Cybersecurity Fundamentals and Threat Landscape

Surachet Suchaiya, PhD.
Director of
Cyber Innovation Promotion
Association of Technology (CIPAT)

15 August 2024, 2:00PM - 5:00PM

Colllege of Innovation Management, SSRU

MYSURACHET.COM

College of Innovation Management
Suan Sunandha Rajabhat University

MYSURACHET.COM

Surachet Suchaiya, PhD.

Educational history, work history
Expertise, experience
Training certificates received
and research.

Cybersecurity Fundamentals and Threat Landscape

Agenda

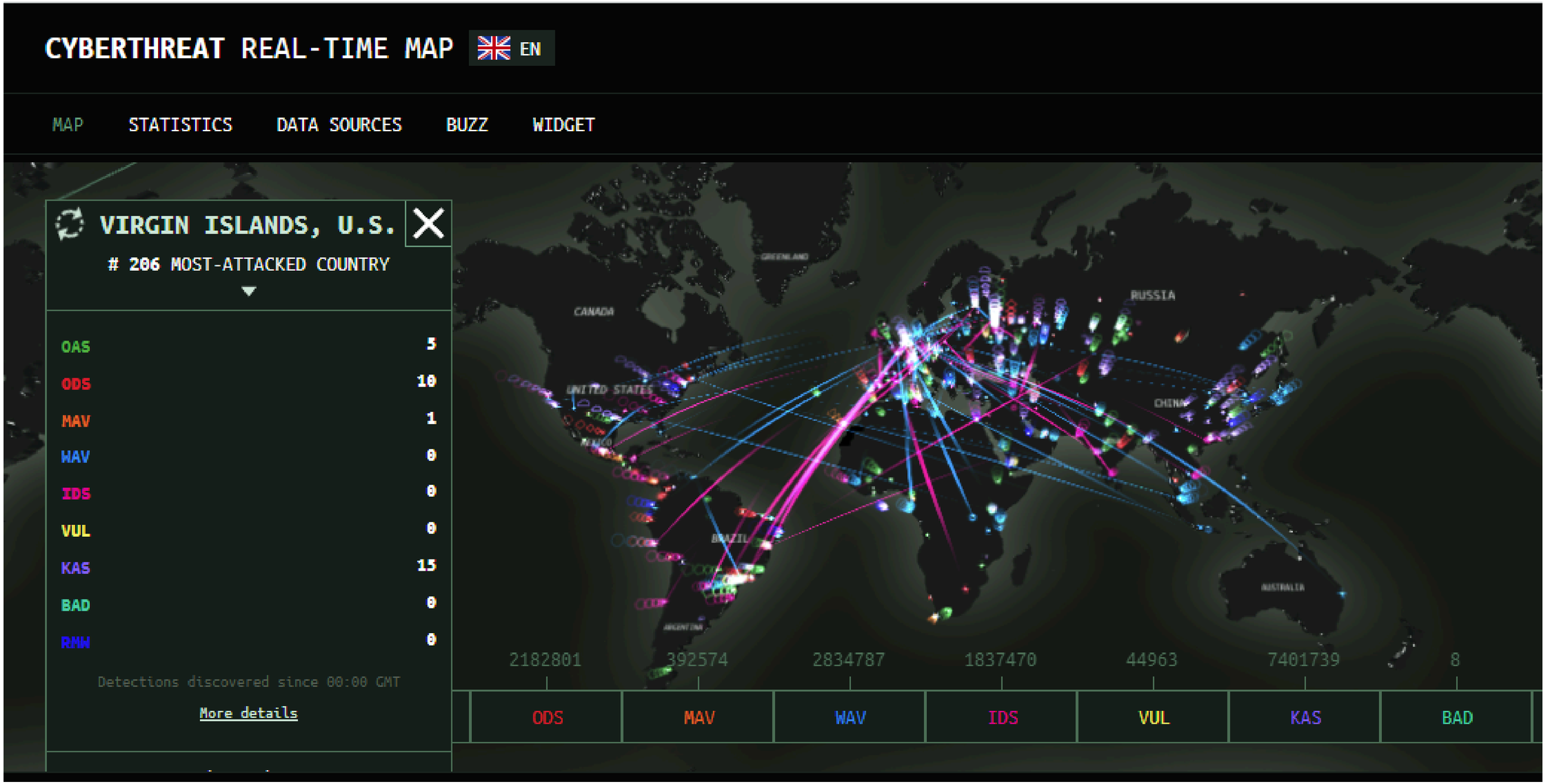
1. Cyber threats in the AI era
2. Threat landscape
3. Cyber Threat Case study that impact to the economy
4. สรุปและตอบคำถาม

