CYBERSECURITY TREND 2023

พลอากาศตรี อมร ชมเชย
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ประวัติวิทยากร

https://www.ncsa.or.th/

ตำแหน่งปัจจุบัน

- เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
- คณะที่ปรึกษาสภาความมั่นคงแห่งชาติ ด้านวิทยาศาสตร์ เทคโนโลยี และดิจิทัล

ประสบการณ์ทำงาน

- รองเลขาธิการ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
- ผู้อำนวยการกองปฏิบัติการไซเบอร์ ศูนย์ไซเบอร์กองทัพอากาศ
  Director of Cyber Warfare Division
  Department of Information and Communication Technology, Royal Thai Air Force
- Electronics Warfare Manager, F-16 MLU, Gripen
- คณะทำงาน Tactical Data Link (TDL) (F-16, Gripen)
- ริเริ่มการนำอินเทอร์เน็ตมาใช้งานใน ทอ.
- ริเริ่มการจัดแข่งทักษะทางไซเบอร์
- ร่างระเบียบการรักษาความปลอดภัยระบบสารสนเทศ ทอ. ปี 43
  ริเริ่มการตั้งหน่วยงานด้านไซเบอร์ ใน ทอ.

เกียรติคุณเพิ่มเติม

- บุคคลดีเด่นกองทัพอากาศปี 49, 62
- (ISC)² Government Professional Award 2021
- อาจารย์พิเศษ จุฬาลงกรณ์มหาวิทยาลัย
- วิทยากรรับเชิญงาน US-Thailand Cybersecurity Standards and Data Protection Workshop, OpenGov Insider

การศึกษา

- หลักสูตรผู้บริหารด้านความมั่นคงปลอดภัยไซเบอร์ (Executive Chief Information Security Officer: Executive CISO) รุ่นที่ 1
- หลักสูตรพัฒนาเครือข่ายและศักยภาพผู้บริหารระดับสูงของกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม WiNS รุ่นที่ 2
- เตรียมทหารรุ่นที่ 28
- วิทยาลัยการทัพอากาศ รุ่นที่ 51
- วท.บ. วิทยาการคอมพิวเตอร์
  United States Air Force Academy
- วท.ม. เทคโนโลยีสารสนเทศ มหาวิทยาลัยเกษตรศาสตร์
- นักเรียนนายเรืออากาศรุ่นที่ 35

CERTIFICATES

พลอากาศตรี อมร ชมเชย

เลขาธิการ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

รายงานเหตุการณ์ภัยคุกคามไซเบอร์ และผลการดำเนินการ ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

การโจมตีทางไซเบอร์หน่วยงานด้านสาธารณสุข

Ransomware หรือ มัลแวร์เรียกค่าไถ่ ชื่อที่หลายคนอาจจะเคยได้ยินมาบ้าง หรือแม้กระทั่งบางคนเคยโดนภัย Ransomware มากับตัวเอง โดยพฤติกรรมของ Ransomware มักจะทำการ Lock file หรือ encryption file เพื่อไม่ให้เหยื่อเข้าใช้งานไฟล์ที่ถูก Lock ไว้ได้ จากนั้นจะมีข้อความเพื่อทำการเรียกค่าไถ่ข้อมูลที่ได้ Lock ไว้ หากเหยื่อยินยอมจ่ายค่าไถ่แฮกเกอร์ก็จะปลดล็อคให้

Source : https://www.blockdit.com/posts/5f587dffc72e9f38d539f514

เช่น จากกรณีโรงพยาบาลสระบุรีถูกโจมตีด้วย Ransomware โดนเรียกค่าไถ่การเข้าถึงข้อมูลคนไข้เป็นเงิน 200,000 Bitcoin หรือถ้าคิดเป็นเงินไทย 63,000 ล้านบาท (Exchange rate ณ วันที่เกิดเหตุ) ทำให้การบริการของโรงพยาบาล ณ วันนั้นเกิดโกลาหล ไม่สามารถให้บริการคนไข้ได้ เนื่องจากไม่สามารถเข้าถึงข้อมูลคนไข้ได้ เช่น ประวัติการรักษา, ประวัติการใช้ยาเดิม และ ประวัติคนไข้ เป็นต้น

