technical Issue)	วาระทางยุทธศาสตร์และเศรษฐกิจระดับชาติ (Strategic & Economic Agenda)
ผู้รับผิดชอบหลัก	แผนกไอที (IT Department)	ผู้บริหารระดับสูงและคณะกรรมการบริษัท (Boardroom Level)
กลยุทธ์หลัก	เน้นการป้องกันและตั้งรับ (Reactive / Defense-only)	การสร้างความยืดหยุ่นและการฟื้นฟู (Proactive Resilience & Rapid Recovery)

ช่องว่างความเหลื่อมล้ำทางไซเบอร์ (Cyber Inequity)

ช่องว่างแห่งความปลอดภัยกำลังขยายกว้างขึ้นอย่างรวดเร็ว
อุปสรรคที่สำคัญที่สุดในการสร้างความยืดหยุ่น ไม่ใช่การขาดแคลนเทคโนโลยี
แต่คือการไร้ซึ่งมนุษย์ผู้เชี่ยวชาญในการควบคุมระบบ



วิกฤตการขาดแคลน
บุคลากรที่มีทักษะเฉพาะทาง

องค์กรที่มีทรัพยากรพร้อม
- Resource-rich organizations

องค์กรที่ขาดแคลน
- Resource-poor organizations

ความเปราะบางของห่วงโซ่อุปทาน (Supply Chain Risk)

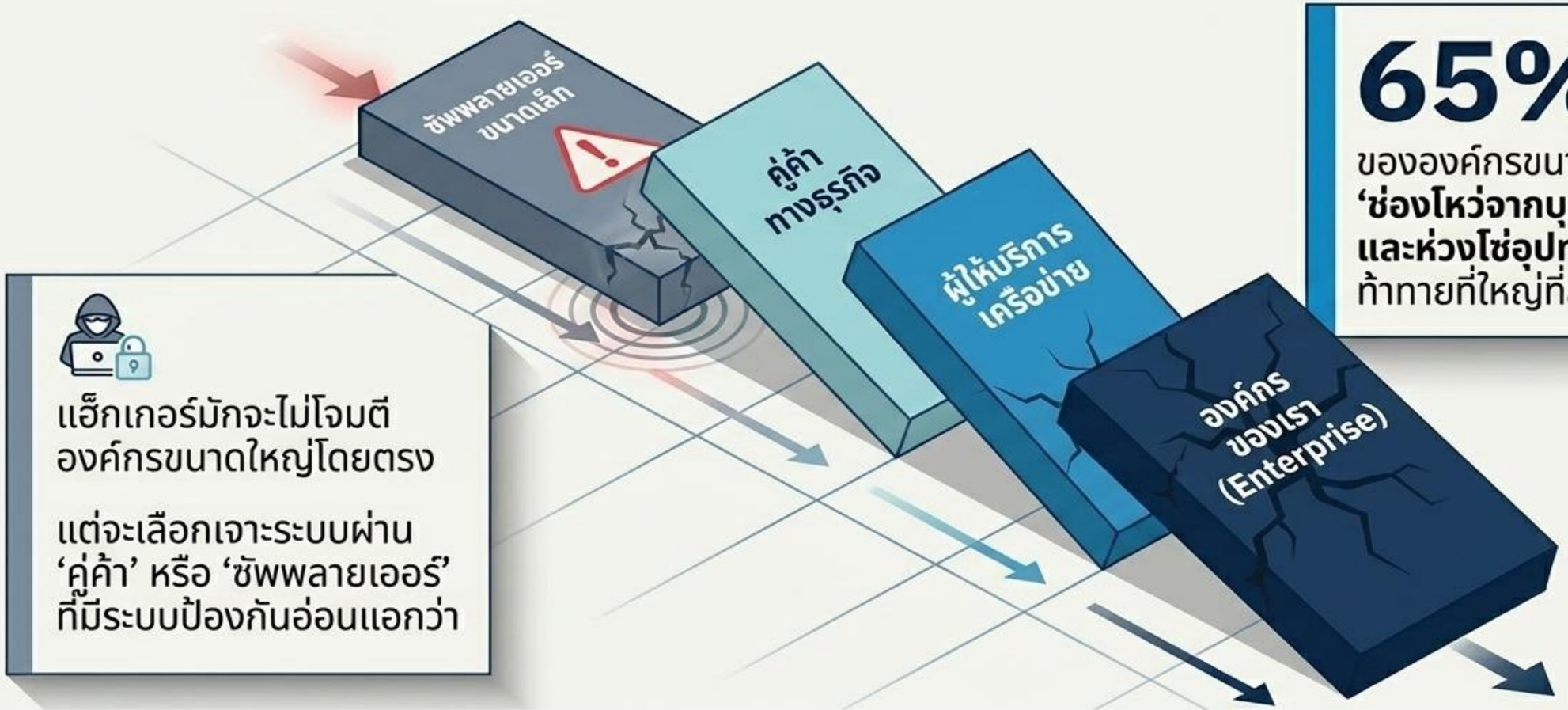
วิกฤตการกระจุกตัว (Concentration Risk)

ระบบเศรษฐกิจดิจิทัลพึ่งพาผู้ให้บริการรายใหญ่เพียงไม่กี่ราย
หากเกิดเหตุขัดข้องทับศูนย์กลาง
จะสร้างผลกระทบแบบโดมิโนต่อธุรกิจนับแสนแห่งทั่วโลก

กล่องดำแห่งความปลอดภัย

องค์กรประสบความยากลำบากอย่างยิ่งในการเข้าตรวจสอบซัพพลายายนอก
ทำให้ความเสี่ยงถูกซ่อนอยู่ในจุดที่มองไม่เห็น

ปรากฏการณ์โดมิโน ในห่วงโซ่อุปทานดิจิทัล



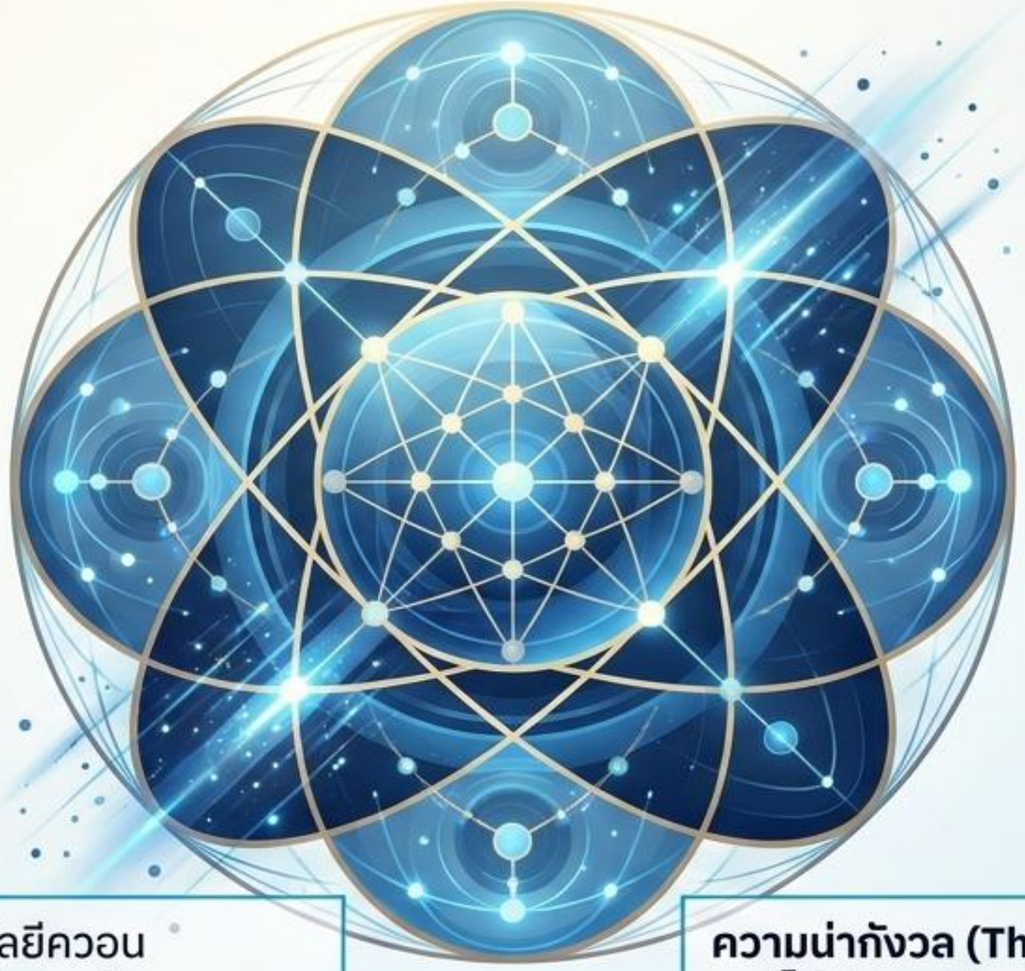
65%

ขององค์กรขนาดใหญ่ระบุว่า **‘ช่องโหว่จากบุคคลที่สามและห่วงโซ่อุปทาน’** คือความท้าทายที่ใหญ่ที่สุดในปี 2026

แฮ็กเกอร์มักจะไม่โจมตีองค์กรขนาดใหญ่โดยตรง

แต่จะเลือกเจาะระบบผ่าน ‘คู่ค้า’ หรือ ‘ซัพพลายเออร์’ ที่มีระบบป้องกันอ่อนแอกว่า

ภัยคุกคามแห่งอนาคตที่กำลังใกล้เข้ามา: เทคโนโลยีควอนตัม



คอมพิวเตอร์ควอนตัมมีพลังการประมวลผลมหาศาล ซึ่งในอนาคตอันใกล้จะสามารถถอดรหัสผ่านและระบบรักษาความปลอดภัยระดับสูงที่โลกใช้อยู่ในปัจจุบันได้ในพริบตา

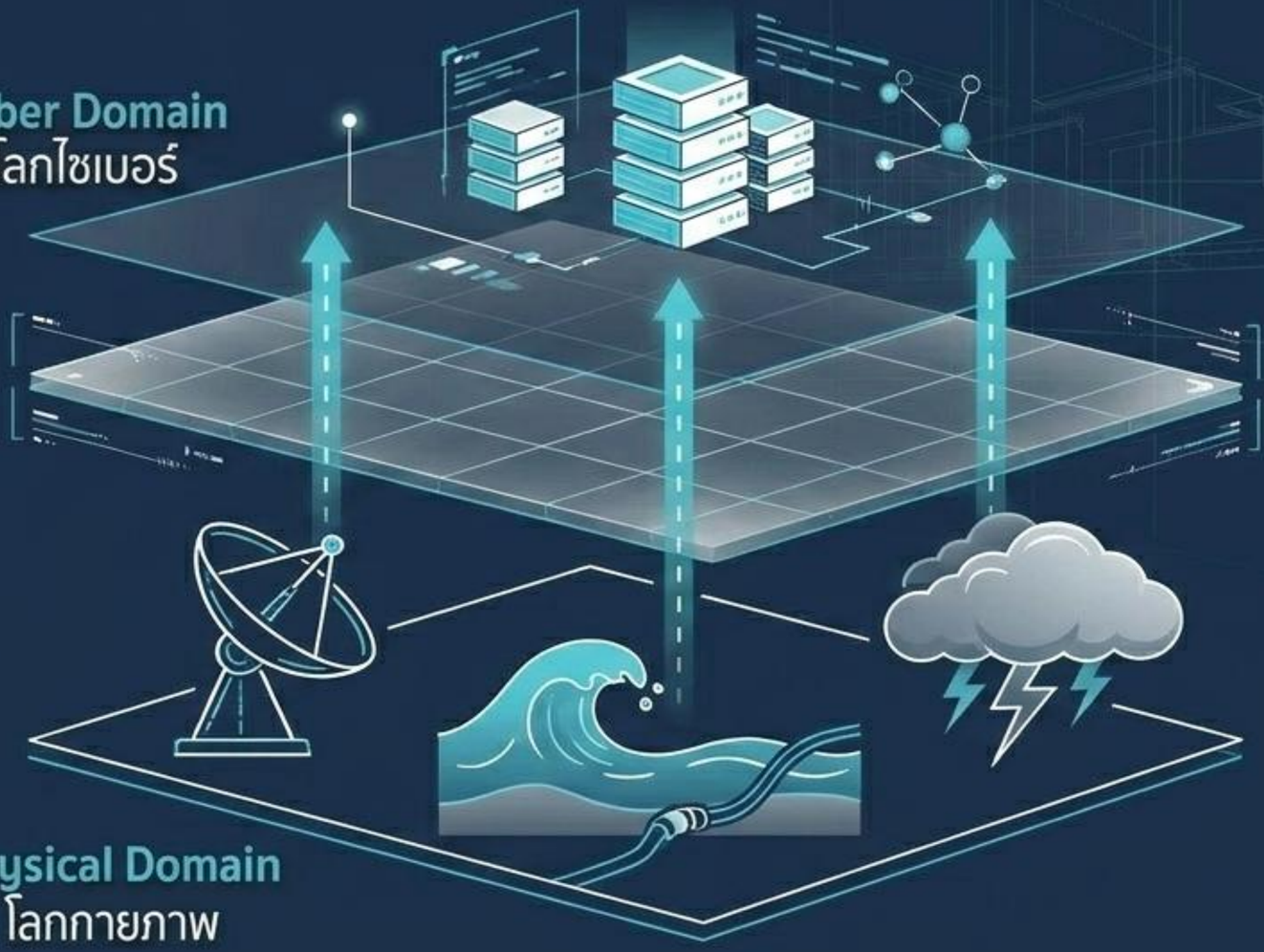
37% ของผู้นำระดับโลกมองว่าเทคโนโลยีควอนตัมจะส่งผลกระทบโดยตรงต่อความปลอดภัยไซเบอร์ภายใน 12 เดือนข้างหน้า

ความน่ากังวล (The Concern):
หากไม่มีการเตรียมพร้อม ข้อมูลที่ถูกเข้ารหัสไว้ในวันนี้อาจถูกถอดรหัสและขโมยไปใช้อย่างง่ายดายในวันพรุ่งนี้

จุดตัดวิกฤต: เมื่อโลกกายภาพหลอมรวมกับโลกไซเบอร์

Core Concept:
วิกฤตทางกายภาพสามารถลุกลามและ
กลายเป็นวิกฤตทางไซเบอร์ได้อย่างรวดเร็ว
ต้องเฝ้าระวังปัจจัยโครงสร้างพื้นฐาน ได้แก่:

- ✓ - เทคโนโลยีอวกาศ (Space Tech)
- ✓ - สายเคเบิลใต้ทะเล (Subsea Cables)
- ✓ - ผลกระทบจากภัยธรรมชาติ (Natural Disasters)



เรดาร์สแกนภัยคุกคามแห่งอนาคต (มุ่งสู่ปี 2030)

Agentic AI & หุ่นยนต์
ระบบ AI ที่ตัดสินใจและลงมือโจมตีด้วยตนเอง

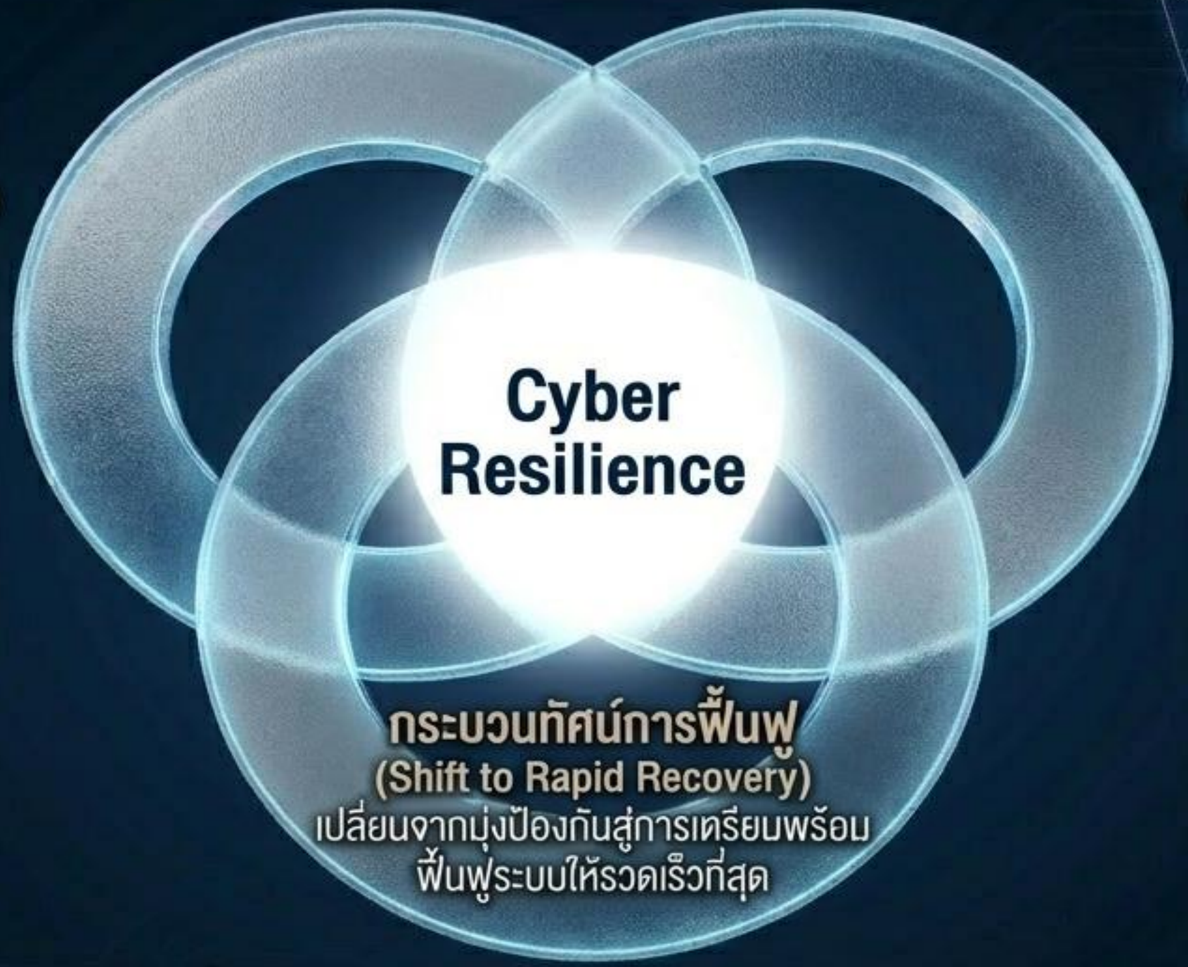
เทคโนโลยีอวกาศ (Space Tech)
ช่องโหว่ในโครงสร้างพื้นฐานดาวเทียม

สายเคเบิลใต้น้ำ (Undersea Cables)
เป้าหมายการทำลายล้างทางกายภาพ

เทคโนโลยีควอนตัม (Quantum Technologies)
ภัยคุกคามร้ายแรงที่จะทำลายระบบการถอดรหัสลับ (Encryption) ที่ใช้งานอยู่ในปัจจุบันทั้งหมด

ภัยธรรมชาติ
โดมิโนเอฟเฟกต์ที่เปลี่ยนวิกฤตสิ่งแวดล้อมสู่วิกฤตไซเบอร์

ยุทธศาสตร์เพื่อความอยู่รอด: สมการรับมือแห่งปี 2026



ความร่วมมือระดับมหภาค
(Public-Private Cooperation)
บูรณาการข้อมูลและทรัพยากร
จากบการระหว่าง
ภาครัฐและเอกชนอย่างไร้รอยต่อ

มนุษย์ + เครื่องจักร
(Human + Tech Investment)
ลงทุนในทักษะบุคลากรควบคู่กับ
การอัปเกรดเทคโนโลยี AI

กระบวนทัศน์การฟื้นฟู
(Shift to Rapid Recovery)
เปลี่ยนจากมุ่งป้องกันสู่การเตรียมพร้อม
ฟื้นฟูระบบให้รวดเร็วที่สุด

ผู้ชนะในปี 2026 คือองค์กรที่สามารถรับแรงกระแทก และกลับคืนสู่สภาพเดิมได้เร็วกว่าคู่แข่ง

แนวโน้มภัยคุกคามทางไซเบอร์และสถิติอาชญากรรมทางไซเบอร์

THREAT LANDSCAPE OVERVIEW

89% increase in attacks by AI-enabled adversaries

Average eCrime breakout time dropped to **29** minutes, a **65%** increase in speed from 2024, and the fastest breakout time was only **27** seconds

82% of detections in 2025 were malware-free, up from **51%** in 2020

24 new adversaries tracked by CrowdStrike, raising the total to **281**

China-nexus activity increased **38%** across all sectors, with an **86%** increase in logistics

42% increase in zero-day vulnerabilities exploited prior to public disclosure

Valid account abuse accounted for **35%** of cloud incidents

37% rise in cloud-conscious intrusions, with **266%** increase by state-nexus threat actors

EC-COUNCIL UNIVERSITY
ACCREDITED. FLEXIBLE. ONLINE.