innovation management
SUAN SUNANDHA RAJABHAT UNIVERSITY

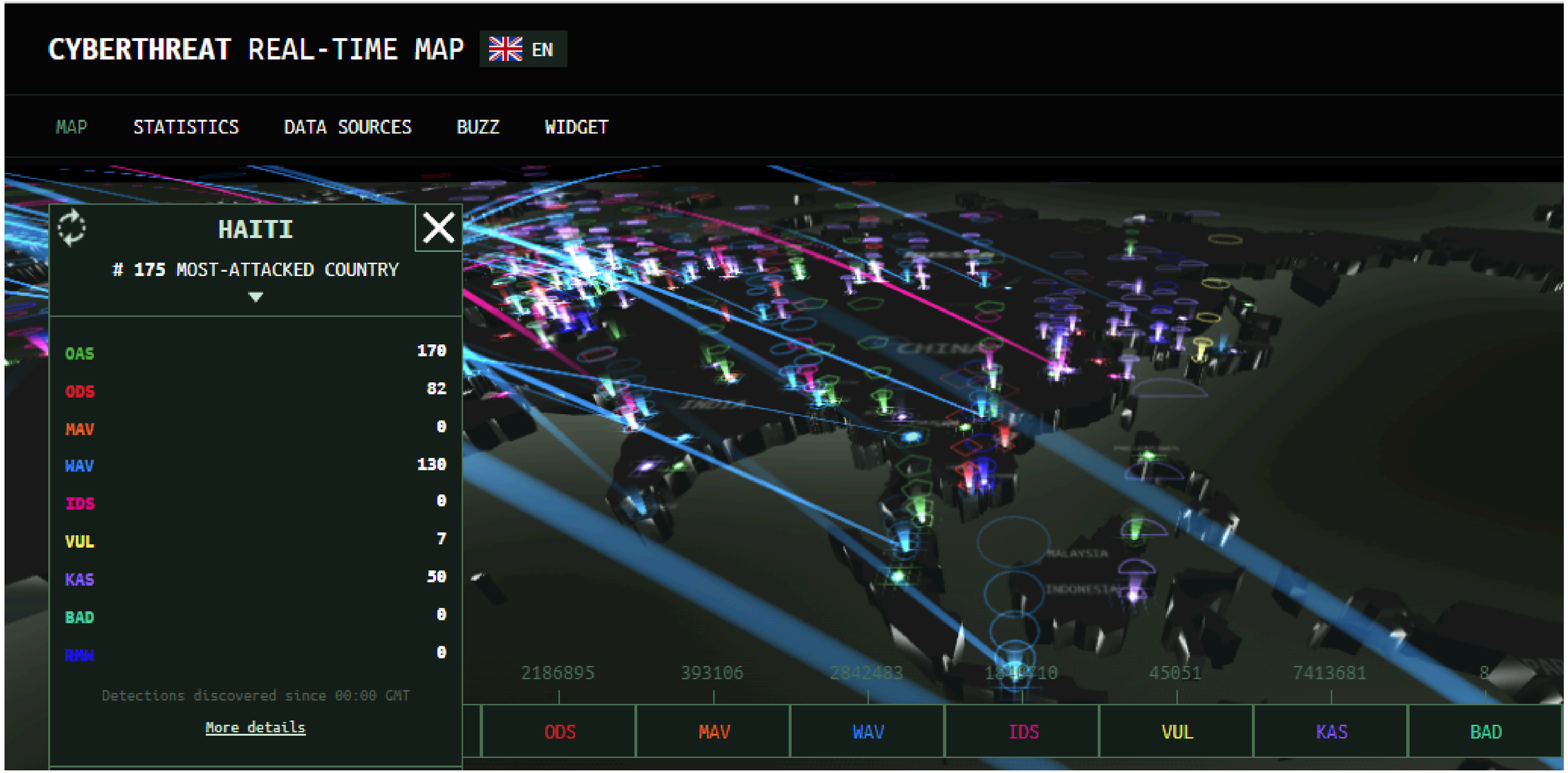
MYSURACHET.COM

1 Cyber threats in the AI era

1 Cyber threats in the AI era

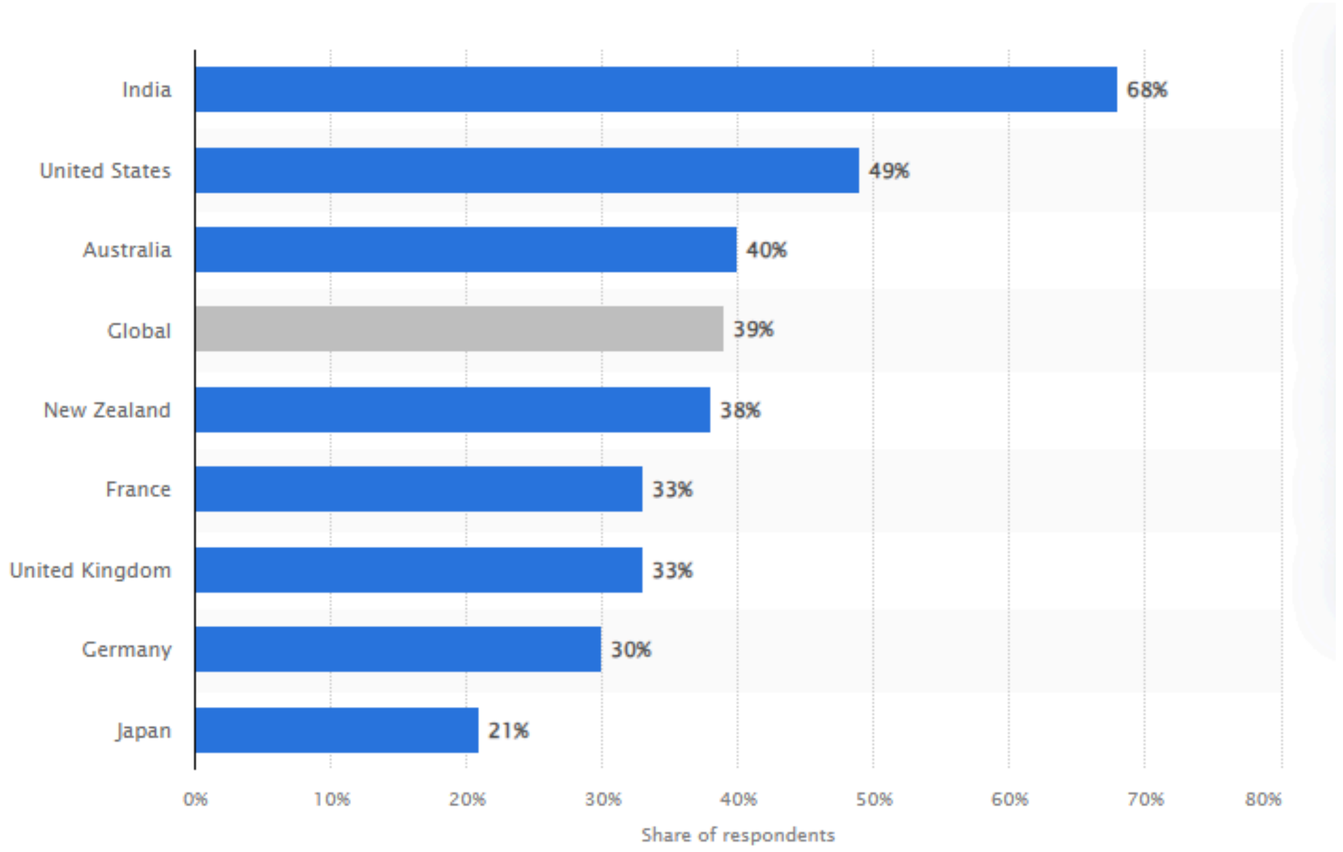


1 Cyber threats in the AI era