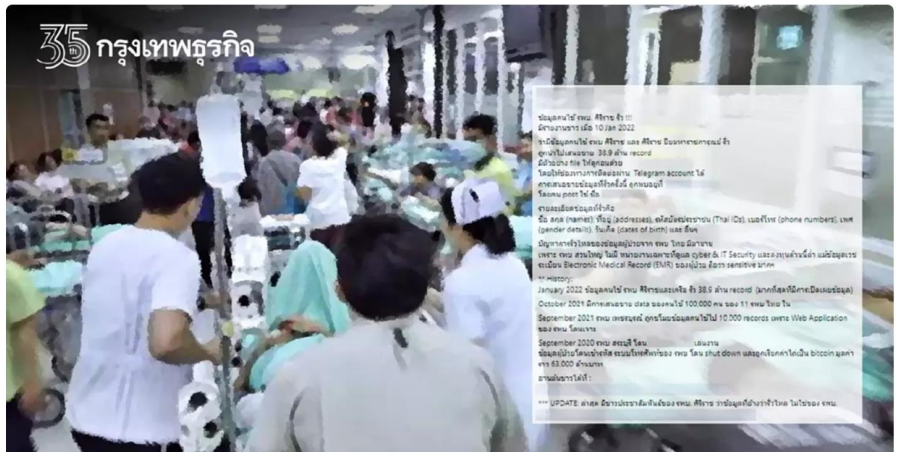
เหตุการณ์ข้อมูลรั่วไหล

OLVG กรณีศึกษาเหตุข้อมูลรั่วไหลของโรงพยาบาล

By ศุภวัชร์ มาลานนท์ | Tech, Law and Security | 11 พ.ย. 2564 เวลา 8:18 น. | 1.1k

ศิริราช แจงแล้ว! หลังแชร์ว่อน ข้อมูลผู้ป่วยกว่า 39 ล้านคน รั่วไหล - ขายตลาดมืด

10 มิ.ย. 2565 เวลา 18:52 น. | 7.6k



เหตุการณ์โจมตีทางไซเบอร์ในต่างประเทศ

BBC NEWS ไทย

หน้าแรก ประเทศไทย ต่างประเทศ วิทยาศาสตร์ สุขภาพ วิดีโอ ยอดนิยม

นาโตสอบสวนเหตุแฮกเกอร์ขายข้อมูลลับบริษัทผลิตขีปนาวุธ

27 สิงหาคม 2022

องค์การสนธิสัญญาแอตแลนติกเหนือ หรือ นาโต เปิดการสืบสวนสอบสวนเพื่อประเมินผลกระทบจากการละเมิดข้อมูลในเอกสารลับด้านการทหารที่แฮกเกอร์กลุ่มหนึ่งขโมยไปขายทางออนไลน์

แฮกเกอร์กลุ่มดังกล่าวได้ขโมยข้อมูลที่เชื่อมโยงกับบริษัทผู้ผลิตอาวุธรายใหญ่ในยุโรป โดยแฟ้มข้อมูลที่อาชญากรกลุ่มนี้นำออกขาย รวมถึงพิมพ์เขียวอาวุธของชาติพันธมิตรนาโตที่ใช้ในสงครามยูเครน

BBC NEWS ไทย

หน้าแรก ประเทศไทย ต่างประเทศ วิทยาศาสตร์ สุขภาพ วิดีโอ ยอดนิยม