Top 10 Cybersecurity Threats of 2026

AI-Assisted Autonomous Attacks

Identity Abuse & Credential Compromise

Supply Chain Attacks

Deepfake & Synthetic Identity Fraud

Adversarial AI & Data Poisoning

AI-Enhanced Phishing & Social Engineering

Ransomware 3.0 & Intelligent Extortion

DDoS Megascale Operations

IoT & Edge Vulnerabilities

Post-Quantum Cryptographic Pressure

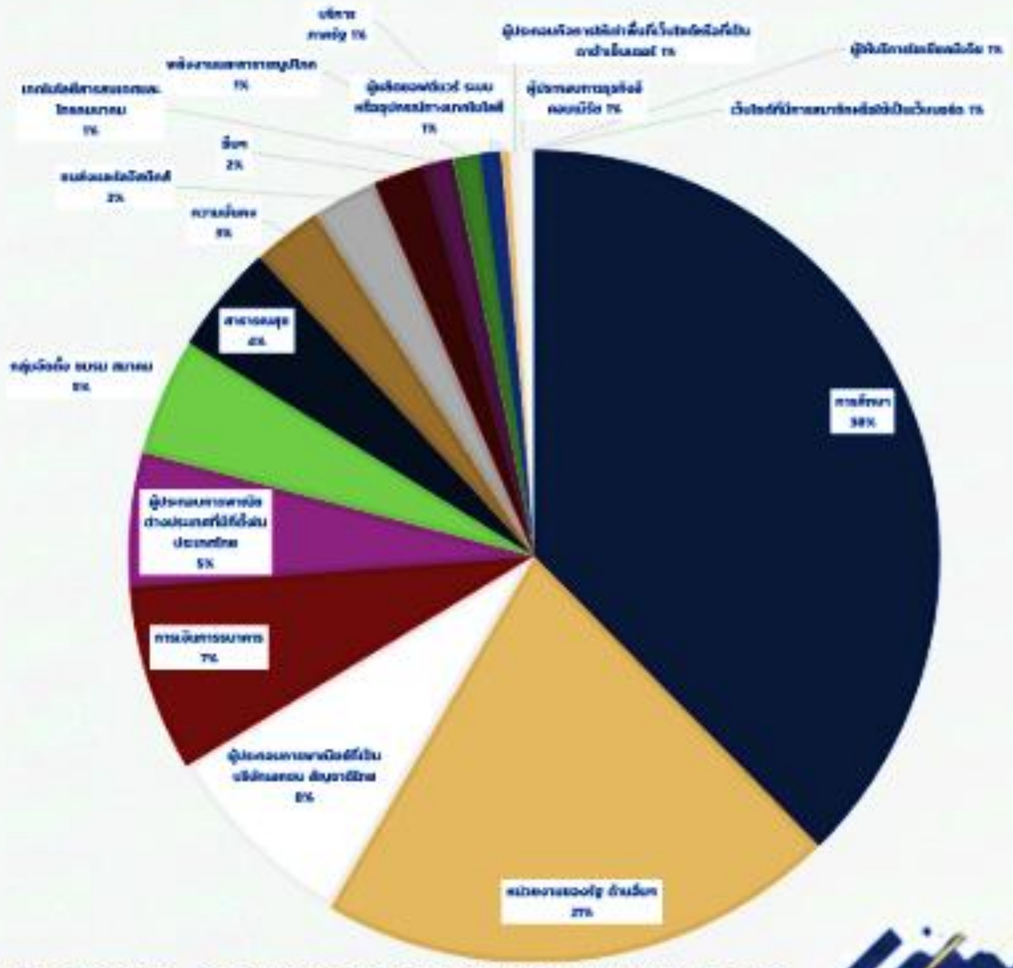
สถิติภัยคุกคามทางไซเบอร์ ประจำปี พ.ศ. 2569

มกราคม 2569 – มีนาคม 2569

NCSA สกมช

รวมทั้งสิ้น 1,149 เหตุการณ์

การศึกษา	432
หน่วยงานของรัฐ ด้านอื่นๆ	239
ผู้ประกอบการพาณิชย์ที่เป็นบริษัทเอกชน สัญชาติไทย	92
การเงินการธนาคาร	85
ผู้ประกอบการพาณิชต่างประเทศที่มีที่ตั้งในประเทศไทย	61
กลุ่มจัดตั้ง ขมรม สมาคม	54
สาธารณสุข	50
ความมั่นคง	32
ขนส่งและโลจิสติกส์	30
อื่นๆ	23
เทคโนโลยีสารสนเทศและโทรคมนาคม	14
พลังงานและสาธารณูปโภค	13
ผู้ผลิตซอฟต์แวร์ ระบบ หรืออุปกรณ์ทางเทคโนโลยี	9
บริการภาครัฐ	4
ผู้ประกอบกิจการให้เช่าพื้นที่เว็บไซต์หรือที่เป็นดาต้าเซ็นเตอร์	4
ผู้ประกอบการธุรกิจอีคอมเมิร์ซ	3
ผู้ให้บริการโซเชียลมีเดีย	3
เว็บไซต์ที่มีการสมาชิกหรือใช้เป็นเว็บบอร์ด	1



SAFE, SECURE, & TRUSTED CYBERSPACE FOR THAILAND

หมายเหตุ – หน่วยงานการเงินการธนาคารลักษณะภัยคุกคามถูกปลอมแปลงหน้าเว็บไซต์ เพื่อใช้หลอกลวงประชาชน

ภูมิทัศน์ภัยคุกคามไทย: ตรวจพบ 1,149 การโจมตีใน 3 เดือน

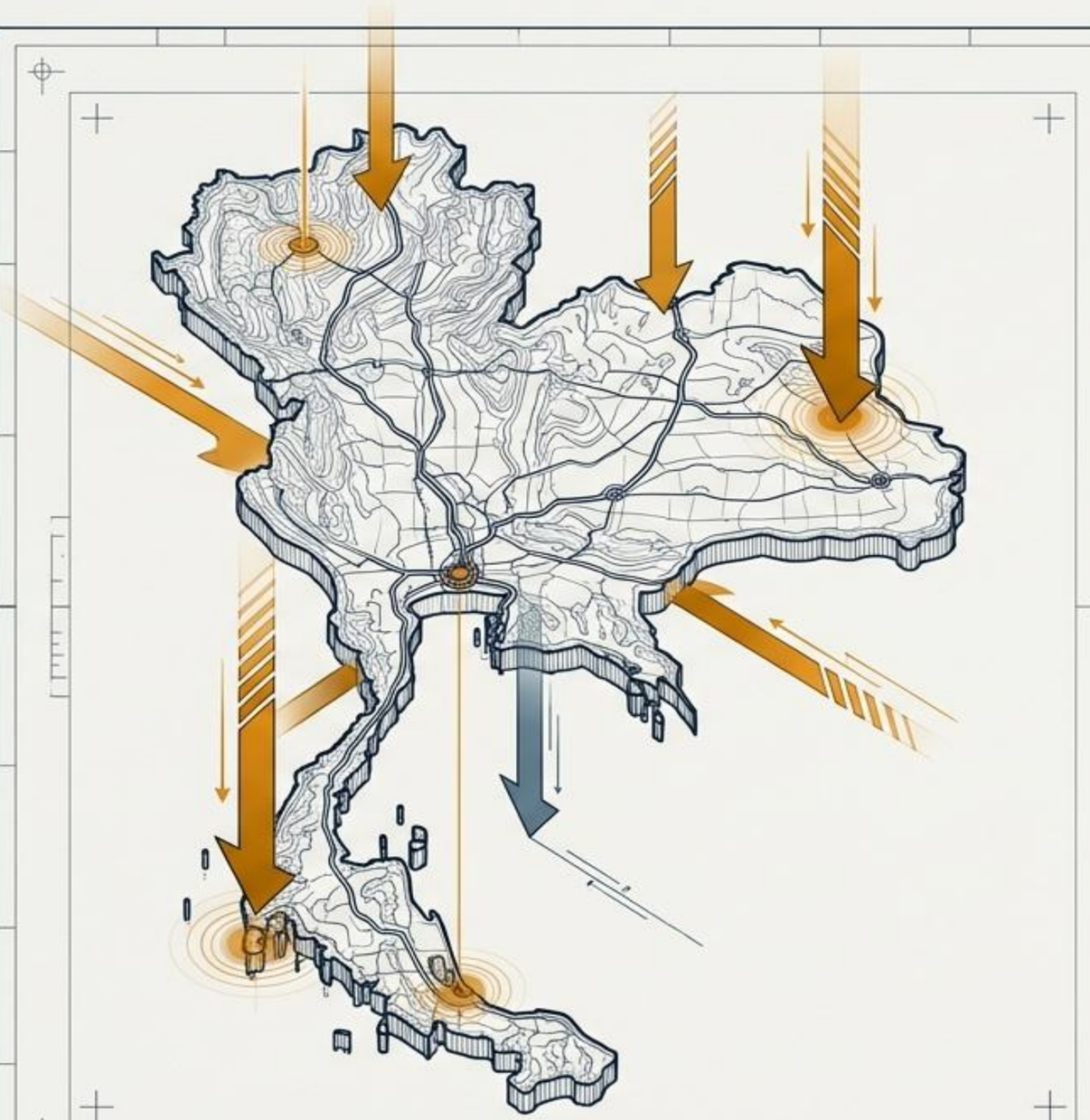
เป้าหมายระดับวิกฤต (Critical Targets)

- ภาคการศึกษา (Education) - **432** ครั้ง (เป้าหมายอันดับ 1)
- หน่วยงานรัฐ (Government) - **239** ครั้ง

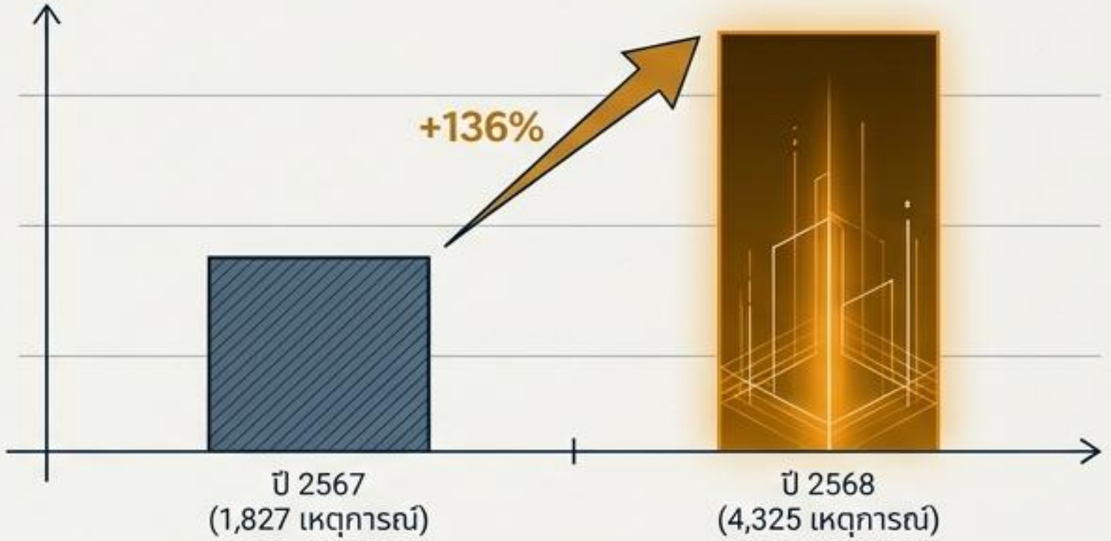
เป้าหมายความเสี่ยงสูง (High Risk Targets)

- พาณิชย์เอกชนไทย (Commerce) - **92** ครั้ง
- การเงินการธนาคาร (Finance) - **85** ครั้ง
- สาธารณสุข (Healthcare) - **50** ครั้ง

ข้อมูลเชิงลึก: ภัยคุกคามเติบโตอย่างก้าวกระโดดเมื่อเทียบกับสถิติปี 2567 ทั้งปีที่มีเพียง **1,827** รายการ



สงครามที่มองไม่เห็น: การเติบโตของอาชญากรรมไซเบอร์ที่มุ่งเป้าสู่ภาครัฐ



สถิติล่าสุด (ม.ค. – มี.ค. 2569)

1,149 เหตุการณ์

ภายในเวลาแค่ **3 เดือน**

เป้าหมายสูงสุด:

1. การศึกษา (432)
2. ภาครัฐ (239)
3. เอกชนไทย (92)

สรุปสถิติภัยคุกคามทางไซเบอร์ของประเทศไทย ปี 2569

ข้อมูลสถิติรวมจากทุกรูปแบบการโจมตีที่เกิดขึ้น ม.ค.– มี.ค. 2569

NCSA สกมช

ความพยายามในการบุกรุกระบบ

286 ครั้ง

การหลอกลวงหรือฉ้อโกงออนไลน์

260 ครั้ง

1,149

พบเหตุการณ์ภัยคุกคามรวม (ครั้ง)

ความปลอดภัยข้อมูล (Information Content) ครองอันดับ 1

465

มีจำนวนสูงถึง **465 เหตุการณ์** ซึ่งเป็นภัยคุกคามที่ต้องเฝ้าระวังมากที่สุด

ภัยด้านระบบและความพร้อมใช้งาน

พบปัญหาด้านการทำให้ระบบใช้งานไม่ได้ **73 ครั้ง**

มัลแวร์ **51 ครั้ง**

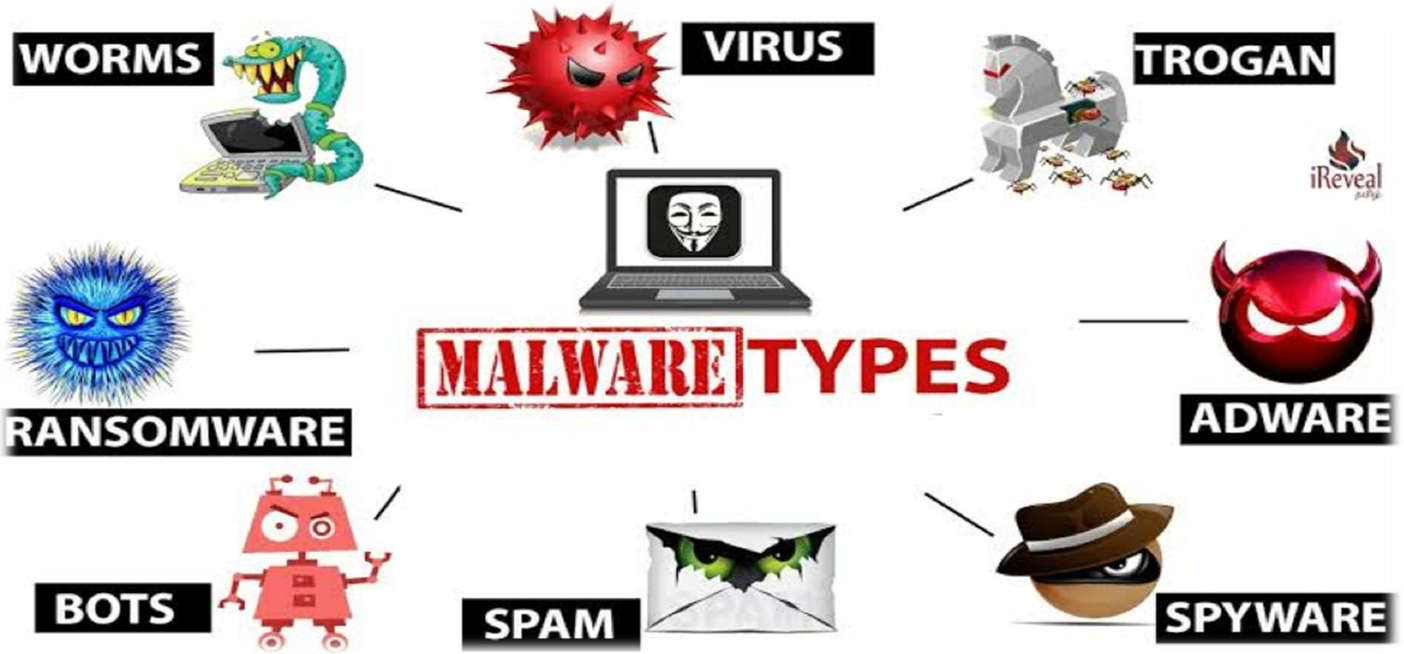
อัตราการบุกรุกสำเร็จอยู่ในระดับต่ำ

มีการบุกรุกเข้าสู่ระบบสำเร็จเพียง **14 ครั้ง** จากความพยายามทั้งหมด

รูปแบบภัยคุกคามทางไซเบอร์

รูปแบบของภัยคุกคามทางไซเบอร์

Malware (มัลแวร์)