1 Cyber threats in the AI era : Economic Review

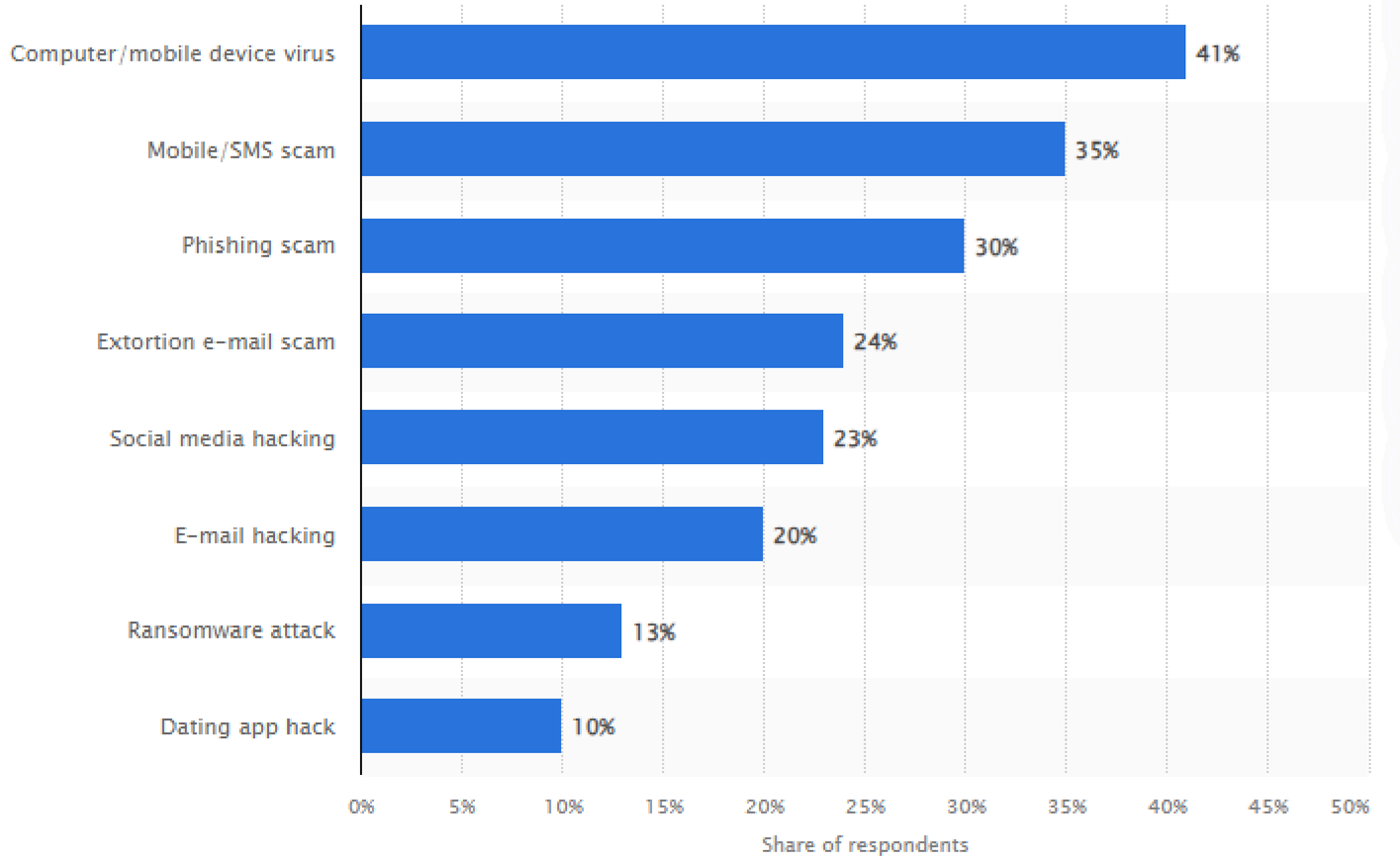
Percentage of internet users in selected countries who have ever experienced any cybercrime in 2022