Hydra: เปิดภารกิจปิดเว็บตลาดมืดรัสเซียของตำรวจในเยอรมนี

โจ ไทดี
ผู้สื่อข่าวไซเบอร์

7 เมษายน 2022

"มันทำให้พวกเราขนลุก" เซบาสเตียน สวีเบิล เล่าความรู้สึกตอนที่ทีมงานของเขาสามารถปิด "ไฮดรา" (Hydra) เว็บตลาดมืดที่ใหญ่ที่สุดในโลกได้สำเร็จ

ที่มา : https://www.bbc.com/thai

https://www.infoquest.co.th/2022/187117

infoquest

โควิด-19 ข่าวเศรษฐกิจ ข่าวหุ้น ข่าวต่างประเทศ ข่าวธุรกิจ ข่าวทั่วไป

ผู้เชี่ยวชาญเตือนรัสเซียจ่อโจมตีไซเบอร์ต่อโครงสร้างพื้นฐานน้ำมันและก๊าซ

https://www.foxnews.com/tech/cyber-attack-major-hospital-system-could-affect-20-million-americans

CYBERCRIME · **Published** November 16, 2022 1:44pm EST

Cyber attack on major hospital system could affect 20 million Americans

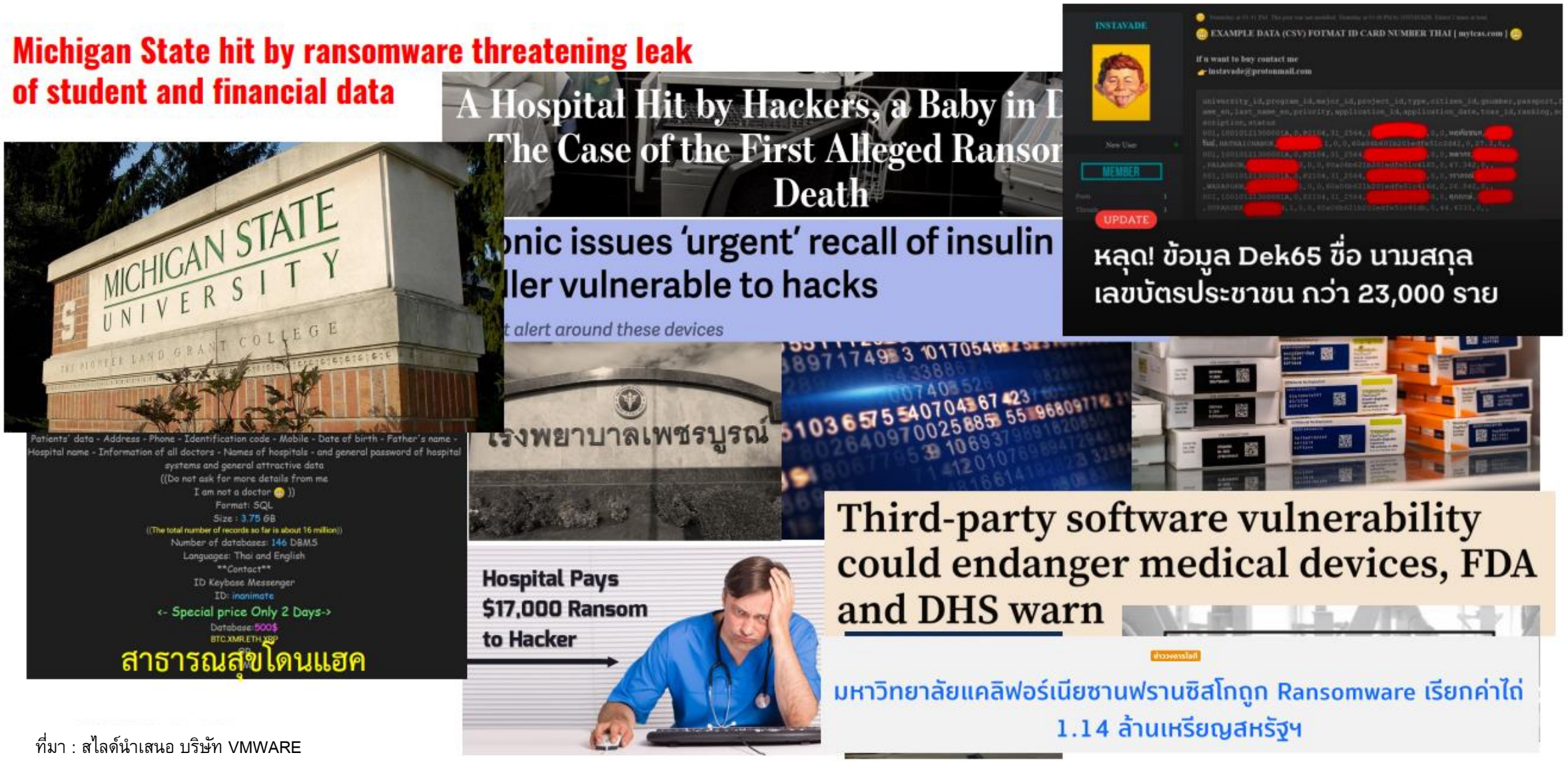
https://www.foxnews.com/politics/fbi-charges-three-iranians-cyber-attacks-targeting-local-us-governments-power-companies