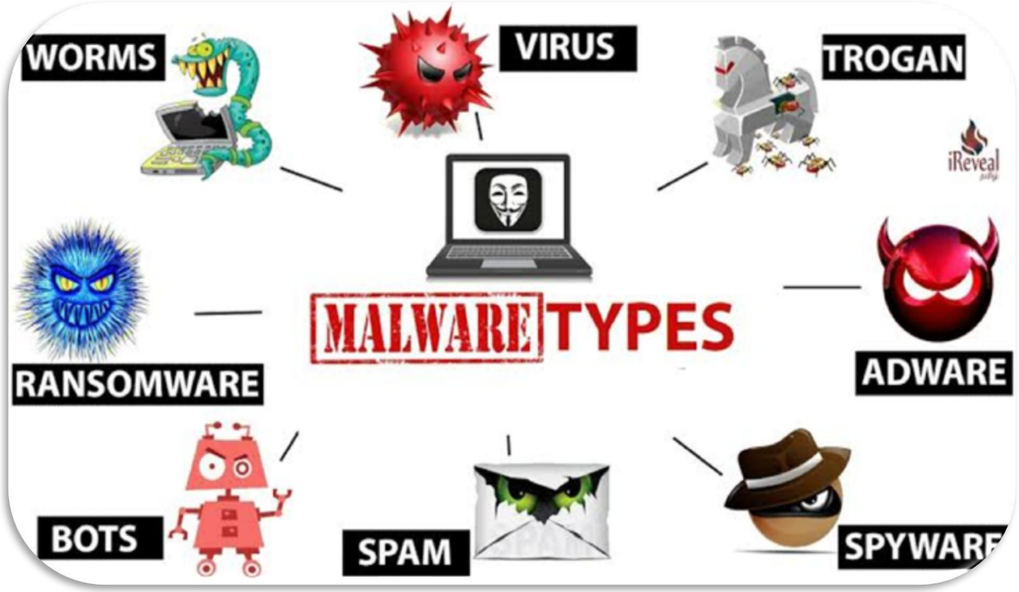
“ซอฟแวร์อันตราย ประสงค์ร้าย”

ภัยคุกคามประเภทนี้ มัก**แฝง**ตัวมากับ**ไฟล์ที่เราดาวน์โหลดจากเว็บไซต์ อีเมล** หรือจากอุปกรณ์เสริมที่เชื่อมต่อเข้ากับคอมพิวเตอร์

nt CYFENCE Securing your Business

รูปแบบของภัยคุกคามทางไซเบอร์

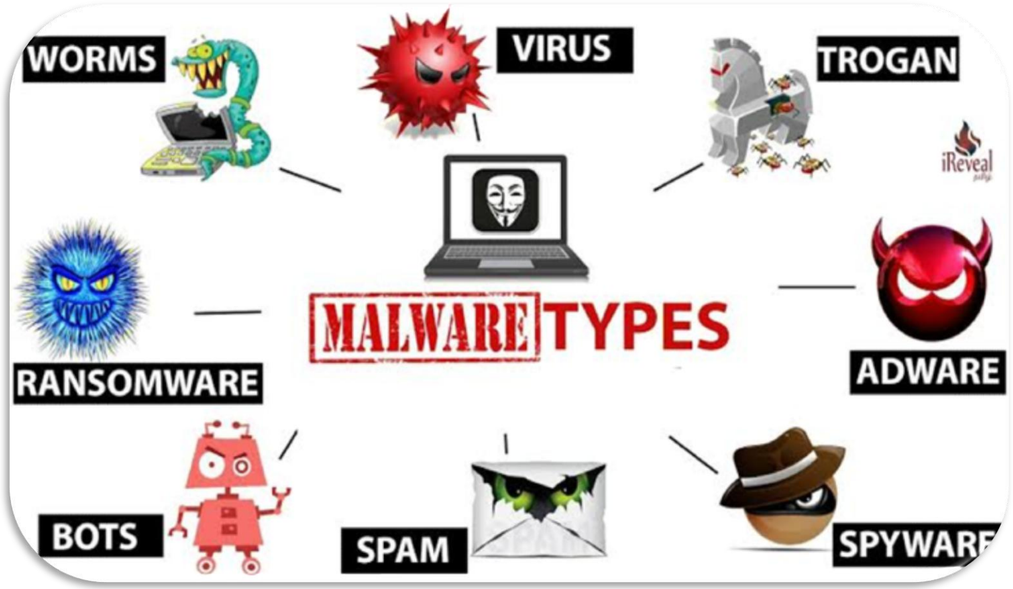
Malware (มัลแวร์)



- **Virus** แฝงตัวมากับโปรแกรมคอมพิวเตอร์หรือไฟล์ และสามารถแพร่กระจายไปยังเครื่องอื่น ๆ ได้โดยแนบตัวเองไปกับโปรแกรมหรือไฟล์ โดยไวรัสจะทำงานก็ต่อเมื่อมีการรันโปรแกรมหรือเปิดไฟล์เท่านั้น
- **Worm** เป็นมัลแวร์ชนิดที่สามารถแพร่กระจายตัวเองไปยังคอมพิวเตอร์และอุปกรณ์เครื่องอื่น ๆ ผ่านทางระบบเครือข่ายได้เองอัตโนมัติโดยไม่จำเป็นต้องอาศัยไฟล์โฮสต์หรือการเปิดไฟล์
- **Trojan** เป็นมัลแวร์ที่หลอกผู้ใช้ว่าเป็นโปรแกรมที่ปลอดภัย โทรจันไม่ได้แพร่กระจายตัวเองโดยตรง แต่เมื่อเผลอติดตั้งหรือเปิดใช้งาน จะแฝงการทำงานที่เป็นอันตรายไว้ มันจะเปิดช่องทางให้ผู้ไม่หวังดีเข้ามาควบคุมเครื่องหรือขโมยข้อมูล
- **Backdoor** คือช่องทางลับที่ Hacker สร้างขึ้นในระบบคอมพิวเตอร์ ซอฟต์แวร์ หรือเครือข่าย หลังจากเจาะระบบสำเร็จ เพื่อใช้ช่องทางนี้เข้าถึงระบบได้ โดยไม่ต้องผ่านการตรวจสอบปกติ เช่น ไม่ต้องใช้รหัสผ่าน หรือการยืนยันตัวตน

รูปแบบของภัยคุกคามทางไซเบอร์

Malware (มัลแวร์)



- **Rootkit** ซอฟต์แวร์ที่ถูกออกแบบมา เพื่อซ่อนการมีอยู่ของมัลแวร์เพื่อเปิดช่องทางให้ผู้อื่นเข้ามาติดตั้งโปรแกรมเพิ่มเติมเพื่อควบคุมเครื่อง พร้อมได้สิทธิ์ของผู้ดูแลระบบ (administrator,root)

- **Spyware** คือมัลแวร์ที่ออกแบบมาเพื่อแอบสอดแนม" พฤติกรรมการใช้งานคอมพิวเตอร์หรือโทรศัพท์ และอาจขโมยข้อมูลส่วนตัว เช่น บัญชีชื่อผู้ใช้งาน, รหัสผ่าน หรือข้อมูลทางการเงิน ข้อมูลบัตรเครดิต เป็นต้น

- **Adware** ซอฟต์แวร์ที่แสดงโฆษณาให้ผู้ใช้เห็นโดยอัตโนมัติ สร้างความรำคาญโดยการ โผล่เป็นป๊อปอัปโฆษณาบ่อย ๆ ขณะใช้งานอินเทอร์เน็ตหรือโปรแกรม แม้ไม่ได้เปิดเว็บเบราว์เซอร์

รูปแบบของภัยคุกคามทางไซเบอร์

Malware (มัลแวร์)

- Ransomware(แรนซัมแวร์)

คือ Hacker ที่ทำการขโมยข้อมูลไฟล์และเข้ารหัส ล็อกไฟล์ ไม่ให้ผู้ใช้สามารถเปิดไฟล์หรือระบบได้ จากนั้นก็จะส่งข้อความหาผู้ใช้หรือองค์กร เพื่อ “เรียกค่าไถ่ (Ransom)” แลกกับการถอดรหัสเพื่อกู้ข้อมูลคืนมา มักพบเจอบ่อยในระดับองค์กร หรือหน่วยงานรัฐบาล

กลุ่ม PUNK SPIDER (เน้นการบุกรุก – Execution)
ใช้สคริปต์ที่สร้างงโดย AI ในระหว่างการรโจมตี
สถิติ 2026: พบว่าการโจมตีเพิ่มขึ้น 134% จากปี2025

กลุ่ม HACKER LockBit ดำเนินการในรูปแบบ Ransomware as a Service (RaaS) คืออาชญากรให้บริการโครงสร้างพื้นฐานและมัลแวร์แก่ผู้โจมตี และรับส่วนแบ่งค่าไถ่

รูปแบบของภัยคุกคามทางไซเบอร์

Spam คือ วิธีการที่ผู้ส่งหรือผู้ไม่ประสงค์ดีส่งข้อมูล ข้อความ หรือโฆษณาต่าง ๆ ไปยังผู้รับผ่านช่องทางต่าง ๆ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับเพื่อสร้างความรำคาญ หรือก่อกวน และใช้แพร่กระจาย Malware




พรบ.คอมพ์ฯ ฉบับใหม่ 2560

ฝากร้านใน Facebook IG ส่ง SMS มาโฆษณา ส่ง Email ขายของ

ถือเป็น **Spam** **ปรับ 200,000 บาท**

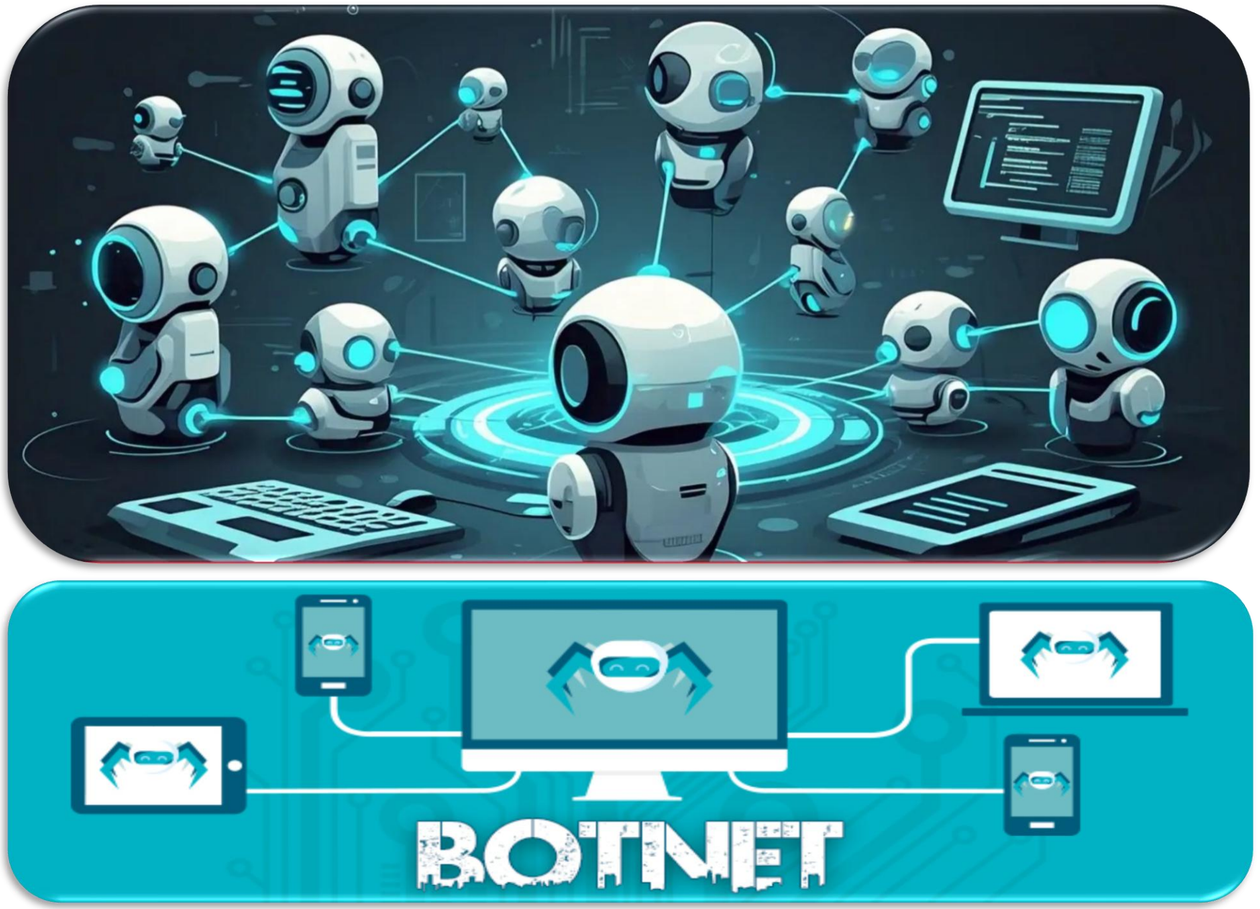
รูปแบบของภัยคุกคามทางไซเบอร์

Malware (มัลแวร์)

- **BOTNET**

อุปกรณ์ที่ติดมัลแวร์และถูกเปลี่ยนเป็น Bot (ย่อมาจาก Robot) ไม่ว่าจะเป็นอุปกรณ์คอมพิวเตอร์ เว็บแคม เราท์เตอร์ หรืออุปกรณ์ IoT อื่นๆ ในบ้าน เพื่อรอรับคำสั่งจากแฮ็กเกอร์

โดยแฮ็กเกอร์จะนำ Botnet ที่มีไปใช้ในโจมตีขนาดใหญ่ กรณีของ Mirai Botnet ที่โด่งดัง ซึ่งใช้ Botnet กว่า 600,000 เครื่องในการ DNS รายใหญ่ของโลกถล่ม



รูปแบบของภัยคุกคามทางไซเบอร์ที่พบบ่อย

Social Engineering

- **Phishing :** การส่งอีเมลปลอมจำนวนมหาศาลไปยังผู้คนนับล้านคน โดยหวังว่าจะมีใครสักคน "ติดเบ็ด"

คือ ภัยคุกคามที่มักใช้ร่วมกับเทคนิค Social engineering (การหลอกลวง ล่อหลอกผู้อื่น
ใช้หลักการพื้นฐานทางจิตวิทยาให้เหยื่อเปิดเผยข้อมูล)

ตัวอย่างเช่นผู้โจมตีส่งอีเมลที่ดูน่าเชื่อถือให้ผู้ใช้งานกดคลิกลิงก์ และเข้าไปกรอกข้อมูลบัตรเครดิต หรือข้อมูล Sensitive อื่น ๆ ในหน้าเพจที่ทำปลอมขึ้นมาอย่างแนบเนียน หรือให้ผู้ใช้ดาวน์โหลดไฟล์ที่แนบมากับอีเมลเพื่อติดตั้ง Malware หรือ Ransomware ในคอมพิวเตอร์ขององค์กร เป็นต้น

ตัวอย่าง: ฟิชชิ่งอีเมล์ ภัยคุกคามทางไซเบอร์

Social Engineering

From : "Webmail Service" <info-mail@seeddesign.co.za>

To : yourmail@kasikornbank.com

Date : Mon, Aug 24, 2015, 16:20

Subject : Email (yourmail@kasikornbank.com) Termination Notice

Account Notification

Your Email (yourmail@kasikornbank.com) will stop receiving messages due to the fact that our system detected a violation of Spam activities.

You have to verify and up-grade youre email address information to avoid account termination. To verify and up-grade yourmail@kasikornbank.com, simply click on the link below

Click Here to Verify & Up-grade your Account

http://webmail-secur.verification152.easywash.mail/mailimages-upgrade3540/

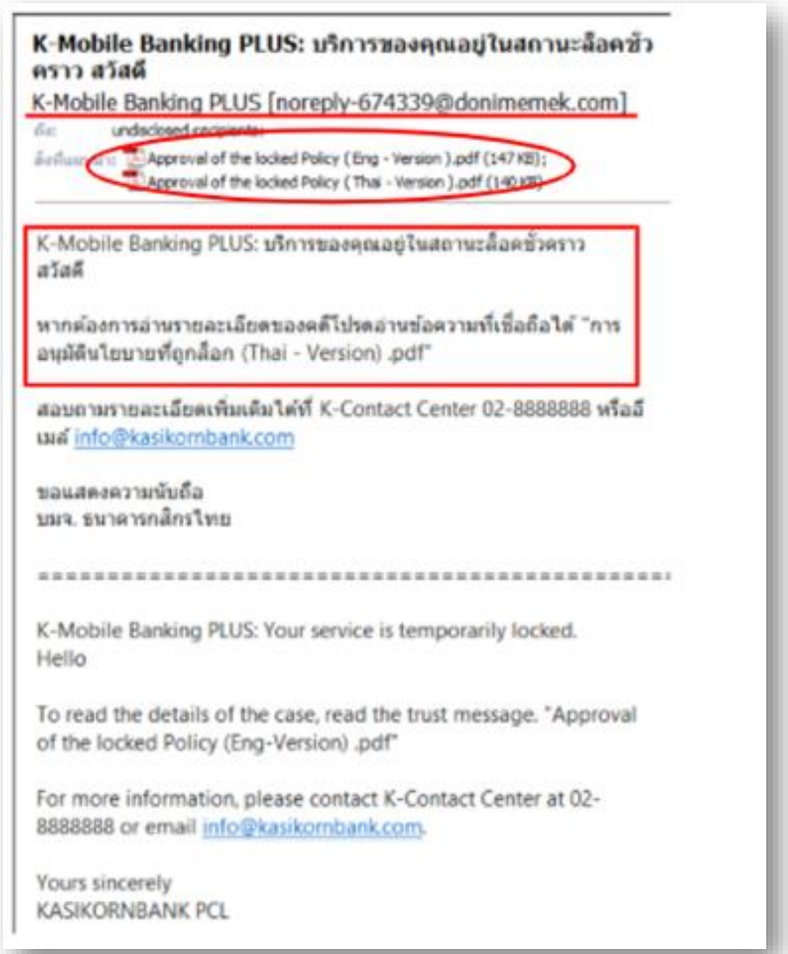
Thanks for using our service.