ข้อมูลจาก https://www.statista.com/statistics/194133/cybercrime-rate-in-selected-countries/

1 Cyber threats in the AI era : Economic Review

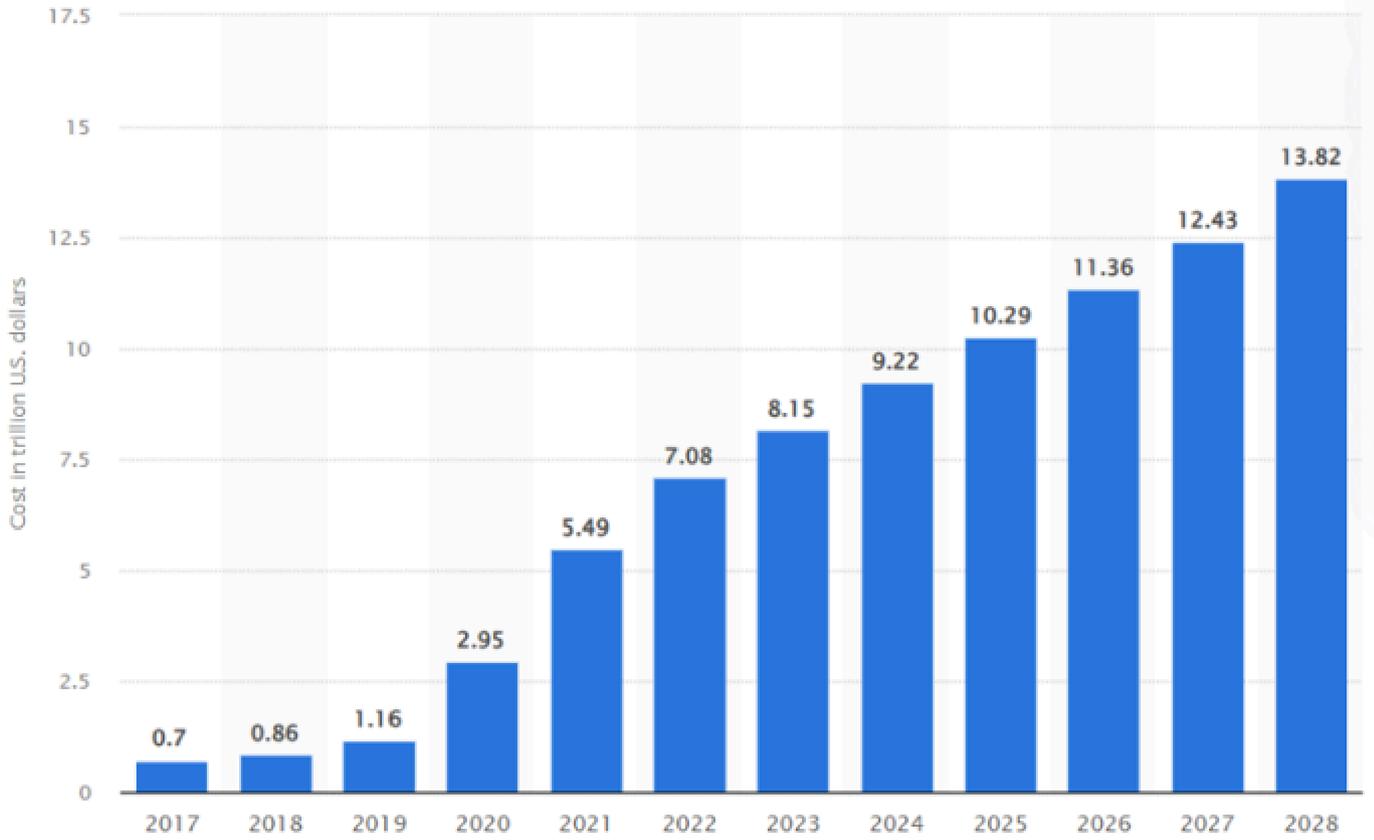
Share of adults worldwide who have experienced cyber crime as of January 2023