FBI · **Published** September 14, 2022 12:00pm EDT

FBI charges three Iranians in cyber attacks targeting local US governments, power companies

ที่มา : https://www.foxnews.com/tech/cyber-attack...

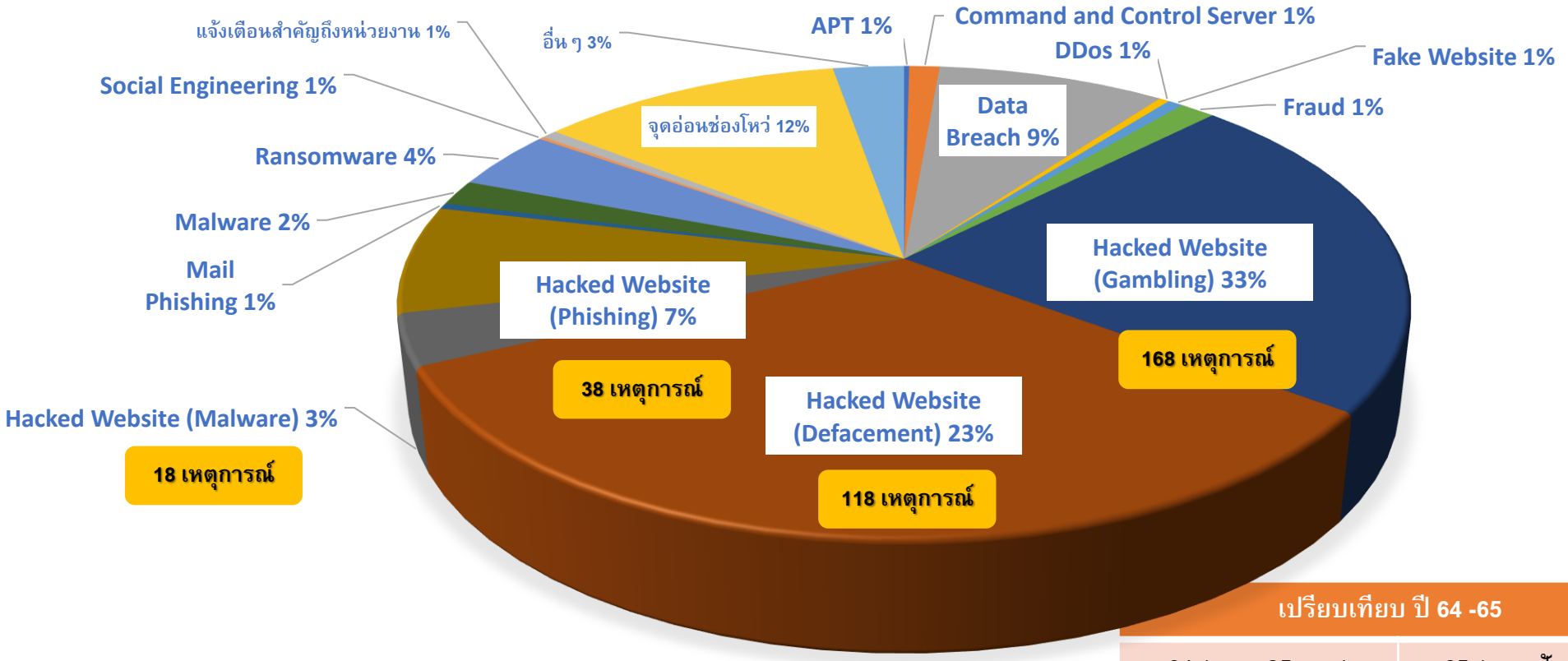
เหตุการณ์โจมตีทางไซเบอร์ต่าง ๆ



ที่มา : สไลด์นำเสนอ บริษัท VMWARE

สถิติการปฏิบัติในการรับมือกับภัยคุกคามทางไซเบอร์

วันที่ 1 ตุลาคม 2564 – 25 กันยายน 2565

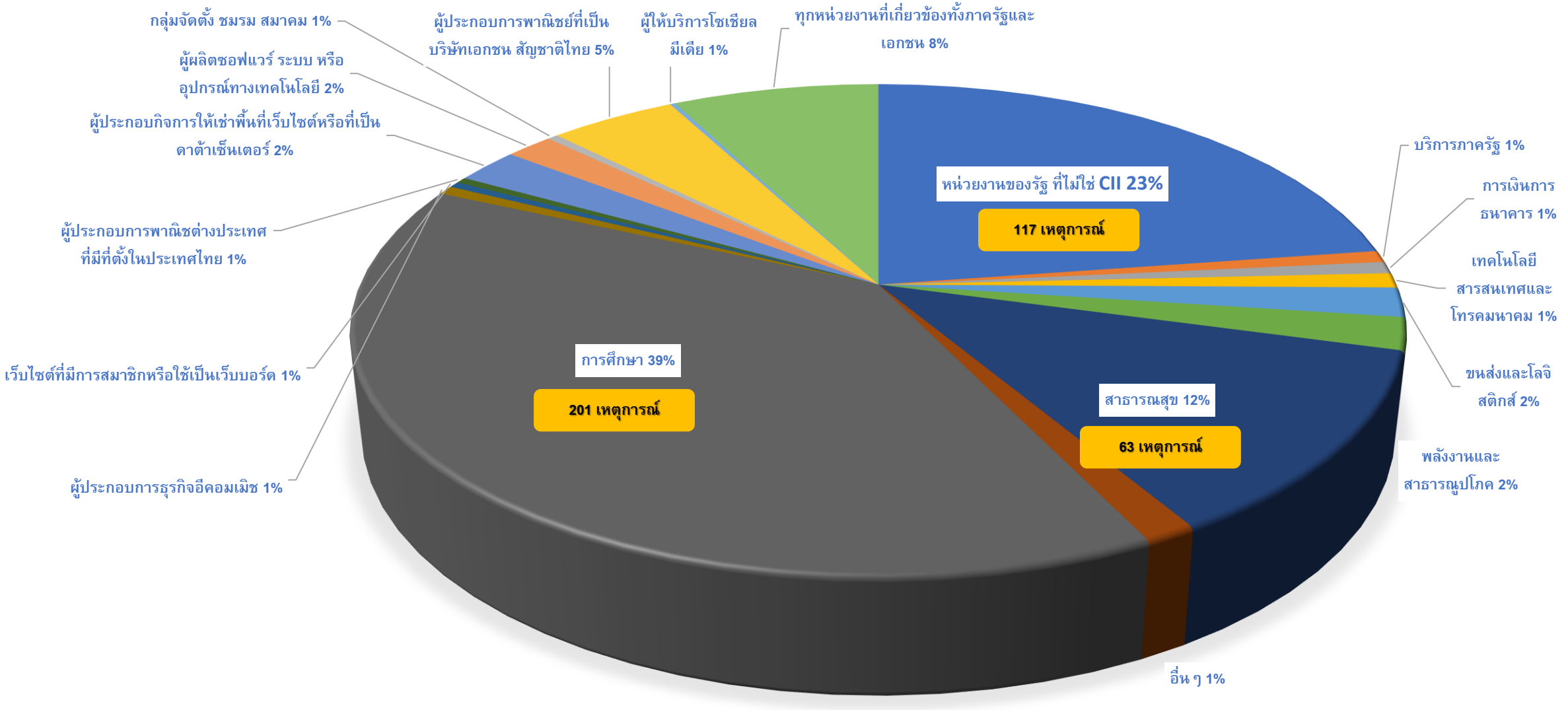


เปรียบเทียบ ปี 64 -65		64 ทั้งปี
64 (ม.ค.- 25 ก.ย.)	65 (ม.ค.-ปัจจุบัน)	ม.ค.-ธ.ค.
74 →	455	135

สรุปสถิติภัยคุกคามทางไซเบอร์ รวมทั้งสิ้น 516 เหตุการณ์

- Hacked Website (Phishing, Defacement, Gambling, Malware) 342 เหตุการณ์
- จุดอ่อนช่องโหว่ 60 เหตุการณ์
- Data Breach 45 เหตุการณ์
- ประเภทอื่น ๆ 69 เหตุการณ์