Sincerely

Webmail Administretor

noreply@kasikornbank.com_20190206.doc

1. ได้รับอีเมลจากผู้ส่งที่ไม่รู้จัก หรือไม่น่าเชื่อถือ
2. คำทักทายทั่วไปที่ไม่ระบุตัวบุคคล
3. เนื้อหาอีเมลมีลักษณะเป็นเรื่องเร่งด่วน และสำคัญ เพื่อให้ผู้ใช้ตกใจจนลืมตรวจสอบข้อเท็จจริง
4. ลิงก์ปลอม ตรวจสอบโดยเอาเมาส์ไปชี้ (ห้ามคลิก) จะปรากฏที่อยู่จริงๆ ซึ่งไม่ตรงกับลิงก์ที่แนบมา
5. เอกสารแนบที่มีชื่อไฟล์หรือนามสกุลน่าสงสัย



K-Mobile Banking PLUS: บริการของคุณอยู่ในสถานะล็อคชั่วคราว สวัสดี

K-Mobile Banking PLUS [noreply-674339@donimemek.com]

undisclosed-recipients:

Approval of the locked Policy (Eng - Version).pdf (147 KB);
Approval of the locked Policy (Thai - Version).pdf (140 KB)

K-Mobile Banking PLUS: บริการของคุณอยู่ในสถานะล็อคชั่วคราว สวัสดี

หากต้องการอ่านรายละเอียดขององค์โปรดอ่านข้อความที่เชื่อถือได้ "การอนุมัตินโยบายที่ถูกล็อก (Thai - Version) .pdf"

สอบถามรายละเอียดเพิ่มเติมได้ที่ K-Contact Center 02-8888888 หรืออีเมล์ info@kasikornbank.com

ขอแสดงความนับถือ
บมจ. ธนาคารกสิกรไทย

K-Mobile Banking PLUS: Your service is temporarily locked.
Hello

To read the details of the case, read the trust message. "Approval of the locked Policy (Eng-Version) .pdf"

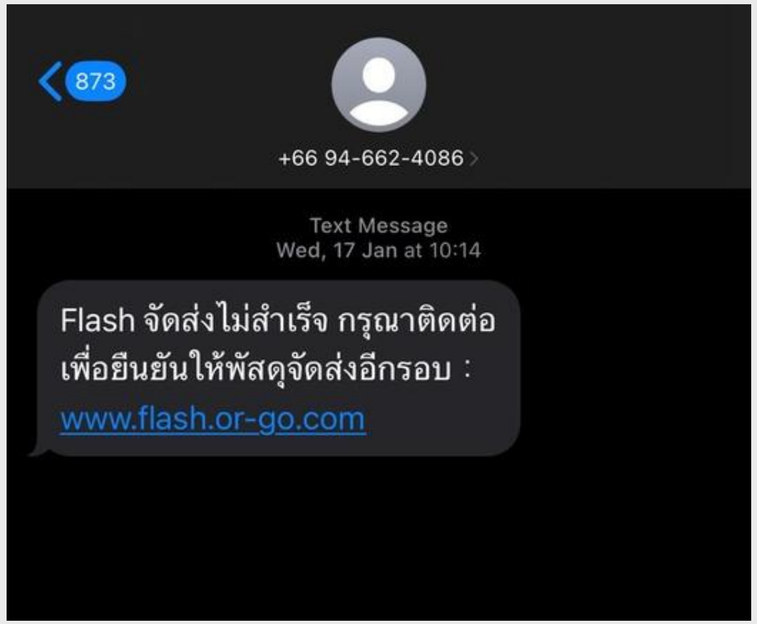
For more information, please contact K-Contact Center at 02-8888888 or email info@kasikornbank.com.

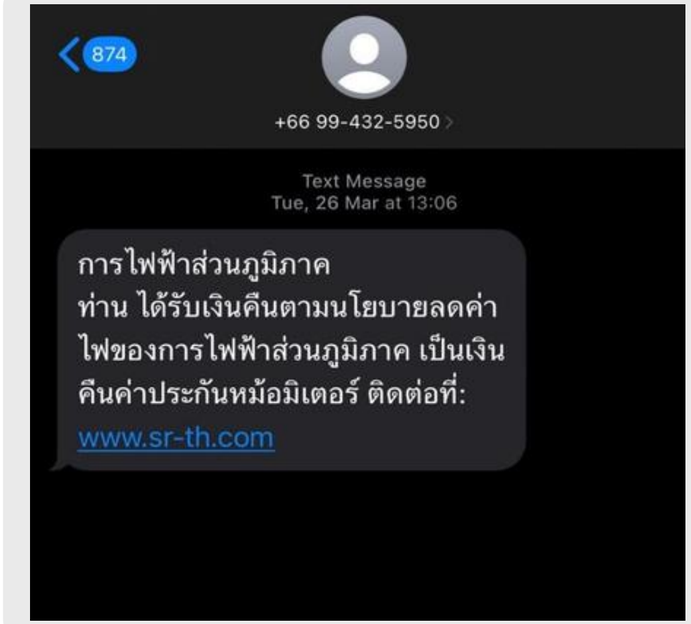
Yours sincerely
KASIKORNBANK PCL

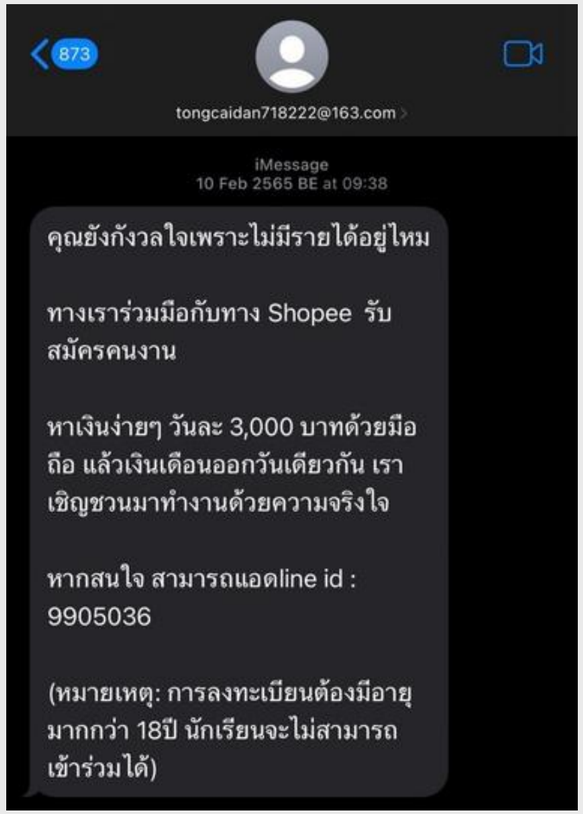
ตัวอย่าง: SMS Phishing ภัยคุกคามทางไซเบอร์

Social Engineering

- SMS Phishing / Smishing







รูปแบบของภัยคุกคามทางไซเบอร์

Social Engineering

- ## Voice Phishing/ Vishing/ แกงค์ Call center
  - หลอกล่อเหยื่อเพื่อขอข้อมูลสำคัญผ่านทาง **"เสียง"** หรือการโทรศัพท์
  - การใช้โทรศัพท์โทรมาหลอกลวง ในปี 2026 มักใช้ **AI Voice Cloning** ปลอมเป็นเสียงคนรู้จัก เพื่อสั่งให้ทำธุรกรรมด่วน
  - **Caller ID Spoofing:**
    แก๊ง Call Center ใช้เทคโนโลยีปลอมแปลงเบอร์โทรศัพท์ให้ดูเหมือนโทรมาจากหน่วยงานรัฐหรือธนาคารจริงๆ

nt CYFENCE
Securing your Business

รูปแบบของภัยคุกคามทางไซเบอร์

Social Engineering

- **Spear Phishing (แบบเจาะจงเหยื่อ)**

แฮกเกอร์จะเลือก "เป้าหมายเฉพาะเจาะจง" (เช่น พนักงานในแผนกบัญชีของบริษัท A หรือเลขานุการของผู้บริหารบริษัท B) โดยมีการศึกษาข้อมูลของเหยื่อมาเป็นอย่างดีก่อนลงมือ เพื่อสร้างเรื่องราวที่ดูสมจริงที่สุดจนเหยื่อแทบแยกไม่ออก

- **Whale Phishing (การล่าปลาวาฬ)**

เป็น Spear Phishing เวอร์ชั่นที่พุ่งเป้าไปที่ "ผู้บริหารระดับสูง" (C-Level) CEO CFO หรือผู้ที่มีอำนาจตัดสินใจเรื่องเงิน

เป้าหมาย: เพื่อขโมยข้อมูลความลับของบริษัท หรือหลอกให้โอนเงินจำนวนมหาศาล

CYFENCE
Securing your Business

รูปแบบของภัยคุกคามทางไซเบอร์

Social Engineering

- **Baiting:**
  การวาง Flash Drive ที่ติดมัลแวร์ทิ้งไว้ในที่สาธารณะ (เช่น ห้องอาหาร)
  เพื่อล่อให้พนักงานเก็บไปเสียบกับคอมพิวเตอร์บริษัทด้วยความอยากรู้อยากเห็น

- **Pretexting**

ผู้โจมตีจะ **"สร้างเรื่องโกหกหรือสถานการณ์สมมติขึ้นมา"** (The Pretext) เพื่อใช้เป็นข้ออ้างในการหลอกล่อให้เหยื่อเชื่อใจ จนยอมเปิดเผยข้อมูลสำคัญหรือทำในสิ่งที่ผู้โจมตีต้องการ

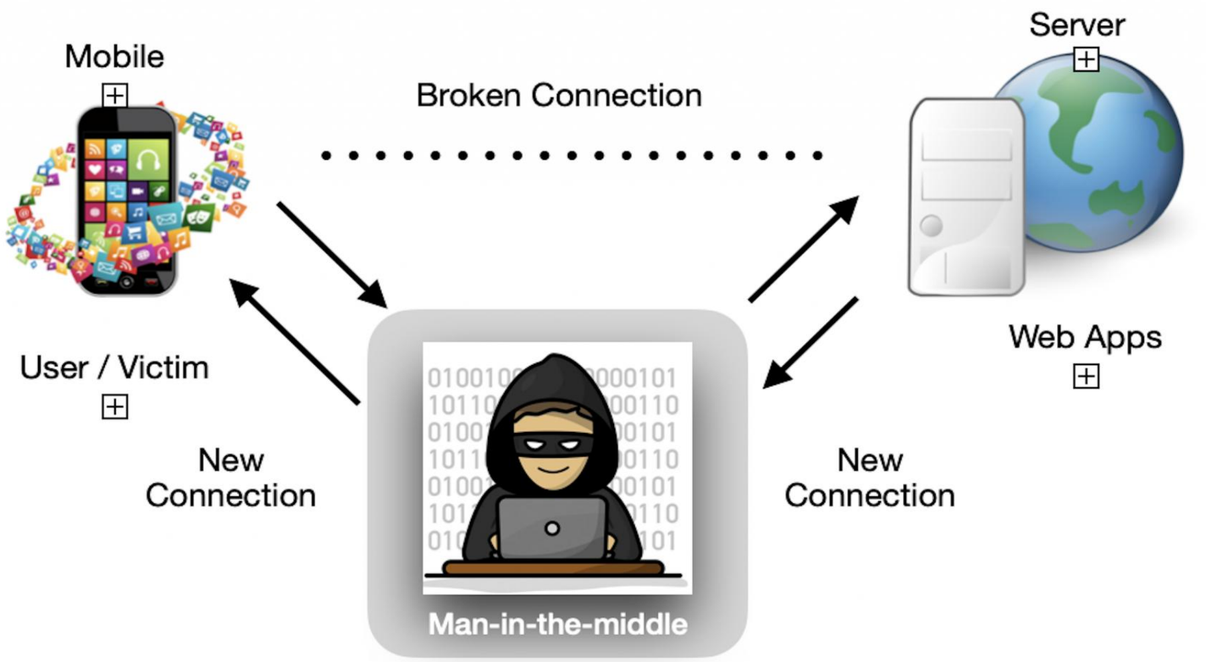
CYFENCE
Securing your Business

รูปแบบของภัยคุกคามทางไซเบอร์

- **Man in The Middle (MitM)**

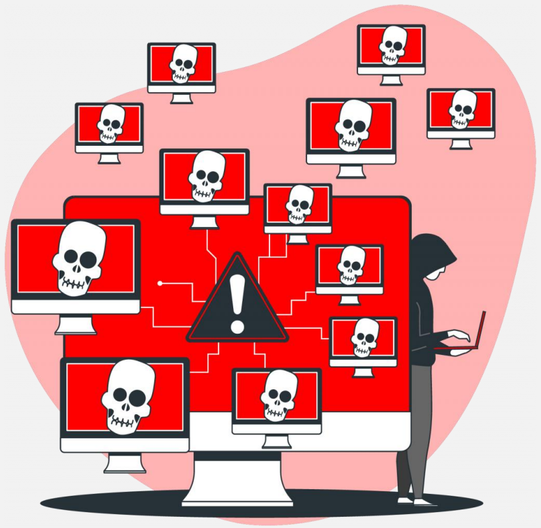
  การโจมตีทางไซเบอร์รูปแบบหนึ่งที่แฮกเกอร์แทรกตัวอยู่ตรงกลางระหว่างการสื่อสารของสองฝ่าย (เช่น ผู้ใช้กับเว็บไซต์ธนาคาร) โดยที่คู่สนทนาไม่รู้ตัว เพื่อดักฟัง ขโมยข้อมูลส่วนตัว รหัสผ่าน หรือแอบแก้ไขข้อมูลที่รับส่งกัน ทำให้ข้อมูลสูญหายหรือการทำธุรกรรมผิดพลาด

➢ **สถานการณ์ในชีวิตจริงที่คนทั่วไปมักโดน:**
- Wi-Fi ปลอมตามคาเฟ่/สนามบิน
- เว็บไซต์ปลอม



รูปแบบของภัยคุกคามทางไซเบอร์

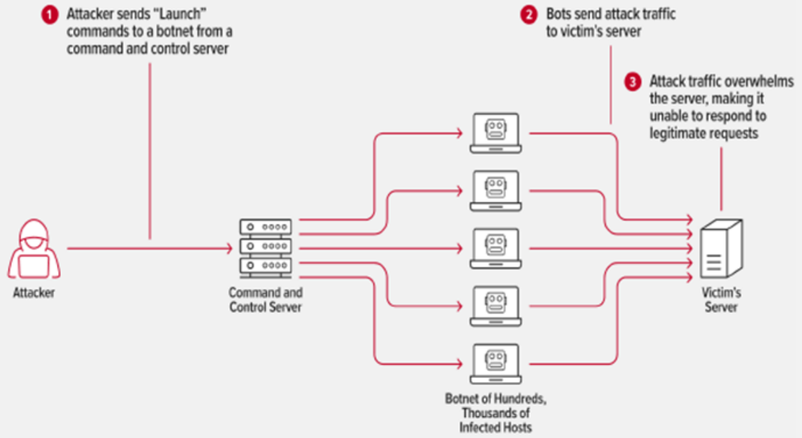
Network



DDoS (Distributed Denial of Service)

(Targeting the Server)

DDOS วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์ หรือระบบการให้บริการ โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียวภายในเวลาเดียวกัน จุดประสงค์เพื่อให้เว็บไซต์ ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือเกิดระบบล่มในที่สุด



https://www.nginx.com/resources/glossary/distributed-denial-of-service/

CYFENCE
Securing your Business

รูปแบบของภัยคุกคามทางไซเบอร์

DATA & Application

หนึ่งในช่องโหว่ของเว็บแอปพลิเคชันที่ร้ายแรงมากที่สุด

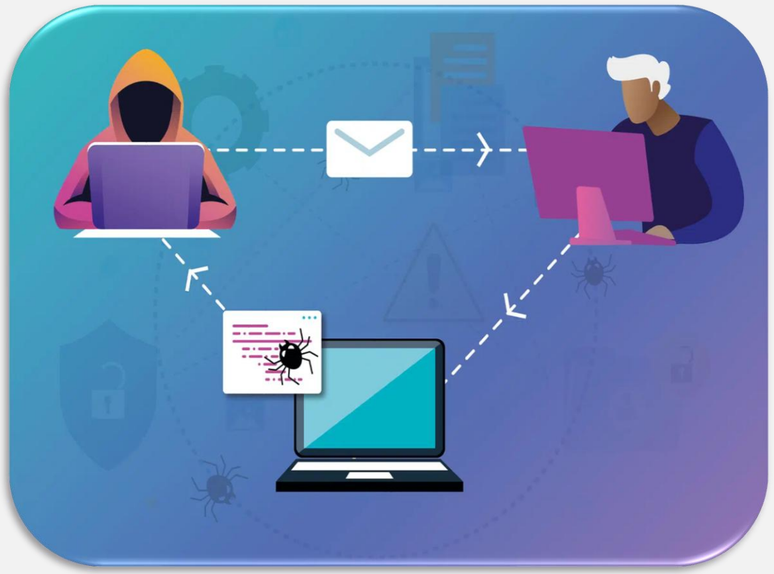
SQL Injection Attacks

(Targeting the Server)

คือเทคนิคการโจมตีทางไซเบอร์ ที่แฮกเกอร์แอบใส่ "คำสั่งคอมพิวเตอร์ที่อันตราย" ลงไปในช่องกรอกข้อมูลปกติบนหน้าเว็บได้ โดยอาศัยช่องโหว่ SQLi เพื่อหลอกให้ระบบฐานข้อมูลหลังบ้านทำงานตามที่แฮกเกอร์ต้องการ แฮกเกอร์สามารถเข้าถึงข้อมูลที่ไม่ได้รับอนุญาตและสามารถ แก้ไข/ สร้าง/ ลบ/ และจัดการข้อมูลที่เป็นความลับของเหยื่อ

CYFENCE
Securing your Business

รูปแบบของภัยคุกคามทางไซเบอร์



Cross-Site Scripting (XSS) (Targeting the User)

คือ ที่ผู้โจมตีฝังสคริปต์ที่เป็นอันตราย เข้าไปในหน้าเว็บที่ดูน่าเชื่อถือ(หรือเว็บจริงที่ถูกแฮก) โดยอาศัย ช่องโหว่ความปลอดภัยบนเว็บแอปพลิเคชัน เมื่อเหยื่อเปิดหน้าเว็บนั้น เบราว์เซอร์จะรันสคริปต์โดยเข้าใจว่าเป็นโค้ดของเว็บไซต์จริง ทำให้ผู้โจมตีขโมยข้อมูล เช่น คุกกี้ เซสชัน ID เพื่อใช้สวมรอยผู้ใช้ได้

Hacker จะฝัง XSS ในส่วนที่ผู้ใช้พิมพ์โต้ตอบกัน (เช่น เว็บบอร์ด, ช่องคอมเมนต์)

XSS ใช้เป็นเทคนิค

- การเปลี่ยนหน้าเว็ปไซด์ (web Defacement)
- การทำเว็ปไซด์ปลอม Phishing
- เปิด" หน้าเว็บที่อันตรายอัตโนมัติ มัลแวร์ก็สามารถแอบติดตั้งลงในเครื่อง

รูปแบบของภัยคุกคามทางไซเบอร์

DATA & Application

0

Zero-Day Attack

คือการที่แฮกเกอร์ใช้ประโยชน์จากช่องโหว่ (Vulnerability) ในซอฟต์แวร์ที่ยังไม่เคยถูกค้นพบมาก่อน ทำให้ผู้พัฒนาไม่มีเวลาสร้างวิธีแก้ไขหรือ Patch ได้ทัน ส่งผลให้การป้องกันทำได้ยากมากและเป็นภัยคุกคามร้ายแรง

"Zero-day" หมายถึงจำนวนวันที่ผู้พัฒนามีเวลาในการแก้ไขหลังจากที่ช่องโหว่ถูกนำมาใช้โจมตีเป็นครั้งแรก