ข้อมูลจาก https://www.statista.com/statistics/194133/cybercrime-rate-in-selected-countries/

1 Cyber threats in the AI era : Economic Review

Estimated cost of cybercrime worldwide 2017-2028(in trillion U.S. dollars)



ข้อมูลจาก https://www.statista.com/statistics/194133/cybercrime-rate-in-selected-countries/

1 Cyber threats in the AI era : Economic Review

Percentage of IT budget allocated to security, by country.

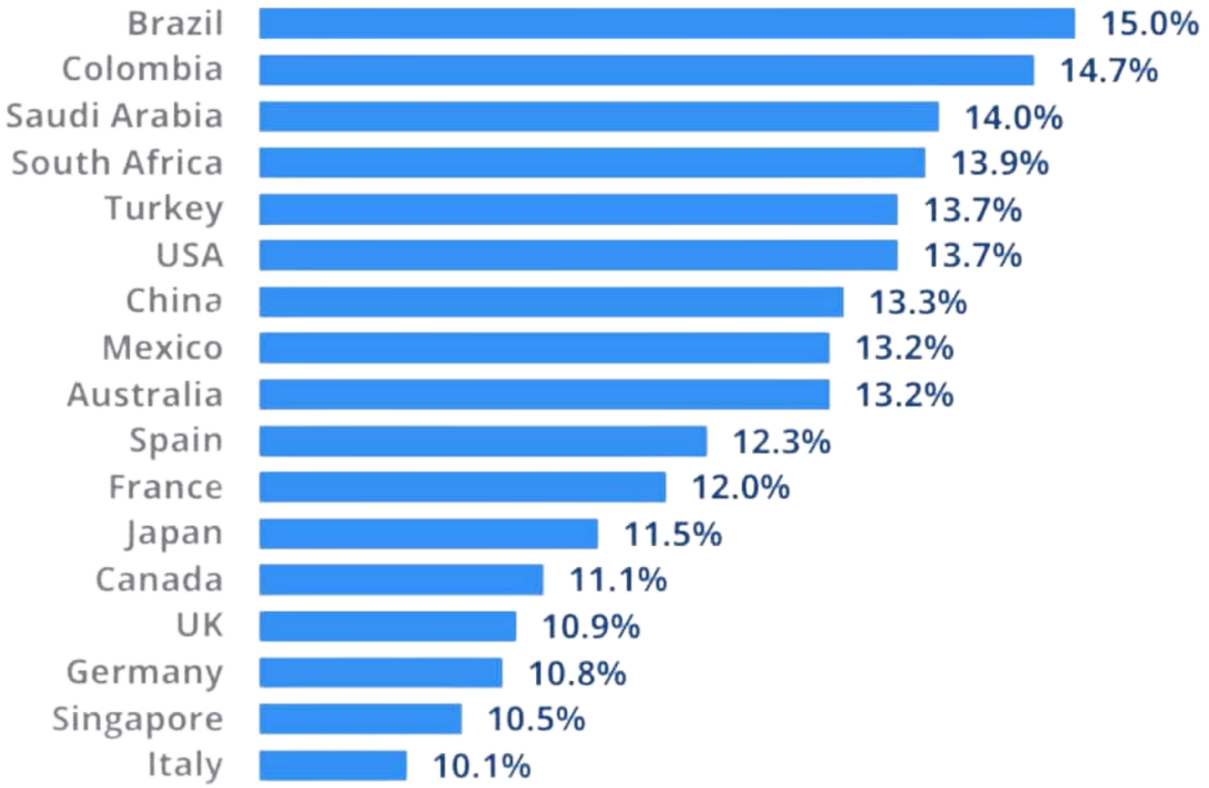
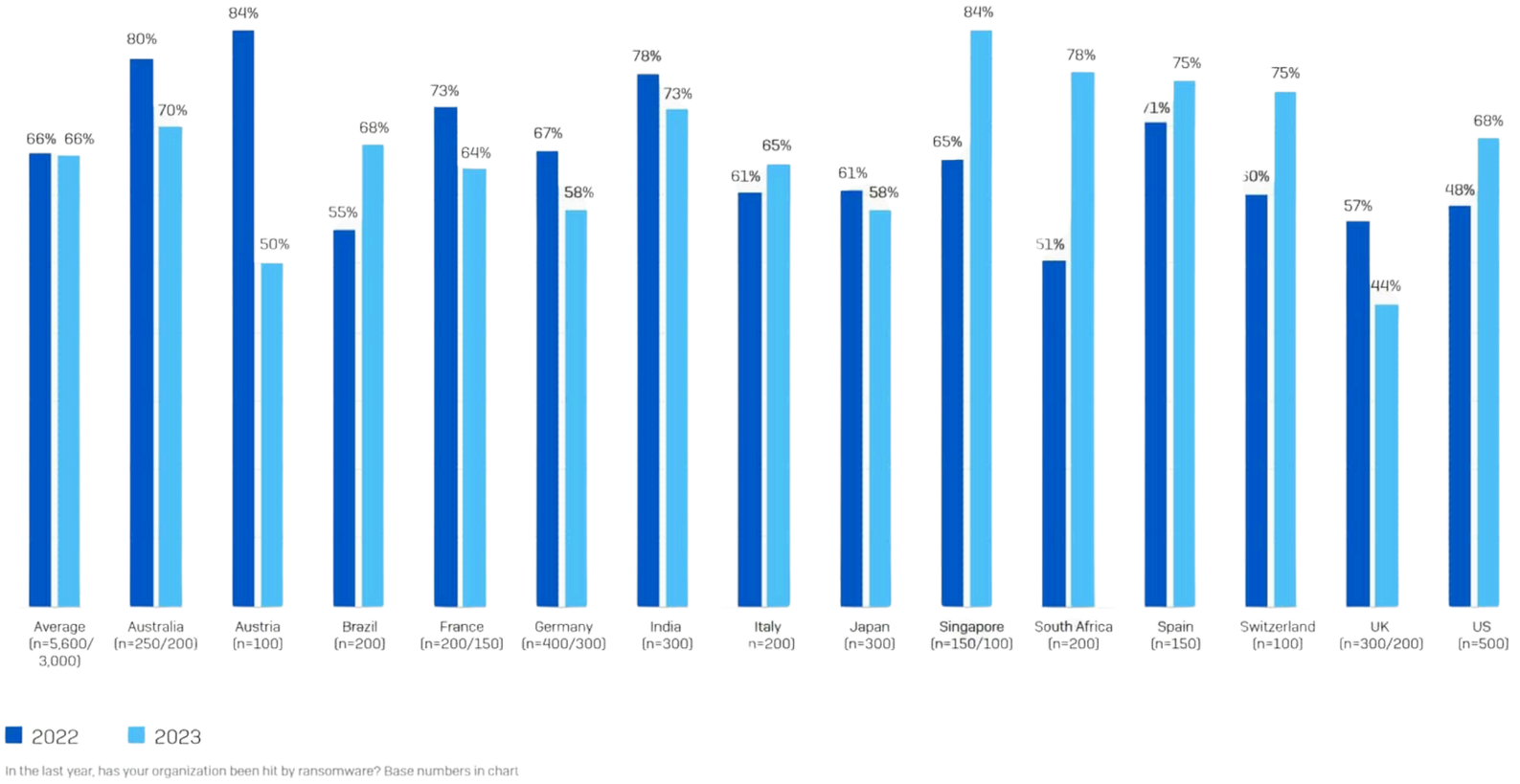


Figure 24: Percentage of IT budget allocated to security, by country.