ประเภทหน่วยงานที่ถูกโจมตี แยกตามภารกิจหรือบริการ



เตือนภัย !!! เว็บรัฐปลอมหรือเลียนแบบ

NCSA สกมช

ในปัจจุบันพบเว็บไซต์หน่วยงานของรัฐถูกปลอมเป็นจำนวนมากโดยผู้ไม่ประสงค์ดี

เว็บปลอมจะมีเนื้อหารูปแบบเหมือนกับเว็บไซต์จริง ทำให้เหยื่อหรือผู้เข้าถึงเว็บไซต์หลงเชื่อว่าเป็นเว็บไซต์จริงของหน่วยงาน โดยแก๊งคอลเซ็นเตอร์ อาจหลอกให้ไปเว็บไซต์เพื่อดาวน์โหลดมัลแวร์ที่เป็นอันตราย สุดท้ายอาจทำให้เงินหมดบัญชี

rd-go-th.com เป็น URL ปลอม

NCSA Thailand www.ncsa.or.th saraban@ncsa.or.th

ตัวอย่าง อันตราย !!! จากเว็บไซต์ปลอมหรือเว็บไซต์เลียนแบบ

NCSA สกมช

เว็บไซต์ปลอม DSI

คนร้ายได้ทำเว็บไซต์ปลอม DSI

อันตราย !!! ไฟล์อันตรายที่ให้ดาวน์โหลดอยู่หน้าเว็บไซต์ปลอม DSI ในรูปแบบ .APK (android) ที่อาจจะโจรกรรมข้อมูลหรือควบคุมเครื่องโทรศัพท์ของผู้ที่ดาวน์โหลดไฟล์นั้นไปใช้กับโทรศัพท์ได้ของคุณได้

เว็บไซต์ปลอมศาลอาญากรุงเทพใต้

คนร้ายได้ทำหน้าเว็บไซต์ปลอมศาลอาญากรุงเทพใต้

อันตราย !!! อย่ากรอกข้อมูลส่วนตัว เช่น เลขบัตรประชาชน ชื่อ นามสกุล เลขหน้าบัตร รหัสผ่านธนาคาร และหมายเลขโทรศัพท์ ซึ่งคนร้ายได้สร้างเว็บไซต์ปลอมขึ้นมาเพื่อหลอกลวงข้อมูล ไปใช้ทำให้เกิดความเสียหายได้

เว็บไซต์ปลอมกรมสรรพากร

คนร้ายได้ทำเว็บไซต์ปลอมกรมสรรพากร

อันตราย !!!! ไฟล์อันตรายที่ให้ดาวน์โหลดอยู่หน้าเว็บไซต์ปลอมกรมสรรพากร ในรูปแบบ .APK (android) ที่อาจจะโจรกรรมข้อมูลหรือควบคุมเครื่องโทรศัพท์ของผู้ที่ดาวน์โหลดไฟล์นั้นไปใช้กับโทรศัพท์ได้ของคุณได้