รูปแบบของภัยคุกคามทางไซเบอร์ที่พบบ่อย

DATA & Application

Data Breach (การละเมิดข้อมูล/ การรั่วไหลของข้อมูล)

คือการเข้าถึงข้อมูลที่เป็นความลับโดยไม่ได้รับอนุญาต เช่น ข้อมูลทางการเงิน ข้อมูลส่วนบุคคล ข้อมูลธุรกิจ หรือข้อมูลที่มีความสำคัญอื่นๆ

<u>สาเหตุของการละเมิดข้อมูล</u>

1.การโจมตีทางไซเบอร์ (Cyber Attacks):

- ที่มุ่งเป้าเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

2. ความผิดพลาดของบุคลากร (Human Error):

- การตั้งค่าความปลอดภัยที่ไม่ถูกต้อง หรือการเปิดเผยข้อมูลโดยไม่ตั้งใจ

3. การถูกขโมยหรือสูญหายของอุปกรณ์ (Theft or Loss of Devices):

- การสูญหายของอุปกรณ์เก็บข้อมูลที่มีข้อมูลสำคัญ : USB FLASH DRIVE/External HDD

ผลกระทบ

ข้อมูลสำคัญส่วนตัวหรือขององค์กรโดนนำไปเผยแพร่

ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล

เสียหายต่อชื่อเสียงและความน่าเชื่อถือ

nt CYFENCE Securing your Business

รูปแบบของภัยคุกคามทางไซเบอร์

Insider Threat

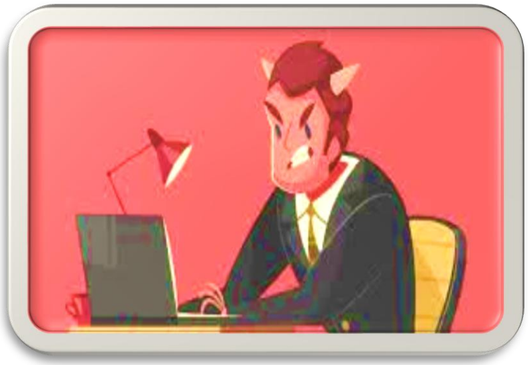
1. พนักงานปัจจุบัน
2. อดีตพนักงาน
3. Partners/Vendors: ผู้ให้บริการภายนอกที่ได้รับสิทธิ์

3 ประเภท

1.กลุ่มนี้มีเจตนาชัดเจนที่จะทำลายหรือขโมยข้อมูล

เกิดจาก :

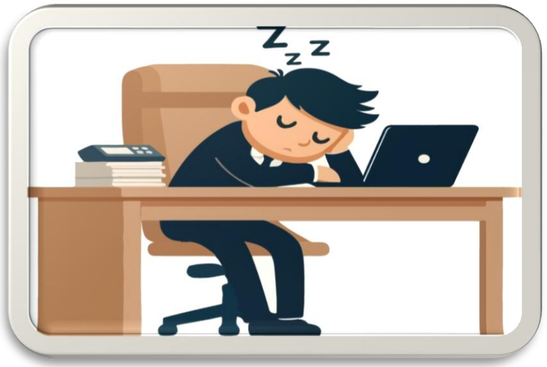
- ความแค้น:
- ผลประโยชน์ทางเงิน



Malicious

2. ผู้ที่ประมาทเลินเล่อไม่ได้ตั้งใจจะทำร้ายองค์กร

- เผลอกดลิงก์ Phishing
- ทำ Flash Drive ที่มีข้อมูลสำคัญหาย



Negligent

3. ผู้ที่ถูกขโมยตัวตน ถูกหลอกเป็นเหยื่อ

- บัญชีผู้ใช้งาน (Username/Password) ของถูกแฮกเกอร์ขโมยไป

Compromise

รูปแบบของภัยคุกคามทางไซเบอร์

IoT Vulnerability

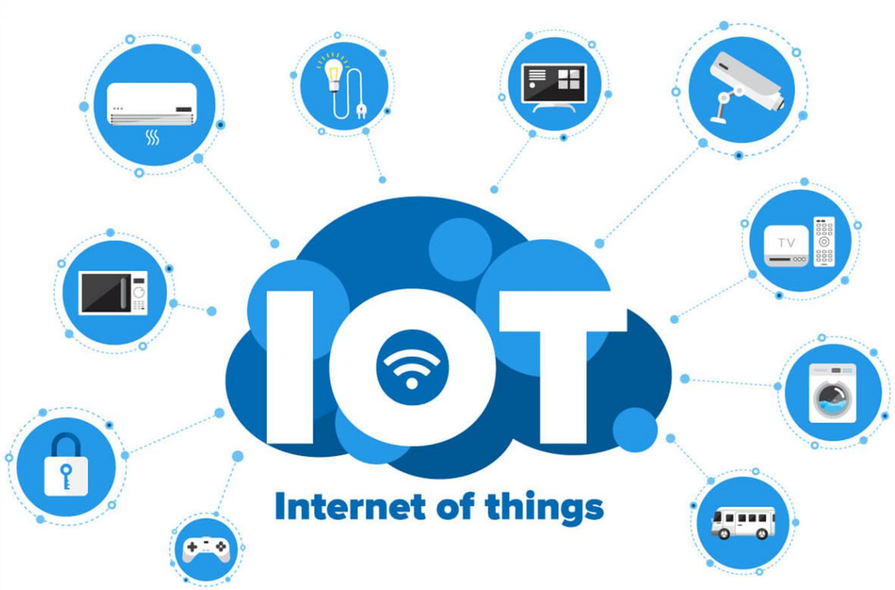
คือ ช่องโหว่ของอุปกรณ์ IoT" ที่เชื่อมต่อกับอินเทอร์เน็ต เช่น กล้องวงจรปิด, หลอดไฟอัจฉริยะ, ตู้เย็นอัจฉริยะ, เครื่องจักรในโรงงาน

ทำไมอุปกรณ์ IoT ถึงมีช่องโหว่เยอะ?

1. ผู้ผลิตตั้งรหัสผ่านที่เดาง่าย และผู้ใช้งานไม่เคยเปลี่ยน

2. ขาดการอัปเดตความปลอดภัยจากผู้ผลิตเหล่านั้น

3. อุปกรณ์ IoTมีการรับส่งข้อมูลที่ไม่ปลอดภัย



รูปแบบของภัยคุกคามทางไซเบอร์

OT Vulnerability

ช่องโหว่ของระบบเทคโนโลยีปฏิบัติการ" (Operational Technology)

ช่องโหว่ในระบบ OT ถึงน่ากลัวและต่างจาก IT

1. อุปกรณ์มีอายุการใช้งานนาน (Legacy Systems)

- เครื่องจักรในโรงงานถูกออกแบบมาให้ใช้งาน 15–20 ปี
- ยังใช้ระบบปฏิบัติการเก่าแก่ (เช่น Windows XP) ที่ไม่มีการอัปเดต

2. เน้น "ความต่อเนื่อง" มากกว่า "ความปลอดภัย"

- อัปเดตแพตช์ (Patch)" เป็นเรื่องใหญ่มาก ทำให้ช่องโหว่ที่ค้นพบมักจะไม่ถูกแก้ไขทันที

3.ไม่ได้ถูกออกแบบมาเพื่อเชื่อมต่ออินเทอร์เน็ต

- มีการเชื่อมต่อ OT เข้ากับ Internet เพื่อให้ดูข้อมูลการผลิตได้จากทุกที่ เสี่ยงต่อ Hacker เจาะระบบ

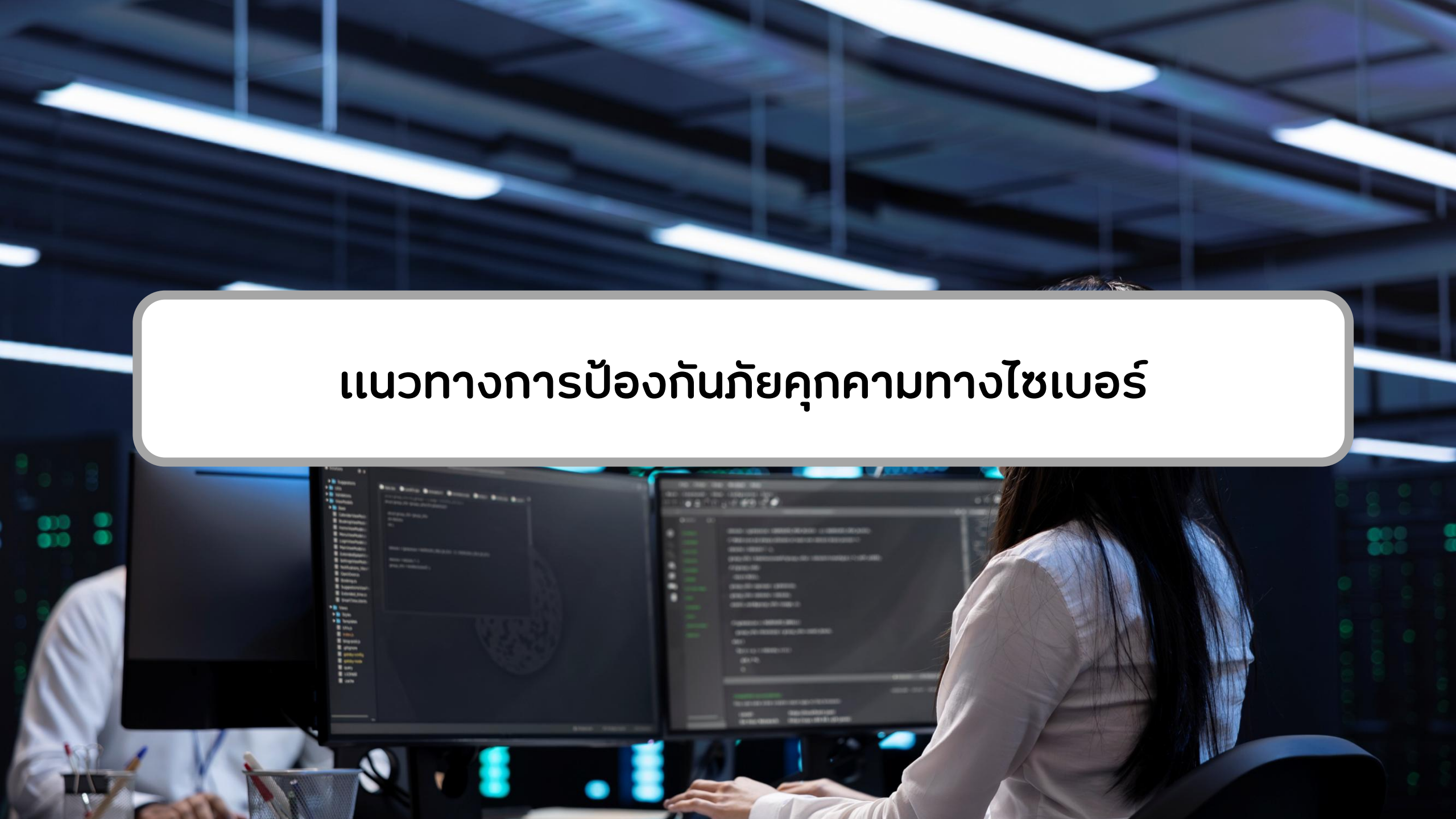
รูปแบบของภัยคุกคามทางไซเบอร์

Deep fakes:

- วิดีโอ/เสียงปลอมที่สร้างโดย AI
- เลียนแบบใบหน้า, เสียง, ท่าทางของบุคคลจริง (ผู้บริหาร, บุคคลสาธารณะ)
- ยากต่อการแยกแยะความจริง

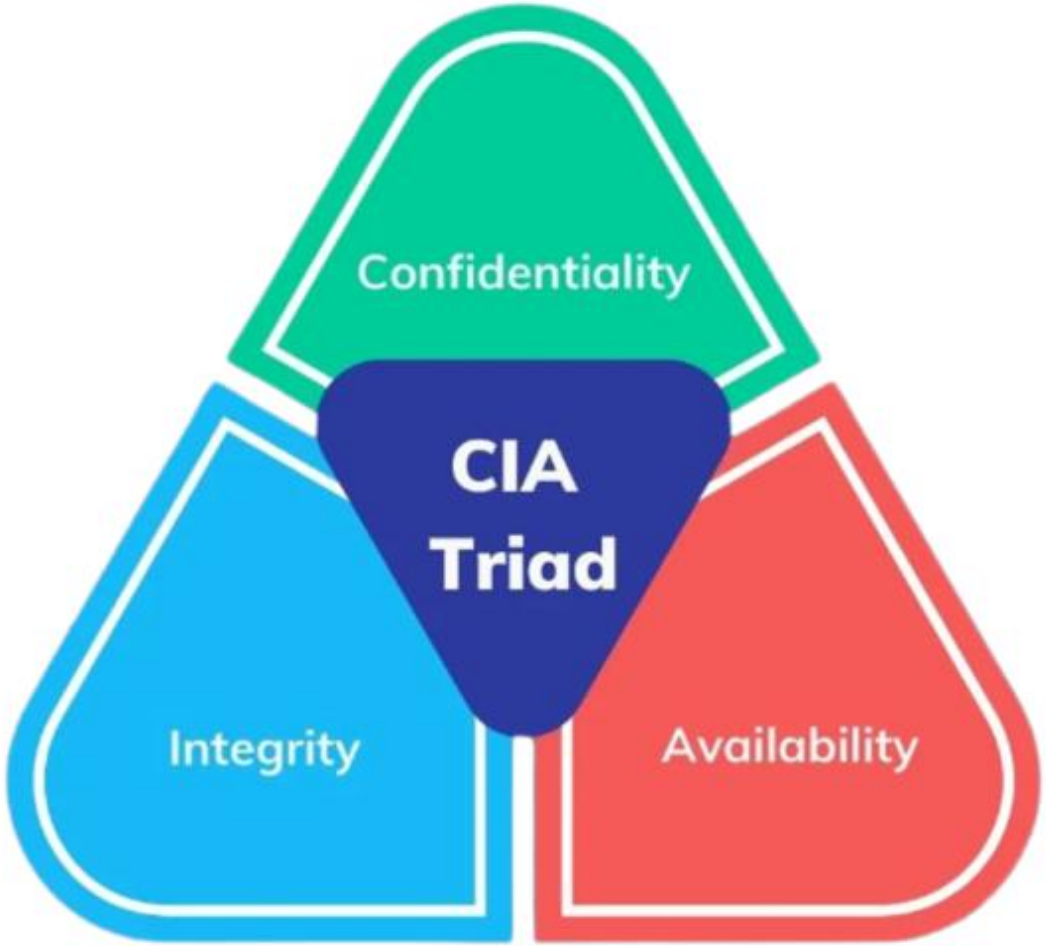
AI-Powered Scams:

- การหลอกลวงที่ซับซ้อนและแนบเนียนขึ้นด้วย AI
- ใช้ AI สร้างบทสนทนา, วิเคราะห์ข้อมูลเหยื่อ
- ตัวอย่าง: Call Center หลอกลวงแนบเนียน, การสร้างข่าวปลอม, เลียนแบบเสียงปลอม



แนวทางการป้องกันภัยคุกคามทางไซเบอร์

ส่วนประกอบหลักของความมั่นคงปลอดภัยสารสนเทศ



- **Confidentiality (การรักษาความลับ)**
  การปกป้องข้อมูลหรือระบบให้สามารถเข้าถึงได้
  เฉพาะผู้ที่มีสิทธิ์เท่านั้น

- **Integrity (ความถูกต้องและความครบถ้วน)**
  การป้องกันไม่ให้ข้อมูลหรือระบบถูกดัดแปลงแก้ไข
  โดยไม่ได้รับอนุญาต และการตรวจสอบให้แน่ใจว่าข้อมูลที่เก็บไว้
  หรือ ส่งต่อยังคงความถูกต้องและครบถ้วนเสมอ

- **Availability (ความพร้อมใช้งาน)**
  การทำให้ข้อมูลหรือระบบสามารถเข้าถึงและใช้งานได้เมื่อผู้ใช้ต้องการ

nt CYFENCE Securing your Business

Model of Process Improvement

People

This includes the employees that execute tasks, managers and leaders who set goals and make decisions, or stakeholders who bring companies toward their goals.

Process

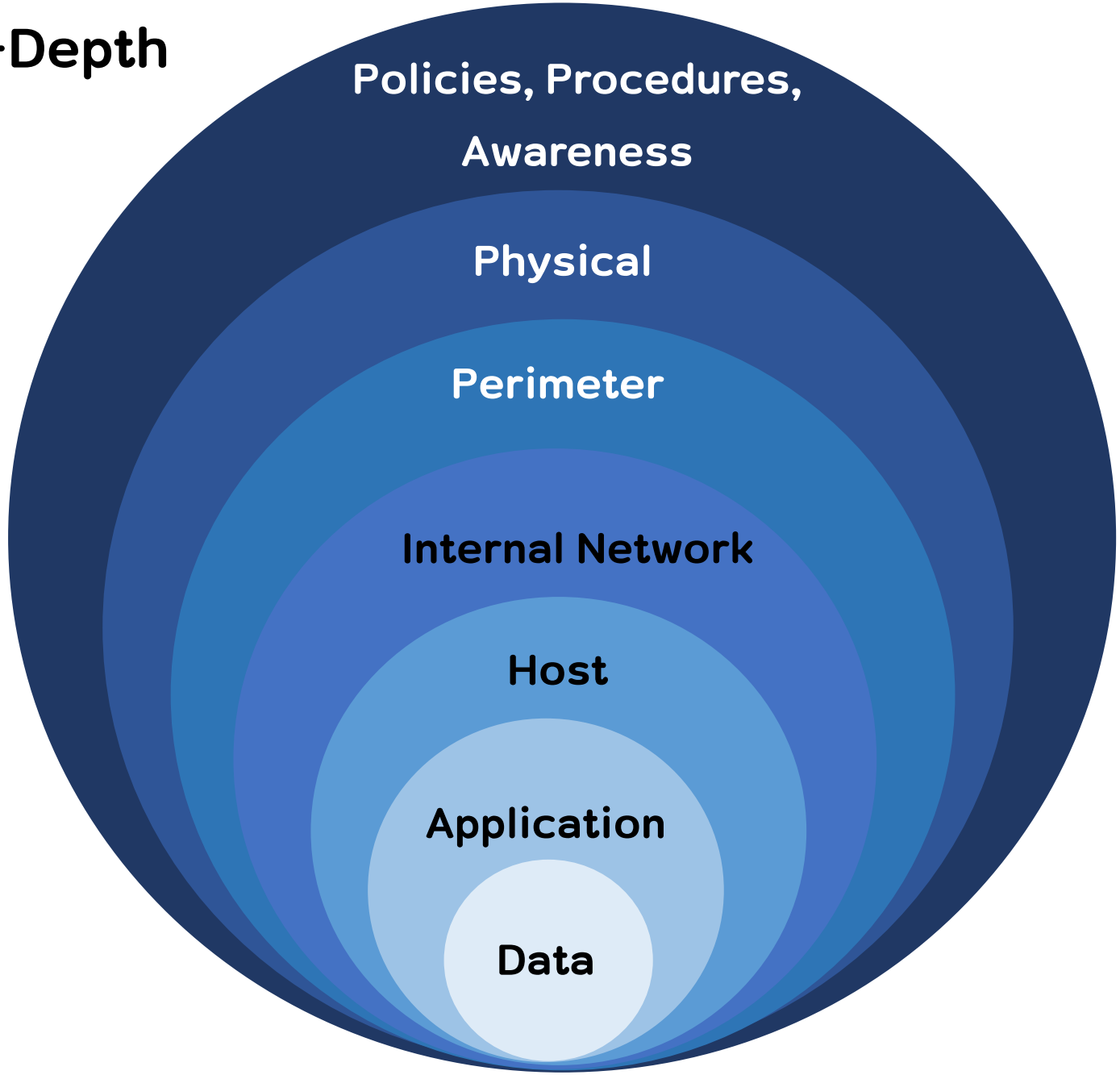
Process enables this by acting as the foundation that aligns people with the culture and quality of work a project or initiative needs.