ข้อมูลจาก https://www.comparitech.com/blog/information-security/italy-cyber-security-statistics/

1 Cyber threats in the AI era : Economic Review

Rate of Ransomware Attacks by Country : 2022 vs 2023

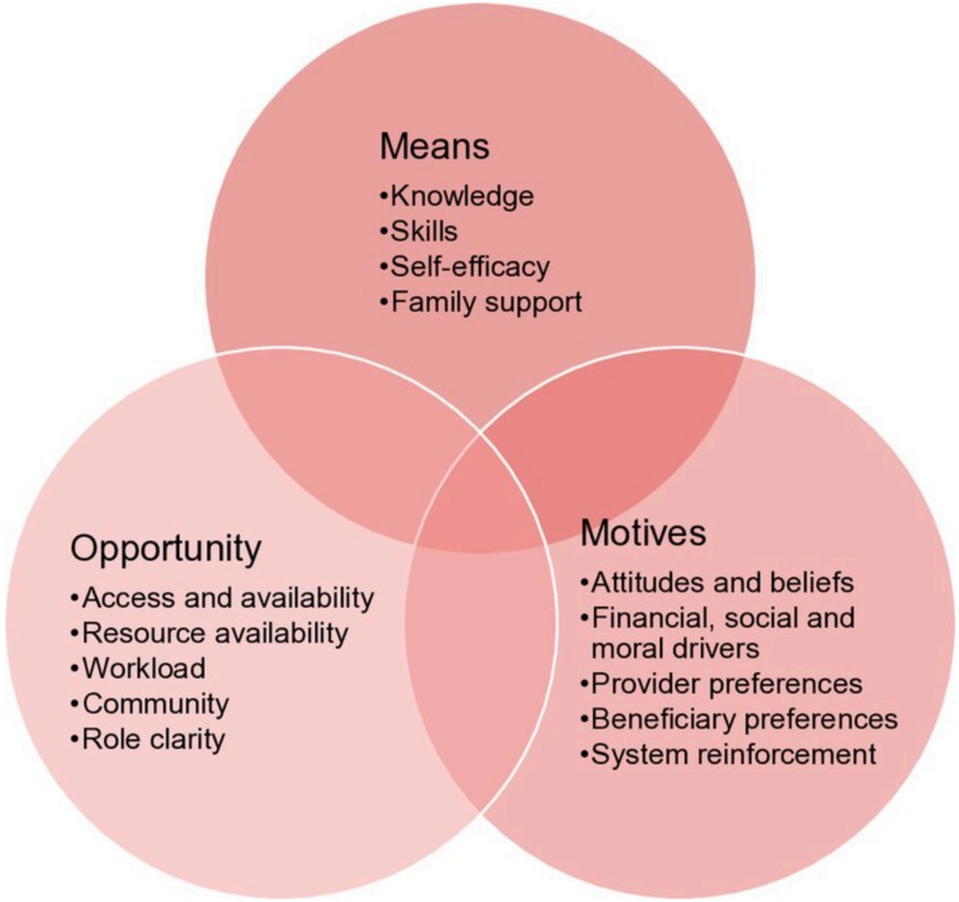


In the last year, has your organization been hit by ransomware? Base numbers in chart

ข้อมูลจาก https://www.comparitech.com/blog/information-security/italy-cyber-security-statistics/