NCSA Thailand www.ncsa.or.th saraban@ncsa.or.th

Top Strategic Technology Trends for 2022

Data Fabric

Cybersecurity Mesh

Privacy-Enhancing Computation

Cloud-Native Platforms

Composable Applications

Decision Intelligence

Hyperautomation

AI Engineering

Distributed Enterprise

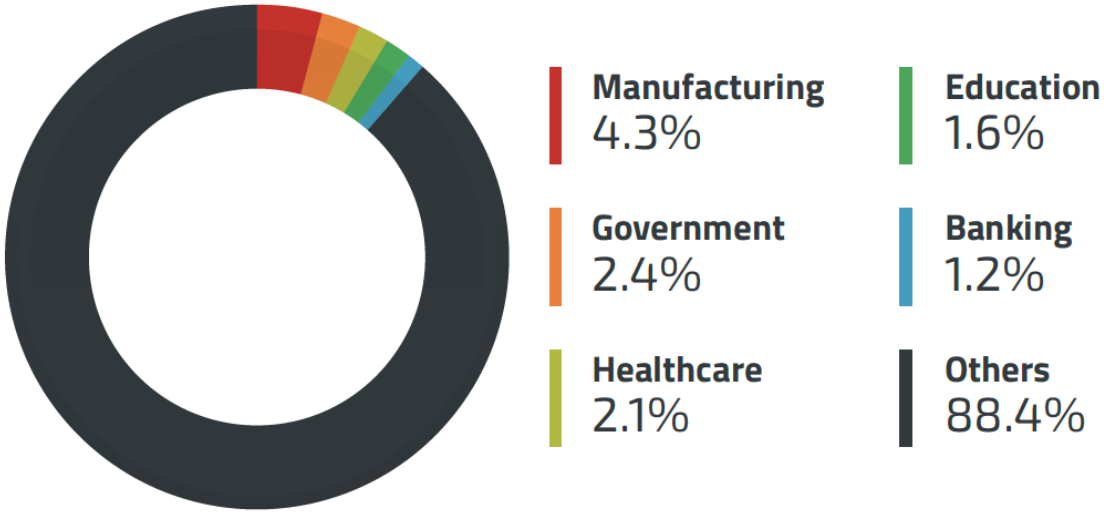
Total Experience

Autonomic Systems

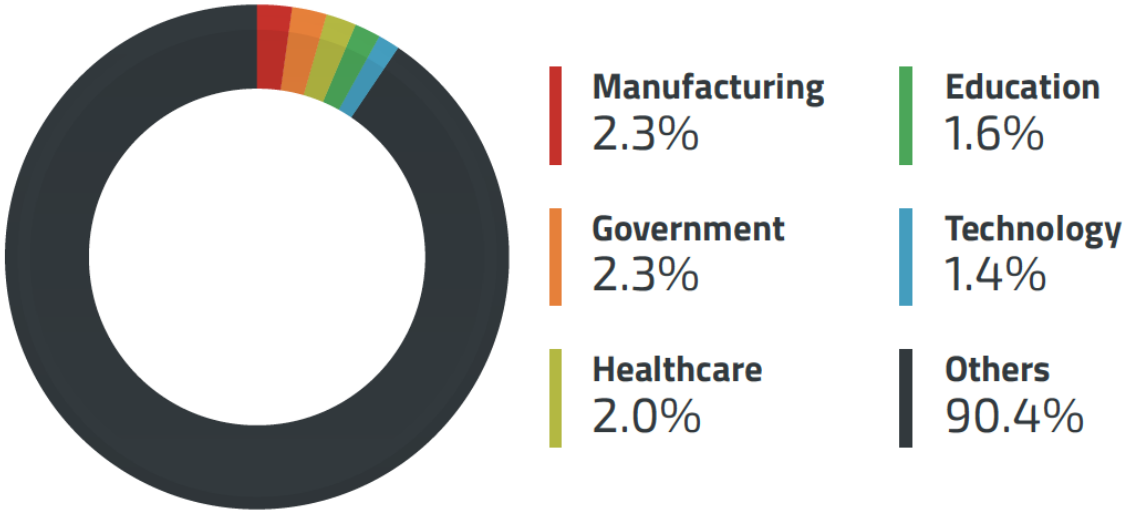
Generative AI

Gartner®

A comparison of the top 5 industries with the highest number of malware detections



1H 2021



1H 2022

Source: Trend Micro 2022 Cybersecurity Report

A Timeline of Global Risks 2022

Environmental Societal Technological Eco

% of respondents

Timeframe: 0–2 years

When Will These Major Global Threats Become a Serious Problem Worldwide?

Each year, the World Economic Forum releases its Global Risks Report, which highlights the top risks that pose a threat to the world in the next decade.

Global Risks Landscape 2021

WORLD ECONOMIC FORUM

Top Global Risks by Likelihood

Top Global Risks by Impact

Economic Environmental Geopolitical Societal Technological

Source: World Economic Forum Global Risks Report 2021

ONLINE THREAT

Internet attacks against small businesses

Country	Jan-April 2021	Jan-April 2022
Indonesia	615,491	2,063,711
Malaysia	99,221	225,025
Philippines	37,388	224,248
Singapore	25,061	206,727
Thailand	**152,848**	**317,347**
Vietnam	478,967	528,360

Source: Kaspersky

BANGKOK POST GRAPHICS

Top 10 Ransomware by Family – Thailand

Thailand (TH)	
Family	**Count**
WCRY	413
LOCKBIT	149
CONTI	89
BLACKCAT	47
STOPCRYPT	45
SODINOKIBI	32
GANDCRAB	31
MOUNTLOCKER	23
HIVE	15
EGREGOR	14
Others	1,052
Total	**1,910**

Source: Trend Micro 2022Smart Protection Network (SPN)

แนวโน้มสำคัญ 4 ประการที่ต้องระวังเพื่อให้องค์กรและบุคคลทั่วไปได้ติดตามภูมิทัศน์ภัยคุกคามทางอินเทอร์เน็ตที่เปลี่ยนแปลงไป

การโจมตีแรนซัมแวร์แบบกำหนดเป้าหมายลดลง

การโจมตีที่เน้นไปที่ประเทศกำลังพัฒนาที่มีความสามารถในการตรวจสอบทางไซเบอร์น้อย หรือประเทศที่ไม่ใช่พันธมิตรของสหรัฐ

การหลอกลวงและวิศวกรรมสังคมขั้นสูง

ผู้โจมตีมุ่งเน้นไปที่การโจมตีที่ไม่เน้นเทคโนโลยี และใช้ช่องโหว่ของมนุษย์แทน อย่างเช่นการหลอกลวงทุกประเภทผ่านเอสเอ็มเอส การโทรอัตโนมัติ แอพแมสเซ็นเจอร์ส่งข้อความยอดนิยม โซเชียลเน็ตเวิร์ค ฯลฯ

การละเมิดข้อมูลโดยผู้โจมตีที่ไม่ระบุชื่อมากขึ้น

การละเมิดข้อมูลในหลายกรณี ผู้ที่ตกเป็นเหยื่อไม่สามารถระบุตัวผู้โจมตี หรือค้นหาว่าตนเองถูกบุกรุกได้อย่างไร จากการวิจัยพบด้วยว่า สัดส่วนดังกล่าวเพิ่มขึ้นอย่างมีนัยสำคัญในช่วงสองปีที่ผ่านมาซึ่งสูงกว่า 75%

การโจมตีวงการเงินคริปโตฯ และเอ็นเอฟที (NFT)

อุตสาหกรรม NFT ที่กำลังเติบโต จะตกเป็นเป้าหมายของอาชญากรไซเบอร์ "เราจะเห็นการโจรกรรมทรัพย์สินเอ็นเอฟทีมากขึ้นในอีกไม่กี่ปีข้างหน้า การโจมตีเหล่านี้ไม่เพียงส่งผลกระทบต่อตลาดสกุลเงินคริปโททั่วโลก แต่ยังรวมถึงราคาหุ้นของบริษัทแต่ละแห่ง ซึ่งผู้โจมตีจะสร้างผลกำไรผ่านการซื้อขายข้อมูลเชิงลึกที่ผิดกฎหมายในตลาดหุ้น"