Technology

The tools and systems you use to support or enable your team to carry out processes more efficiently.

วิธีการป้องกันภัยคุกคามไซเบอร์รูปแบบต่าง ๆ

1. Defense-in-Depth



2. Incident Response Plan

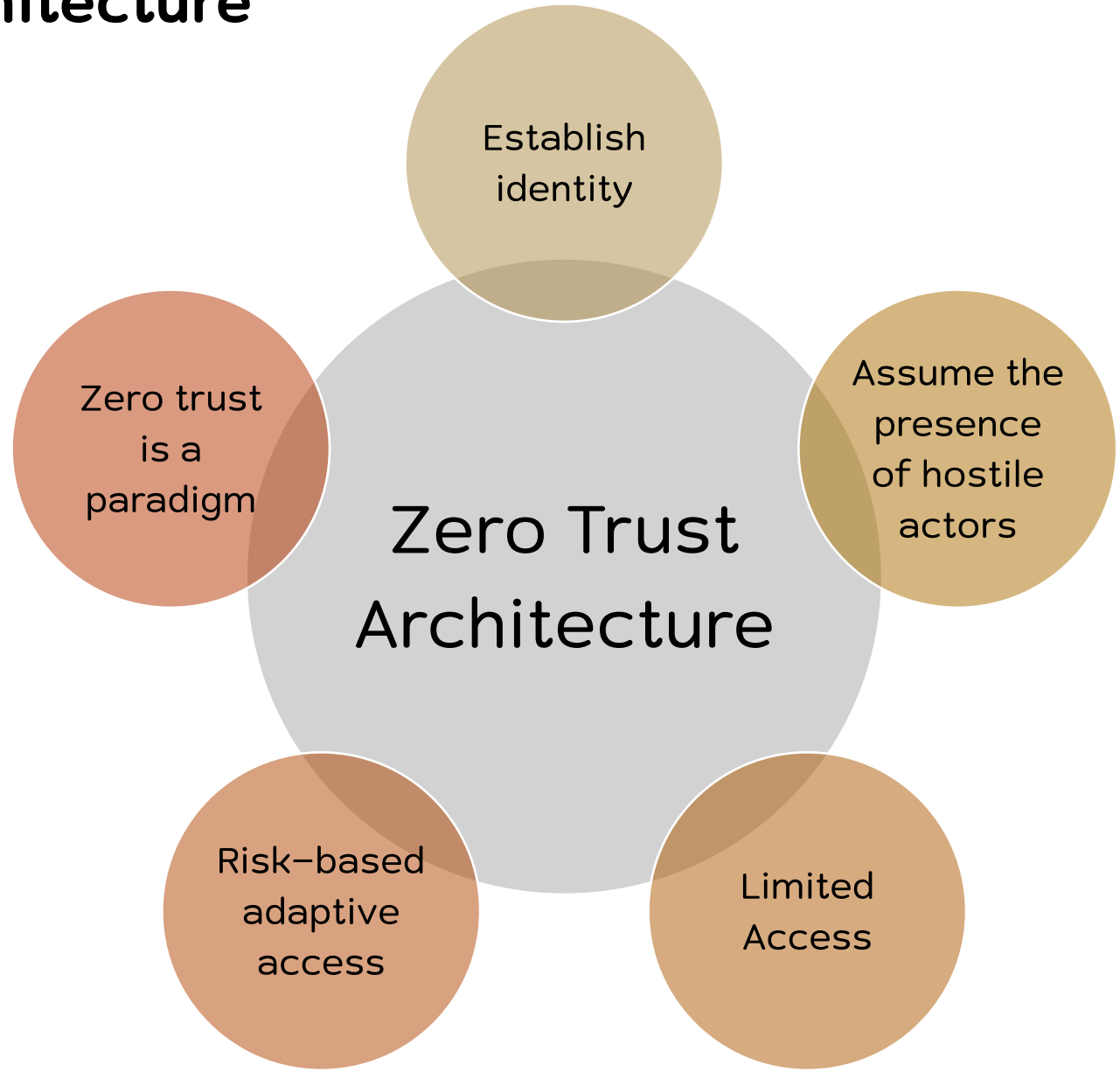
Preparation

Detection & Analysis

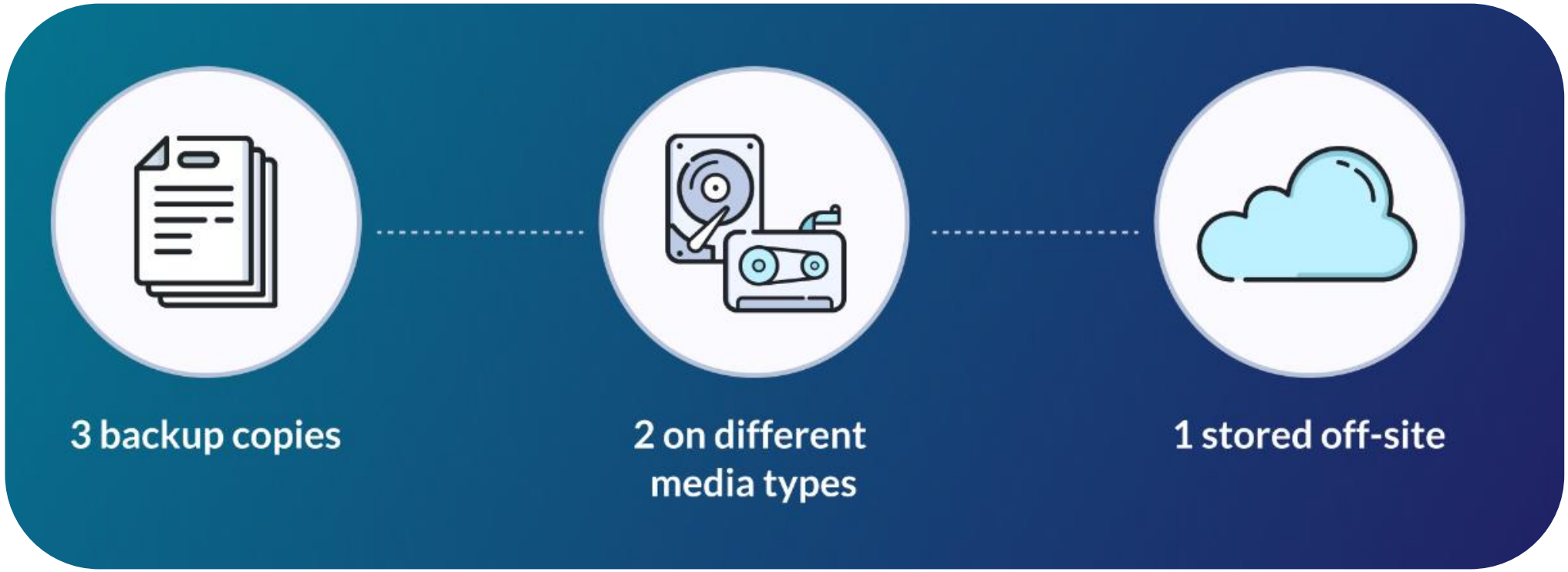
Containment, Eradication & Recovery

Lesson Learned

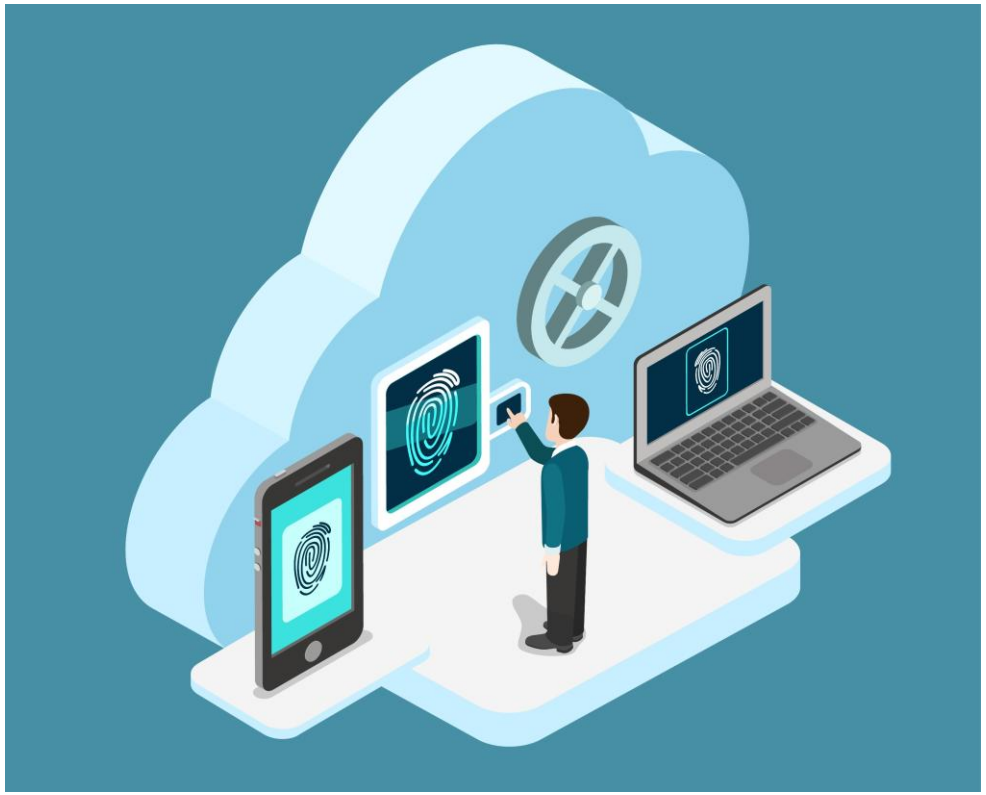
3. Zero Trust Architecture



4. Data Backup



5. Cloud Security



Safeguarding Data Privacy and Compliance

Ensuring Identity Verification and Controlled Access

Detecting Threats and Implementing Responses

Preserving Network Security

Devising Robust Security Configurations

6. Enforce Multi–factor Authentication (MFA)

7. Principle of Least Privilege

Restrict privileges

Only necessary systems and applications

Employee Access

8. AI & Automation

Predictive Analytics and Incident Prevention

Threat Detection and Response

Endpoint Protection

Automating Routine Security Tasks

CYFENCE
Securing your Business

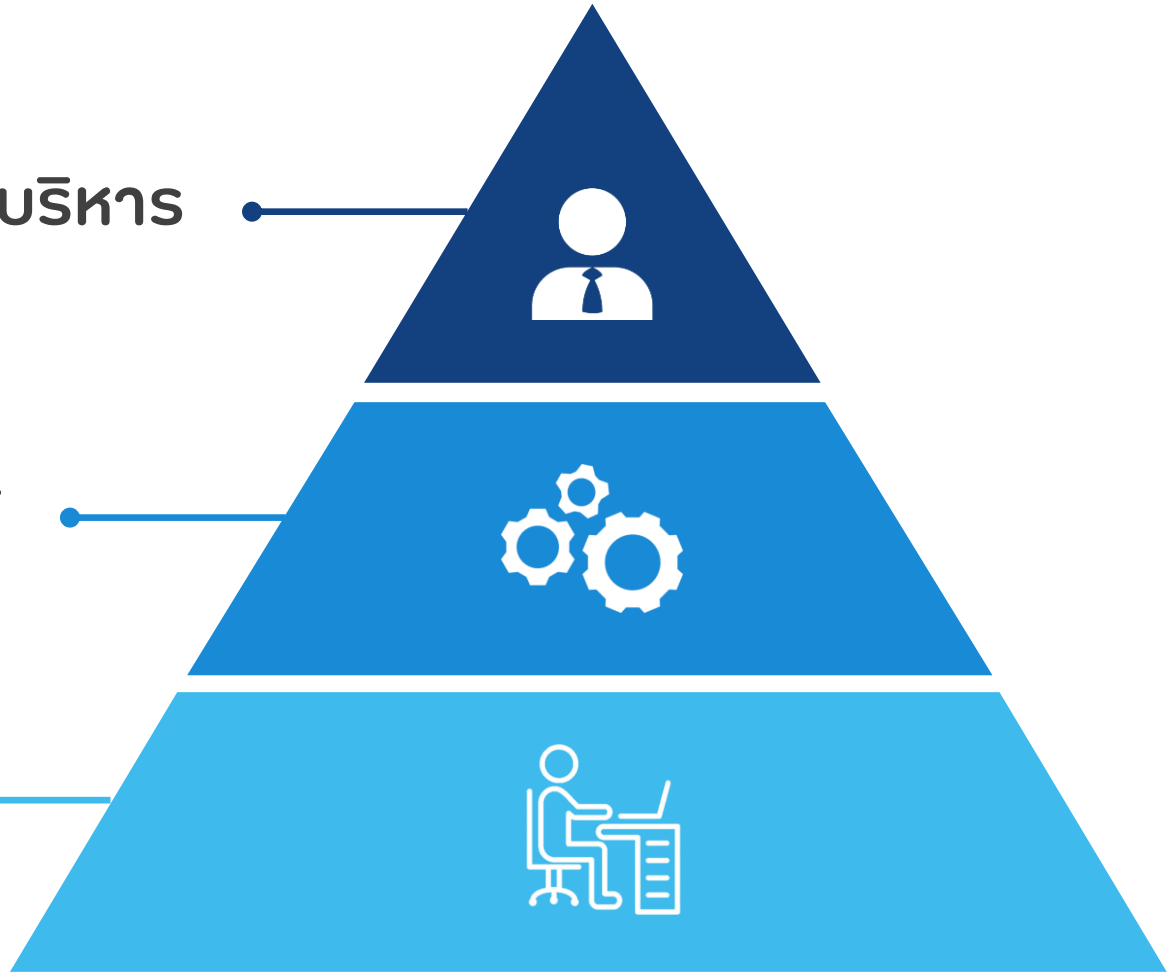
บทบาทและหน้าที่รับผิดชอบของบุคลากรที่เกี่ยวข้อง

บทบาทและหน้าที่รับผิดชอบของบุคลากรที่เกี่ยวข้อง

ผู้บริหาร

เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ

บุคลากรทั่วไป (User)



บทบาทหน้าที่ของผู้บริหาร

1. สนับสนุนด้านความมั่นคงปลอดภัยสารสนเทศ
2. ลงทุนจัดสรรทรัพยากร
3. สนับสนุนบุคลากร

4. กำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ
5. ร่วมมือและสื่อสาร
6. ส่งเสริมวัฒนธรรมแบบมีส่วนร่วม

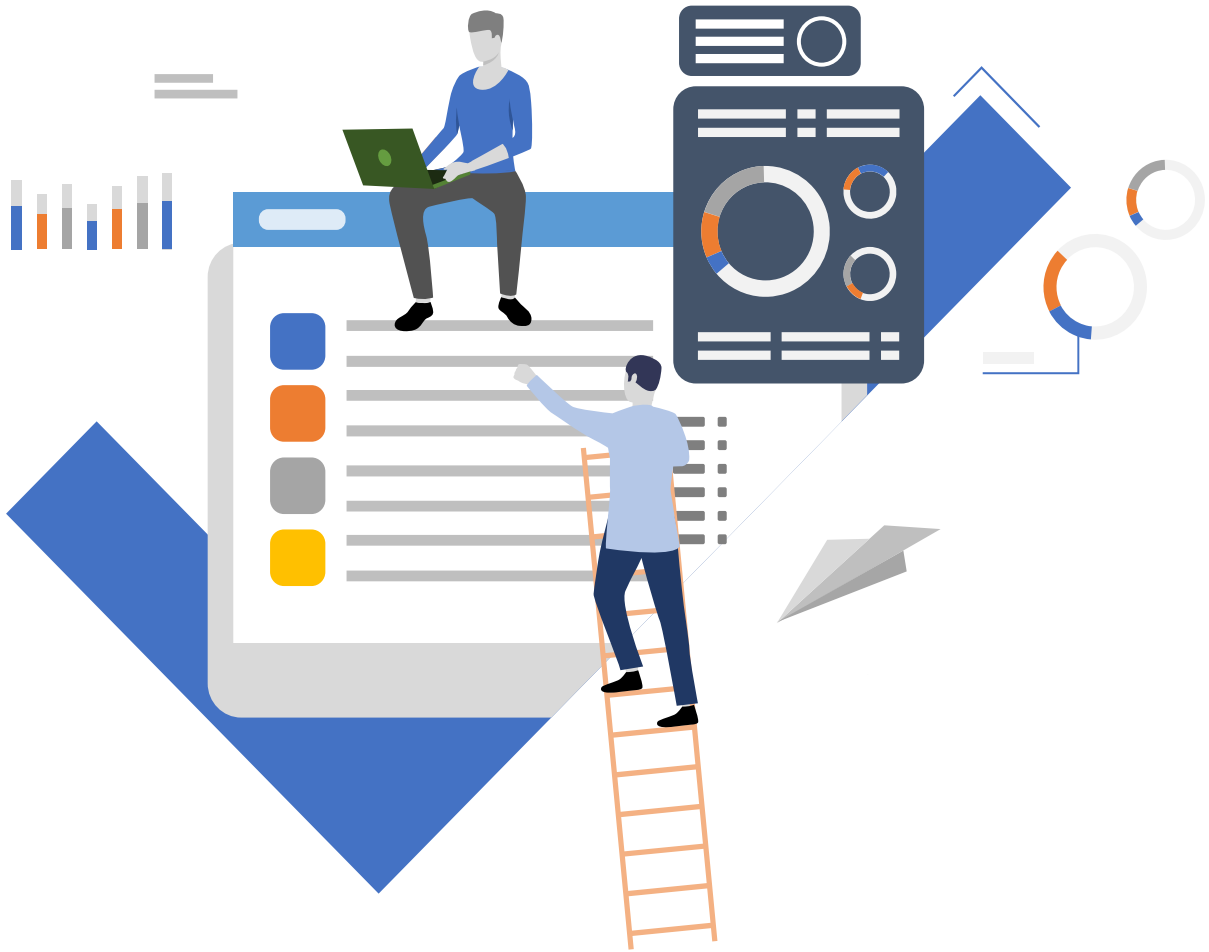
nt CYFENCE Securing your Business

บทบาทหน้าที่ของเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ

1. มีการเฝ้าระวังด้านความมั่นคงปลอดภัยสารสนเทศ
2. ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
3. ติดตั้งระบบป้องกันเครือข่าย อาทิ Firewall
4. Secure Delete อุปกรณ์ที่ไม่ใช้แล้ว
5. Vulnerability Assessment and Penetration Test

nt CYFENCE Securing your Business

บทบาทหน้าที่ของบุคลากรทั่วไป (User)



1. ร่วมกิจกรรมสร้างความตระหนัก
2. ติดตามข่าวสารเกี่ยวกับภัยคุกคาม
3. แจ้งผู้เกี่ยวข้องเมื่อพบกิจกรรมน่าสงสัยหรือภัยคุกคาม
4. ปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ
5. ให้ความร่วมมือในการรักษาความมั่นคงปลอดภัยสารสนเทศ

เมื่อถูกโจมตี! สัญญาณเตือนที่ต้องสังเกต

1. คอมพิวเตอร์/อุปกรณ์ทำงานช้าผิดปกติ, แฮงค์บ่อย
2. มี Pop-up แปลกๆ ขึ้นมาเอง, โปรแกรมเปิด/ปิดเอง
3. ไฟล์งานถูกเข้ารหัส / เปิดไม่ได้ / หายไป
4. บัญชีออนไลน์ถูกล็อก / มีการล็อกอินจากที่ที่ไม่รู้จัก
5. เพื่อน/หน่วยงานแจ้งว่าได้รับอีเมล/ข้อความแปลกๆ จากเรา
6. อินเทอร์เน็ตช้าผิดปกติ / เข้าเว็บไซต์ไม่ได้

เมื่อถูกโจมตี! ขั้นตอนการรับมือเบื้องต้น – Act Immediately

1. ตั้งสติ! อย่าตื่นตระหนก

- การตัดสินใจผิดพลาดในช่วงเวลาฉุกเฉิน อาจทำให้สถานการณ์แย่ลง

2. แจ้งผู้เกี่ยวข้องภายในองค์กรทันที!

- หัวหน้างาน, ฝ่าย IT / ผู้ดูแลระบบ (ตามช่องทางที่กำหนด)
- **ไม่ควรพยายามแก้ไขด้วยตนเอง หากไม่เชี่ยวชาญ**

เมื่อถูกโจมตี! ขั้นตอนการรับมือเบื้องต้น – Isolate & Preserve

3. แยกอุปกรณ์ออกจากเครือข่ายทันที!

- ถอดสาย LAN / ปิด Wi-Fi
- **เพื่อป้องกันการแพร่กระจายของมัลแวร์**

4. อย่าปิดเครื่องทันที (แจ้ง IT ก่อน)

- เพื่อรักษาหลักฐานทางดิจิทัล

5. เก็บหลักฐานเบื้องต้น:

- จับภาพหน้าจอ (Screenshot)
- จดบันทึกเหตุการณ์ (วัน–เวลา, อาการที่พบ)

เมื่อถูกโจมตี! ขั้นตอนการรับมือเบื้องต้น – Action & Recovery

6. เปลี่ยนรหัสผ่านที่สำคัญทั้งหมด

- ทำจากอุปกรณ์ที่ "แน่ใจว่าปลอดภัย" (เครื่องอื่น/โทรศัพท์)
- บัญชีที่เกี่ยวข้องโดยตรง และบัญชีที่ใช้รหัสผ่านเดียวกัน

7. เตรียมพร้อมสำหรับการกู้คืนข้อมูล

- หากมี Backup ที่ดี จะสามารถกู้คืนได้

8. ตรวจสอบความเสียหาย:

- ประเมินว่าข้อมูลใดบ้างที่ได้รับผลกระทบ

การรายงานเหตุการณ์: ช่องทางภายในองค์กร

- **ทำไมต้องรายงาน?**
  - เพื่อให้ผู้เชี่ยวชาญเข้ามาจัดการ
  - ป้องกันการแพร่กระจายของภัย
  - รวบรวมข้อมูลเพื่อป้องกันในอนาคต
- **ใครคือผู้รับผิดชอบ?**
  - ผู้บังคับบัญชาโดยตรง
  - ฝ่าย IT / ผู้ดูแลระบบ / บุคลากรด้านความมั่นคงปลอดภัย
- **ช่องทาง:**
  - โทรศัพท์, อีเมล, ระบบแจ้งเหตุภายใน (ถ้ามี)

การรายงานเหตุการณ์: ช่องทางภายนอกองค์กร (หากจำเป็น)

1. **ThaiCERT (ไทยเซิร์ต):** www.thaicert.or.th, โทร 1212
   ให้คำปรึกษาทางเทคนิค, รวบรวมสถิติภัยคุกคาม

ThaiCERT
Thailand Computer Emergency Response Team
By NCSA Thailand

2. **สกมช. (NCSA):** www.ncsa.or.th
   กรณีภัยคุกคามระดับร้ายแรง/ระดับชาติ

NCSA สกมช

3. **ตำรวจ (บก.ปอท.):** www.tcsd.go.th
   เมื่อต้องการดำเนินคดีตามกฎหมาย

TCSD POLICE

4. **ธนาคาร / สถาบันการเงิน:**
   หากเกี่ยวข้องกับการโจรกรรมข้อมูลทางการเงิน

สมาคมธนาคารไทย
THE THAI BANKERS' ASSOCIATION


5 พฤติกรรมเสี่ยงที่ทำให้ตกเป็นเหยื่อของอาชญากรไซเบอร์

1. รหัสผ่านคาดเดาง่าย

- **รหัสผ่านที่เดาง่าย:** Common Passwords เช่น "123456", "password" วันเกิด ชื่อ เบอร์โทรศัพท์
- **ใช้รหัสผ่านเดียวกันทุกบัญชีหรือทุกแอปพลิเคชัน**

ผลกระทบ:

- เพิ่มโอกาสถูกโจมตีแบบ Brute Force

คำแนะนำ:

- ควรตั้งรหัสผ่านไม่ต่ำกว่า 8–12 ตัวอักษร ประกอบด้วย ตัวอักษรพิมพ์ใหญ่ ตัวอักษรพิมพ์เล็ก ตัวเลข และอักขระพิเศษ

Examples of Common Passwords:

- password
- col123456
- 123456789
- guest
- qwerty
- 111111
- 12345
- 123123
- admin

Time it takes a hacker to brute force your password in 2025

Hardware: 12 x RTX 5090 | Password hash: bcrypt (10)

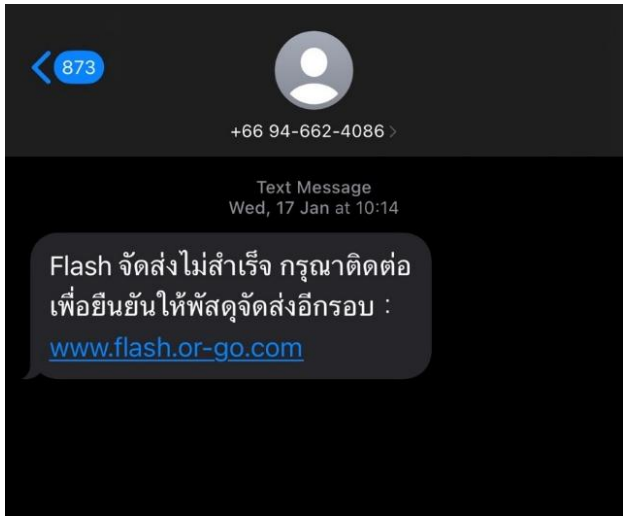
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	57 minutes	2 hours	4 hours
6	Instantly	46 minutes	2 days	6 days	2 weeks
7	Instantly	20 hours	4 months	1 year	2 years
8	Instantly	3 weeks	15 years	62 years	164 years
9	2 hours	2 years	791 years	3k years	11k years
10	1 day	40 years	41k years	238k years	803k years
11	1 weeks	1k years	2m years	14m years	56m years
12	3 months	27k years	111m years	917m years	3bn years
13	3 years	705k years	5bn years	56bn years	275bn years
14	28 years	18m years	300bn years	3tn years	19tn years
15	284 years	477m years	15tn years	218tn years	1qd years
16	2k years	12bn years	812tn years	13qd years	94qd years
17	28k years	322bn years	42qd years	840qd years	6qn years
18	284k years	8tn years	2qn years	52qn years	463qn years

Hive Systems

Read more and download at
hivesystems.com/password

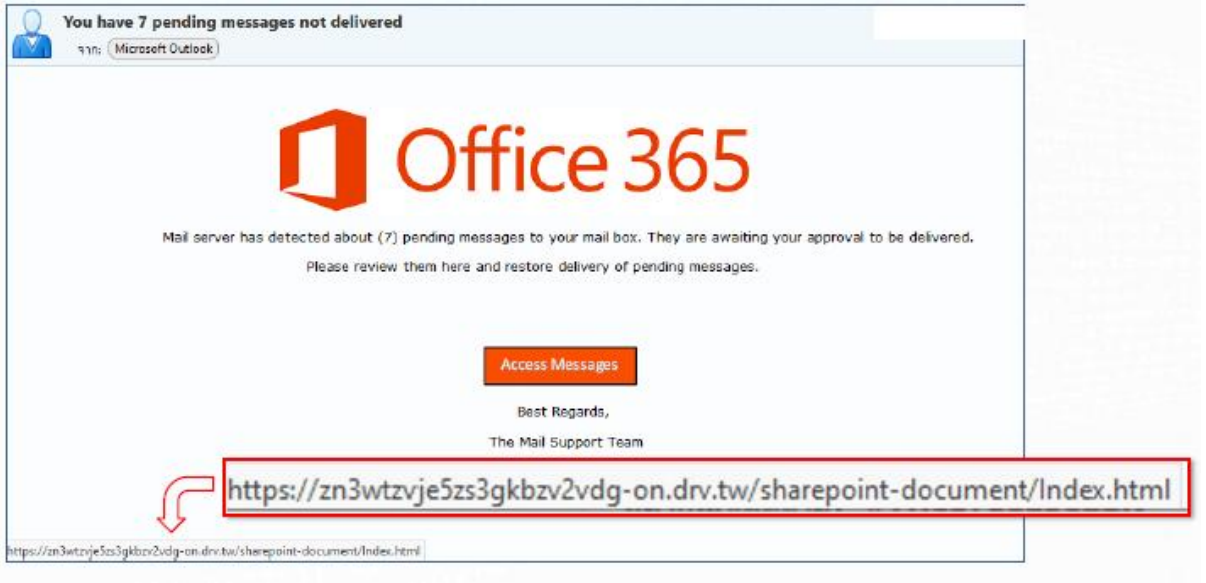
2. คลิกลิงก์แปลกปลอม

- **คลิกลิงก์แปลกปลอม:** จากอีเมล, SMS, Chat ที่ไม่รู้จัก
- **เปิดไฟล์แนบที่ไม่คาดคิด:** โดยเฉพาะนามสกุล .exe, .zip, .js, .vbs



ผลกระทบ:

- ติดมัลแวร์ (แรนซัมแวร์)
- ถูกขโมยข้อมูล (กรอกบนเว็บปลอม)
- ถูกหลอกลวง (Phishing)



3. ใช้ซอฟต์แวร์เถื่อน/ไฟล์จากแหล่งไม่น่าเชื่อถือ

- **ดาวน์โหลดโปรแกรมเถื่อน (Crack Software)**
- **ดาวน์โหลดไฟล์จากเว็บไซต์ที่ไม่รู้จัก/น่าสงสัย**

ผลกระทบ:

มักแฝงมัลแวร์มาด้วย (ไวรัส, โทรจัน, สปายแวร์)

โปรแกรมทำงานผิดปกติ, ไม่เสถียร

เสี่ยงต่อการถูกดำเนินคดีละเมิดลิขสิทธิ์

4. เปิดเผยข้อมูลส่วนบุคคลมากเกินไป

- **แชร์ข้อมูลละเอียดอ่อนบนโซเชียลมีเดีย เช่น วันเกิด ที่อยู่ เบอร์โทรศัพท์ ข้อมูลการเดินทาง กิจกรรมประจำวัน**

ผลกระทบ:

เสี่ยงต่อการถูกขโมยอัตลักษณ์ (Identity Theft)

ถูกใช้ในการหลอกลวงแบบวิศวกรรมสังคม (หาข้อมูล Pretexting)

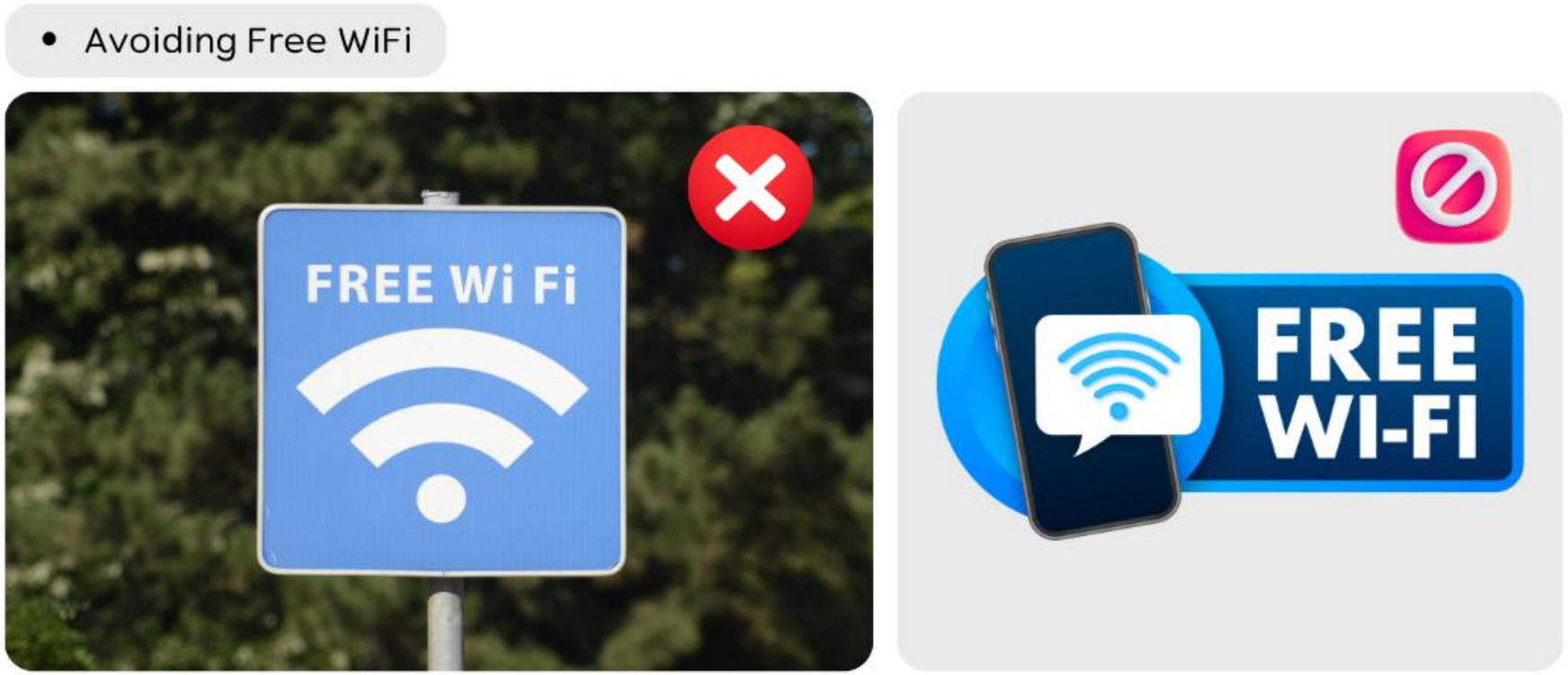
ข้อมูลส่วนตัวรั่วไหลสู่สาธารณะ

5. เชื่อมต่อ Wi-Fi สาธารณะ

- **ความเสี่ยงหลัก:** การโจมตีแบบ Man-in-the-Middle (MitM)
- **หลีกเลี่ยงการทำธุรกรรมสำคัญ:**
  - ธุรกรรมการเงิน, การเข้าสู่ระบบอีเมล/ระบบงานองค์กร

คำแนะนำ:

- ใช้ Wi-Fi ที่เชื่อถือได้ (มีรหัสผ่าน)
- พิจารณาใช้ VPN (Virtual Private Network)
- ใช้ Mobile Data แทน



กฎหมายและมาตรฐานสากลด้านเทคโนโลยีสารสนเทศ

องค์ประกอบสำคัญ

Policy & Procedures 01

กำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

Risk Management 02

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

Cybersecurity Incident Response Plan 03

มีแผนหรือกระบวนการรับมือภัยคุกคามไซเบอร์

nt CYFENCE Securing your Business

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

Critical Information Infrastructure : CII

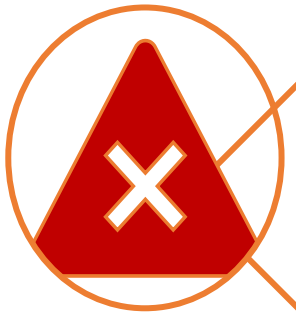
วัตถุประสงค์ของ พ.ร.บ. ไซเบอร์

- เพื่อเตรียมพร้อมด้านความปลอดภัยทางไซเบอร์
- เพื่อทดสอบการตอบสนองเหตุการณ์
- เพื่อพัฒนาทักษะของทีมรักษาความปลอดภัยทางไซเบอร์
- เพื่อตระหนักรู้และการฝึกอบรม
- เพื่อเชื่อมโยงการประสานงานและการสื่อสารให้ราบรื่น
- เพื่อช่วยในการประเมินความเสี่ยง
- เพื่อหาสิ่งที่ต้องปรับปรุง
- เพื่อจัดแนวทางเพื่อตอบสนองต่อภาวะวิกฤติ


ม.54
ประเมินความเสี่ยง
อย่างน้อยปีละ 1 ครั้ง
ม.56
ร่วมทดสอบสถานะความ
พร้อมในการรับมือกับ
ภัยคุกคามทางไซเบอร์
ม.56
การเฝ้าระวัง
ภัยคุกคามทางไซเบอร์
PROCESS
การดำเนินการ
ม.52
แจ้งรายชื่อผู้บริหาร
และเจ้าหน้าที่
ปฏิบัติการ
ม.57
รายงานเหตุ
ภัยคุกคาม
ม.54
รายงานการประเมินความเสี่ยง
ด้านความมั่นคงปลอดภัย
ไซเบอร์
REPORT
รายงาน
CII
critical
information
infrastructure
PLAN
แผนปฏิบัติการ
ม.44(1)
แผนการตรวจสอบ
และประเมินความเสี่ยง
ม.44(2)
แผนการรับมือ
ภัยคุกคามทางไซเบอร์
nt CYFENCE
Securing your Business