ที่มา : https://www.bangkokbiznews.com/tech/982543

12 Cybersecurity Trends Every CISO Must Prepare for in 2023

12 Cybersecurity Trends Every CISO Must Prepare for in 2023

1. Account For the Impact of Ransomware Attacks
2. Rebuild Endpoints Using a Sophisticated EDR
3. Emphasize on Implementing Cybersecurity Best Practices
4. Invest in Employee Trainings To Ward Off Cyber Attacks
5. Zero-Trust Architecture's Importance Will Grow
6. Incorporate Policy-as-Code Into Cybersecurity Practices

https://www.spiceworks.com/it-security/cyber-risk-management/interviews/top-cybersecurity-trends-2023/

12 Cybersecurity Trends Every CISO Must Prepare for in 2023

7. Work Closely With Federal Agencies To Set Security Standards
8. Be Transparent About Cybersecurity Practices With Customers
9. Generative AI Adoption Will Grow in Popularity for Security Tools
10. Prioritize Cyber Resilience and Risk Reduction in 2023
11. New Regulations Will Introduce Mandatory Security Practices in IoT
12. Absence of a Cybersecurity Culture Will Pose a Serious Threat

https://www.spiceworks.com/it-security/cyber-risk-management/interviews/top-cybersecurity-trends-2023/

Gartner's 8 Cybersecurity Predictions for 2023-2025

Gartner's 8 Cybersecurity Predictions for 2023-2025

1. By the end of 2023, modern data privacy laws will cover the personal information of 75% of the world's population.

2. By 2024, organizations that adopt a cybersecurity network architecture will be able to reduce the financial costs of security incidents by an average of 90%.

3. By 2024, 30% of enterprises will deploy cloud-based Secure Web Gateway (SWG), Cloud Access Security Brokers (CASB), Zero Trust Network Access (ZTNA), and Firewall as a Service (FWaaS), sourced from the same vendor.

https://krontech.com/gartners-8-cybersecurity-predictions-for-2023-2025

Gartner's 8 Cybersecurity Predictions for 2023-2025

4. By 2025, 60% of organizations will use cybersecurity risk as the primary determinant in conducting third-party transactions and business relationships.

5. The percentage of states that enact laws regulating ransomware payments, fines and negotiations will increase from less than 1% in 2021 to 30% by the end of 2025.

6. By 2025, 40% of boards will have a dedicated cybersecurity committee overseen by a qualified board member.

https://krontech.com/gartners-8-cybersecurity-predictions-for-2023-2025

Gartner's 8 Cybersecurity Predictions for 2023-2025

7. By 2025, 70% of CEOs will build a culture of corporate resilience to protect themselves from threats from cybercrime, severe weather events, social events, and political instability.

8. By 2025, cyber-attackers will be able to use operational technology environments as weapons successfully enough to cause human casualties.

https://krontech.com/gartners-8-cybersecurity-predictions-for-2023-2025

นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ 2565-2570

“บริการที่สำคัญของประเทศไทยมีความมั่นคงปลอดภัยไซเบอร์ เพื่อความยั่งยืนทางเศรษฐกิจและสังคม”

ยุทธศาสตร์ที่ 1

สร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ (บุคลากร องค์ความรู้ และเทคโนโลยี)

เพื่อเสริมสร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ โดยบูรณาการ บุคลากร องค์ความรู้ และเทคโนโลยี นำไปสู่การพัฒนาผลิตภัณฑ์ ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมของประเทศ

- เพิ่มบุคลากรที่มีความสามารถด้านความมั่นคงปลอดภัยไซเบอร์
- สร้างความตระหนักรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์
- ส่งเสริมการวิจัยและพัฒนาและนวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์

ยุทธศาสตร์ที่ 2

บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้

เพื่อบูรณาการความร่วมมือในการเตรียมความพร้อมสำหรับการรับมือภัยคุกคามทางไซเบอร์ และการฟื้นคืนบริการที่สำคัญสู่สภาพปกติได้อย่างรวดเร็วกับทุกภาคส่วนทั้งภายในประเทศและระหว่างประเทศ

- ส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและภาคเอกชน
- ประสานความร่วมมือระหว่างประเทศเพื่อรับมือภัยคุกคาม

ยุทธศาสตร์ที่ 3

สร้างบริการภาครัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และฟื้นคืนสู่สภาพปกติได้

เพื่อส่งเสริมบริการภาครัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และสามารถฟื้นคืนบริการที่สำคัญสู่สภาพปกติได้

- กำหนดมาตรการการรักษาความมั่นคงปลอดภัยขั้นต่ำ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- กำหนดโครงสร้างการกำกับดูแลและกรอบกฎหมาย สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- ปกป้องระบบข้อมูลและเครือข่ายของหน่วยงานภาครัฐ

ยุทธศาสตร์ที่ 4

สร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน

มุ่งสร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน เพื่อให้การบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

- เพิ่มขีดความสามารถในการรับมือและตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
- ส่งเสริมและสนับสนุนการแบ่งปันข้อมูลภัยคุกคาม
- ส่งเสริมและสนับสนุนความมั่นคงปลอดภัยทางไซเบอร์ สร้างความเชื่อมั่นให้ทุกภาคส่วน

❖ **นโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์** ใช้หลักการตามแนวทางการปฏิบัติที่ดีที่ใช้กันแพร่หลายทั่วโลก รวมถึงประเทศไทย คือ หลักการกำกับดูแล การบริหารความเสี่ยง และการปฏิบัติตาม (Governance, Risk and Compliance: GRC) โดยประกอบด้วย 3 หัวข้อหลัก ดังนี้

1 : การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์
(Good Governance in Cyber Security)

- **จัดองค์กรให้มีการถ่วงดุล**
  (Three lines of defense)
- **ให้มีผู้รับผิดชอบงานบริหารความมั่นคงปลอดภัยไซเบอร์**
  - **หน่วยงานภาครัฐ** กำหนดให้มี head of info security
  - **หน่วยงาน CII** กำหนดให้มี CISO (Chief of Security Officer)

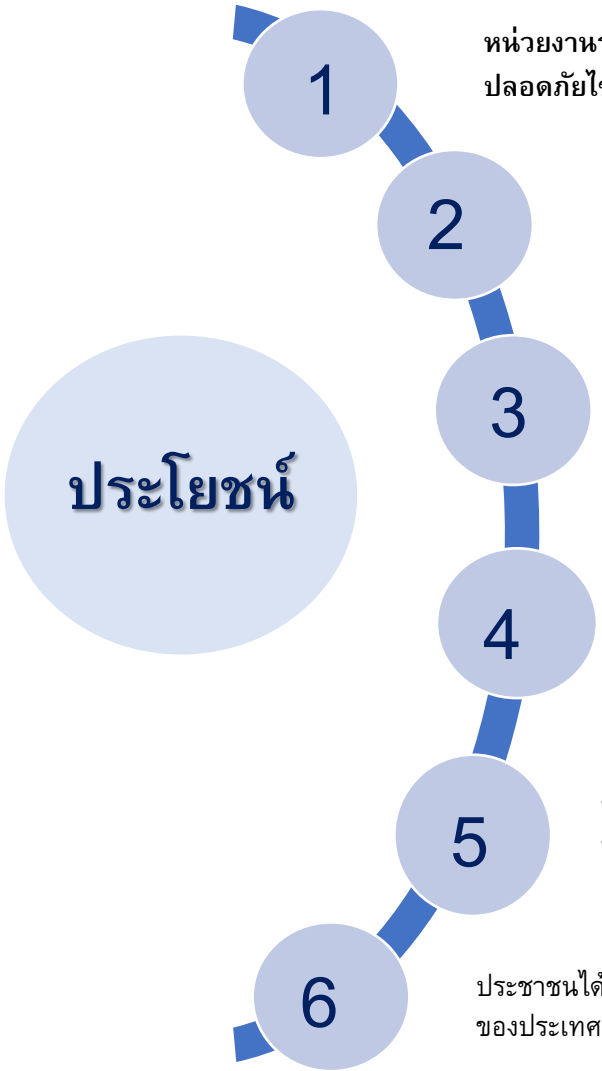
2 : การบริหารความเสี่ยง
(Risk Management)

- **มีกรอบบริหารความเสี่ยงเป็นลายลักษณ์อักษร**
  - เกณฑ์ประเมินความเสี่ยง
  - วิธีประเมินความเสี่ยง
  - เฝ้าระวังติดตามความเสี่ยง
- **ลงทะเบียนความเสี่ยง**
- **ติดตามความเสี่ยงอย่างสม่ำเสมอว่าอยู่ในเกณฑ์ที่ยอมรับได้**

3 : นโยบาย และแนวปฏิบัติ
(Policies and Guidelines)

- **กำหนด อนุมัตินโยบาย มาตรฐาน แนวทางจัดการความเสี่ยง และป้องกันภัยคุกคาม**
  - สอดคล้องประมวลปฏิบัติ
  - เผยแพร่แก่บุคลากรและบุคคลที่เข้าถึงบริการสำคัญ
- **ทบทวนนโยบาย แนวปฏิบัติอย่างน้อย ปีละหนึ่งครั้ง**

ประโยชน์ที่ประเทศชาติ และประชาชนจะได้รับ



1. **หน่วยงานระดับชาติ** มีศักยภาพและมาตรฐาน สามารถสร้างบริการภาครัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มี**ความมั่นคงปลอดภัยไซเบอร์** และฟื้นคืนสู่สภาพปกติได้ และสามารถบริหารจัดการการขับเคลื่อนยุทธศาสตร์ได้อย่างมีประสิทธิภาพ
2. มีการ**บูรณาการความร่วมมือทุกภาคส่วน** เพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์ และฟื้นคืนสู่สภาพปกติได้
3. หน่วยงานทุกภาคส่วน ทั้งรัฐ เอกชน และรัฐวิสาหกิจ มีการบูรณาการความร่วมมือ เพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์ ภายใต้โครงสร้างการกำกับดูแล และกรอบกฎหมายเพื่ออำนวยความสะดวกในการดำเนินการ การประสานความร่วมมือภายในประเทศและระหว่างประเทศเพื่อรับมือภัยคุกคาม พร้อมทั้งการฟื้นคืนบริการที่สำคัญสู่สภาพปกติอย่างรวดเร็ว
4. ทุกประชาชนและธุรกิจมีความตระหนักและทักษะด้านความมั่นคงปลอดภัยไซเบอร์ มีการดำเนินกิจกรรมทางไซเบอร์อย่างชาญฉลาด
5. ประเทศมีขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์แบบครบวงจร ทั้งคน (People) องค์ความรู้หรือกระบวนการ (Process) และเทคโนโลยี (Technology) แบบบูรณาการ
6. ประชาชนได้รับบริการภาครัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศที่มีความมั่นคงปลอดภัยไซเบอร์

Contact us

National Cyber Security Agency - NCSA

NCSA Thailand

Line ID : NCSA Thailand

E-Mail: saraban@ncsa.or.th

02-142-6885

shorturl.at/hkAC2