ระดับความรุนแรงของภัยคุกคามไซเบอร์

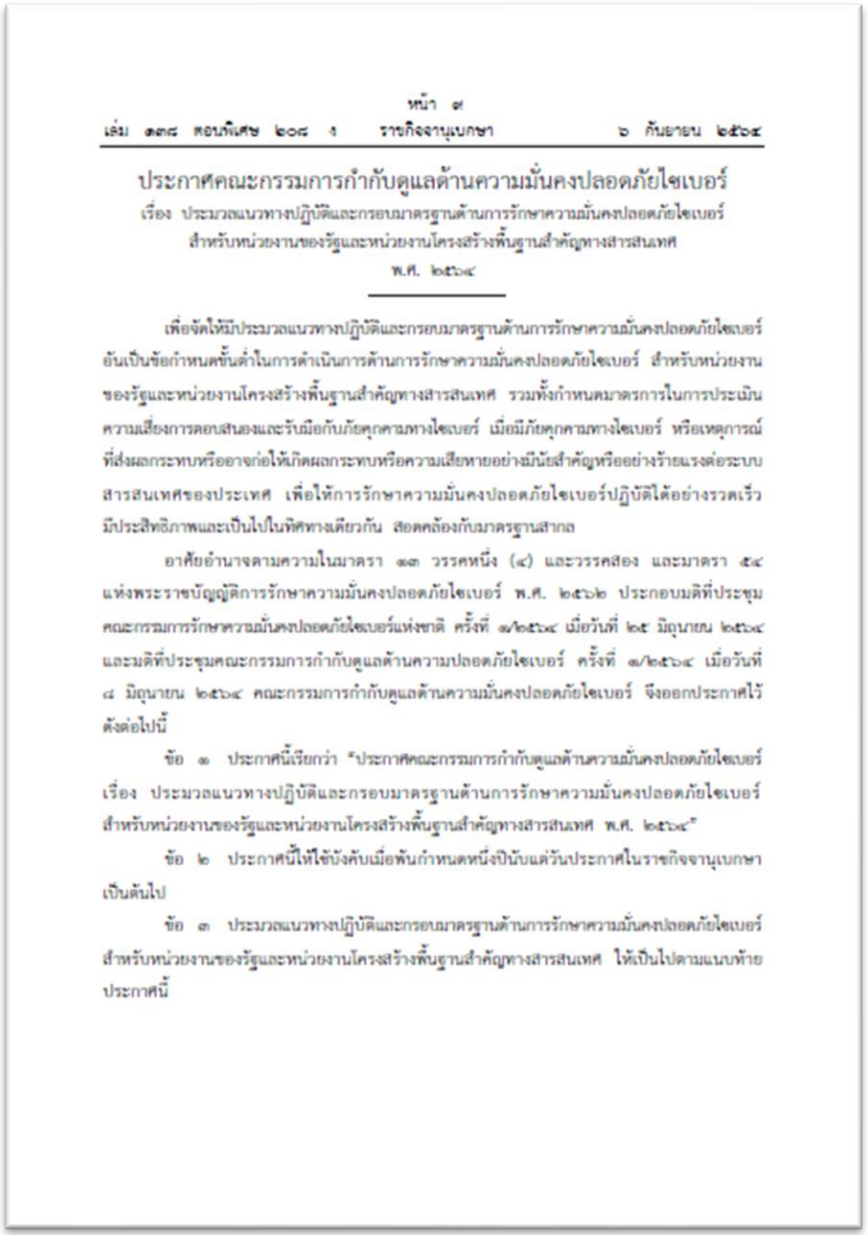
ภัยระดับไม่ร้ายแรง = มีความเสี่ยงอย่างมีนัยสำคัญทำให้ระบบ CII หรือการให้บริการของรัฐด้อยประสิทธิภาพลง



ภัยระดับร้ายแรง = มีความเสียหายต่อระบบ CII จนไม่สามารถทำงานหรือให้บริการได้ อาจมีผลต่อความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ ความปลอดภัยสาธารณะ และความสงบเรียบร้อยของประชาชน

ภัยระดับวิกฤต = การบริการล้มเหลวทั้งระบบ มีความเสี่ยงที่จะลุกลามไปยัง CII อื่นๆ อาจทำให้คนจำนวนมากเสียชีวิต ระบบถูกทำลายเป็นวงกว้างระดับประเทศ เป็นภัยต่อความมั่นคงของรัฐ เกิดภัยก่อการร้าย

ประกาศคณะกรรมการกำกับดูแล ด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้าง พื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔



หน้า ๙
เล่ม ๑๓๘ ตอนพิเศษ ๒๐๘ ง ราชกิจจานุเบกษา ๖ กันยายน ๒๕๖๔

ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
พ.ศ. ๒๕๖๔

เพื่อจัดให้มีประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยงการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพและเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล

อาศัยอำนาจตามความในมาตรา ๑๓ วรรคหนึ่ง (๔) และวรรคสอง และมาตรา ๕๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบมติที่ประชุมคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ ๑/๒๕๖๔ เมื่อวันที่ ๒๕ มิถุนายน ๒๕๖๔ และมติที่ประชุมคณะกรรมการกำกับดูแลด้านความปลอดภัยไซเบอร์ ครั้งที่ ๑/๒๕๖๔ เมื่อวันที่ ๔ มิถุนายน ๒๕๖๔ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

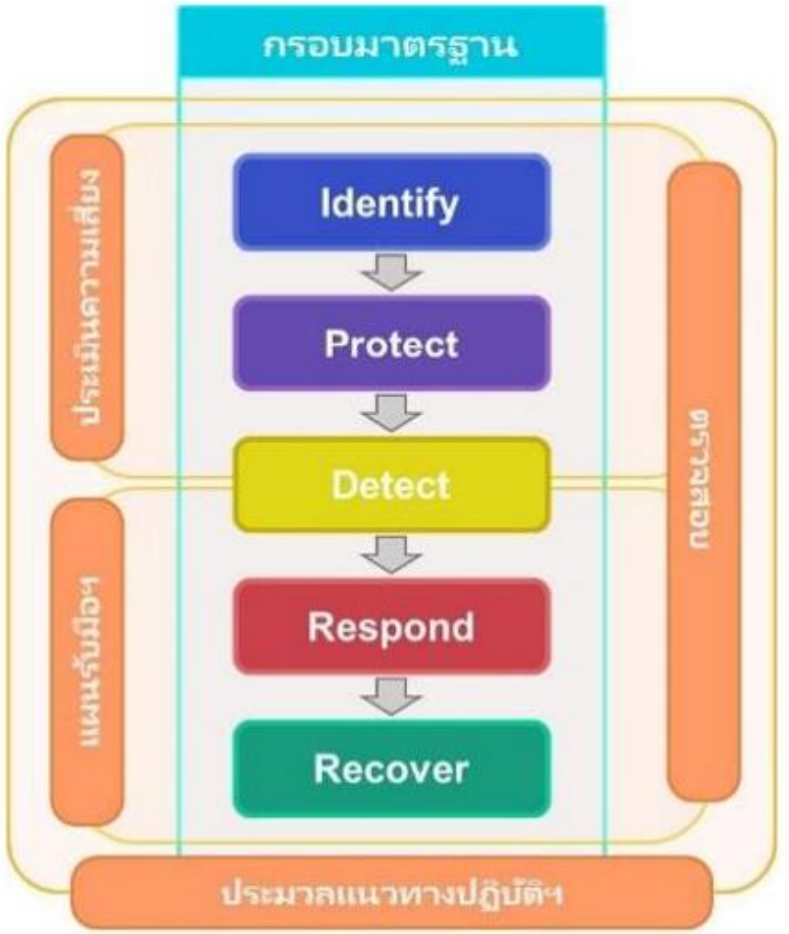
ข้อ ๓ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้เป็นไปตามแนบท้ายประกาศนี้

กรอบมาตรฐานและประมวลแนวทางปฏิบัติ

NIST Cybersecurity Framework

+

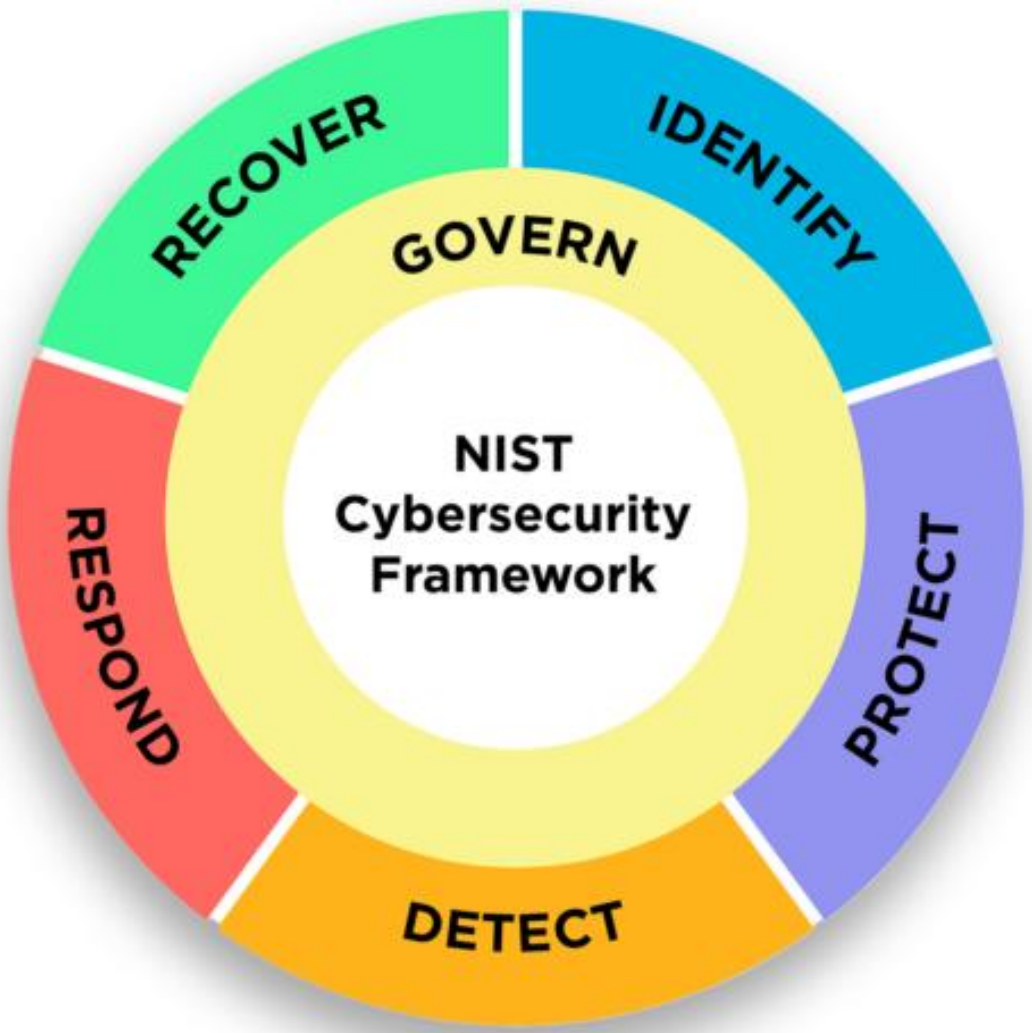
ISO/IEC 27001



NIST Cybersecurity Framework 2.0

CYFENCE
Securing your Business

NIST Cybersecurity Framework 2.0



Govern

Organization Context

Cybersecurity Supply Chain Risk management

Role & Responsibilities

Policies, Processes & Procedures

Risk Management Strategy

Oversight

CYFENCE
Securing your Business

Identify

- Asset Management
- Risk Assessment
- Improvement

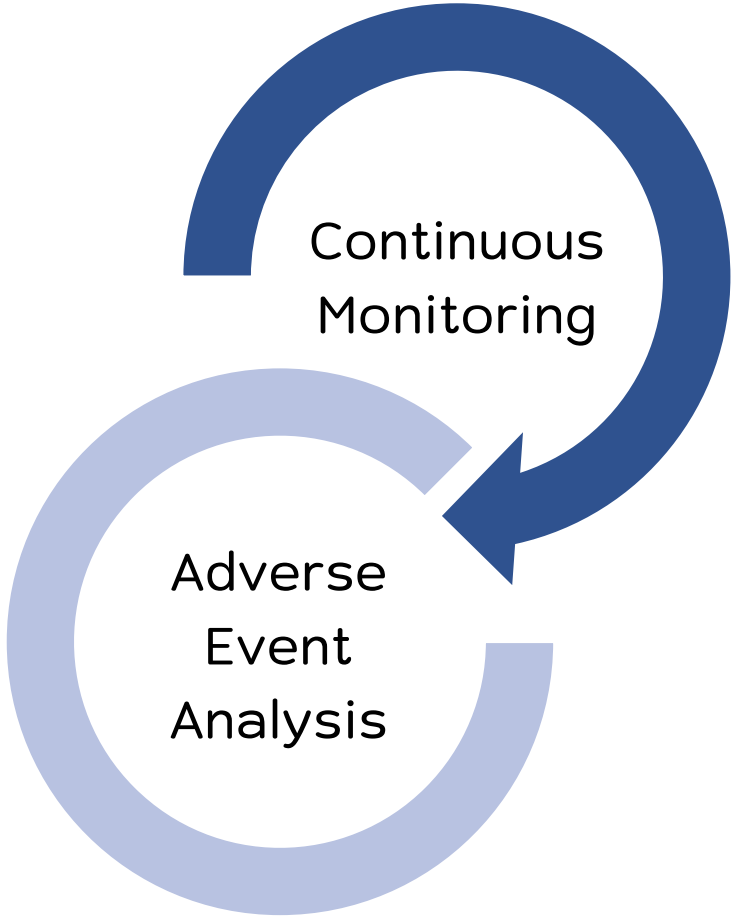
CYFENCE
Securing your Business

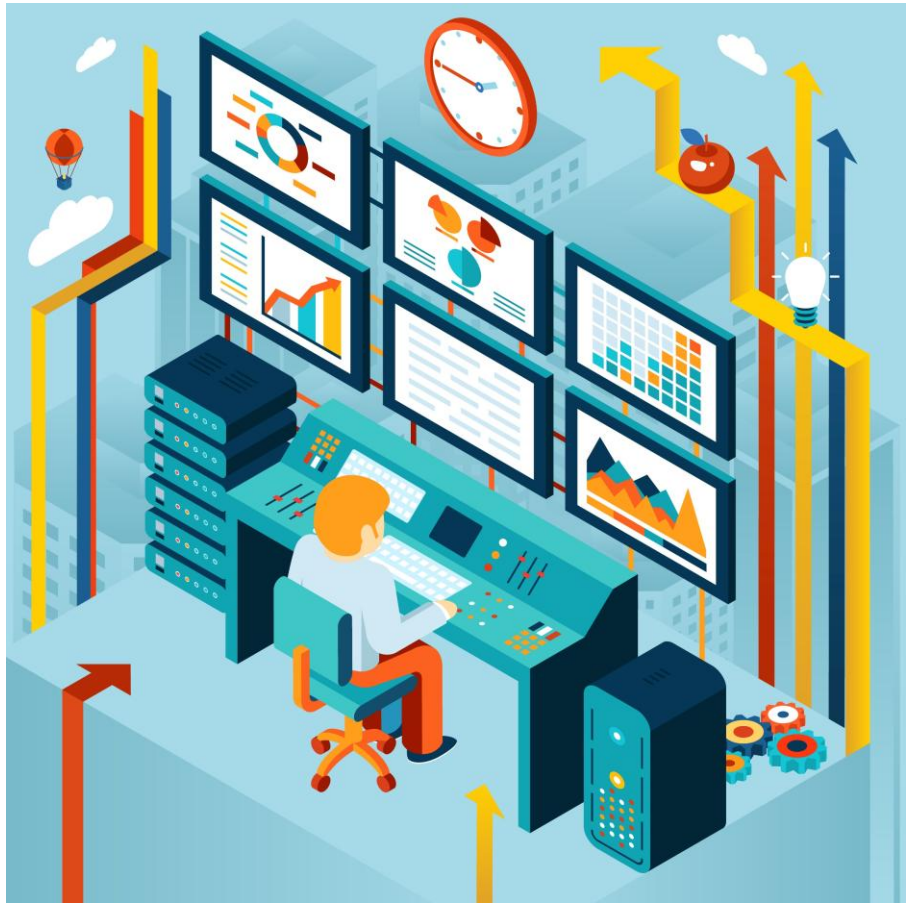
Protect

- Access Control
- Awareness & Training
- Data Security
- Platform Security
- Technology Infrastructure Resilience
- Protection Mechanism

nt CYFENCE
Securing your Business

Detect

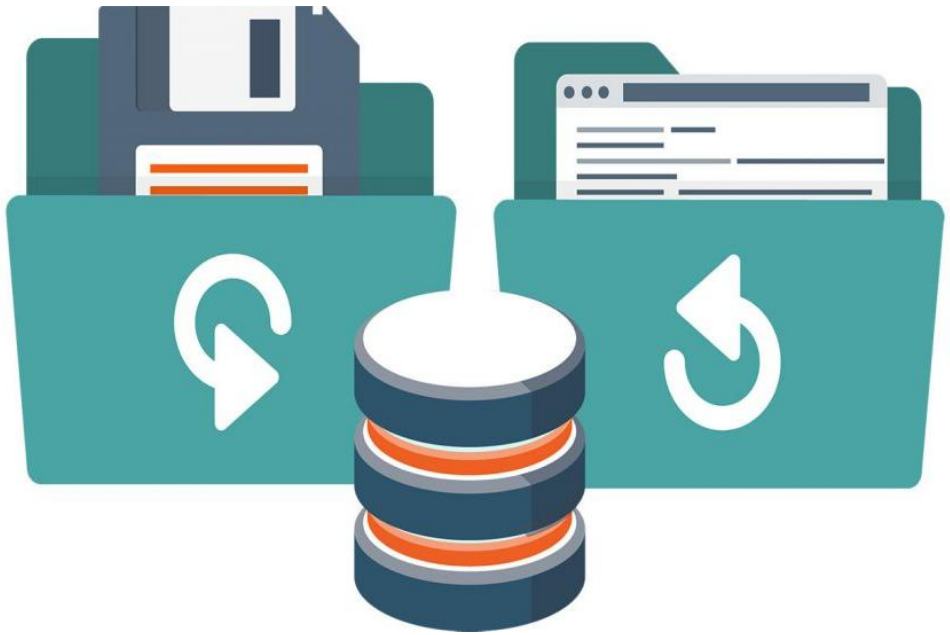




Respond

- Incident Management
- Incident Analysis
- Incident Response Reporting & Communication
- Incident Mitigation

Recover



Incident Recovery Plan Execution

Incident Recovery Communication

CYFENCE
Securing your Business

แบบประเมินความพึงพอใจ

THANK YOU