1 Cyber threats in the AI era : Economic Review

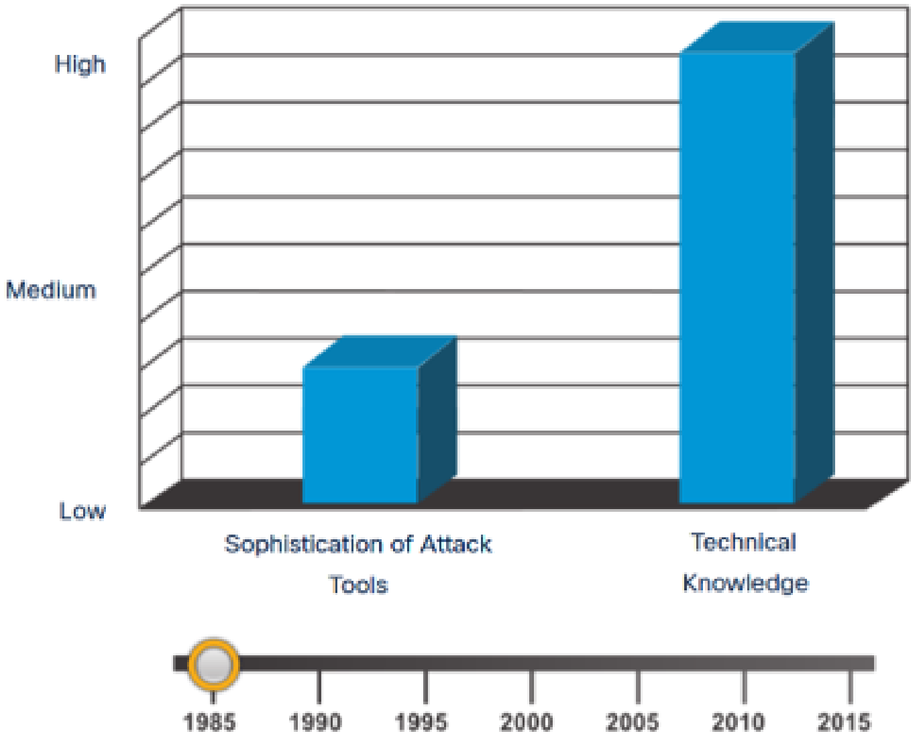
Factor of Cybercrime

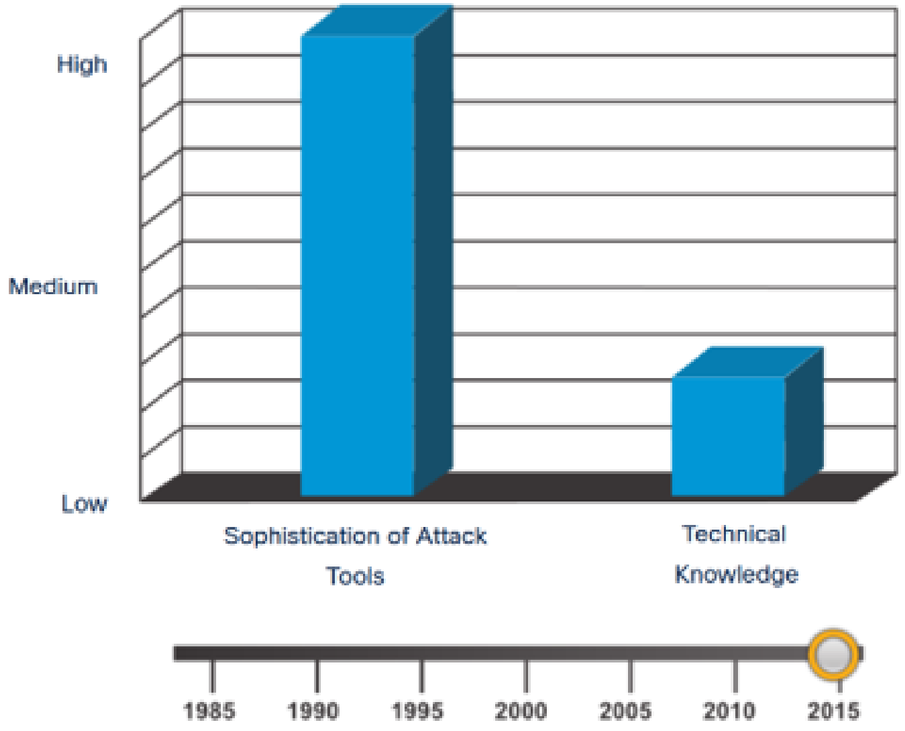


ข้อมูลจาก https://www.secnia.go.th/2018/07/21/เครือข่ายสาธารณสุขสิงตโปร์/

1 Cyber threats in the AI era

Attack Tools



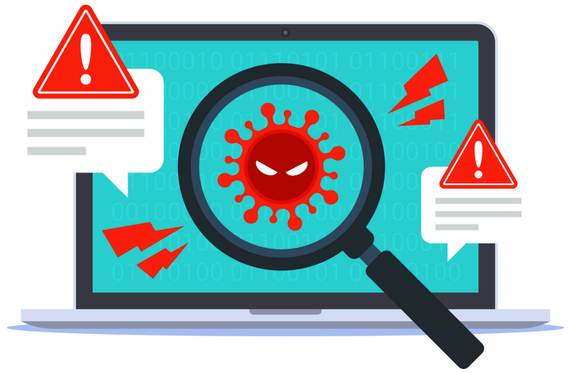



Threat Landscape

2 Threat landscape

1.Malware

- Virus: Code that infiltrates other programs and spreads to other programs when executed.
- Worms: Malware that spreads across a network without relying on a host program.
- Trojans: Malware that disguises itself as harmless software but performs attacks once installed.
- Ransomware: A type of malware that threatens to publish the victim's data or block access to it unless a ransom is paid
- Spyware: Malware that spies and collects user data without permission



2 Threat landscape

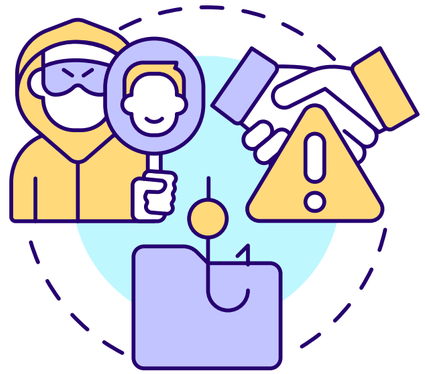
2.Phishing

- Sending emails or text messages that pose as a legitimate source in order to trick users into revealing personal information, such as passwords or credit card information.

2 Threat landscape

3.Social Engineering

- The use of psychological methods to deceive people into disclosing confidential information or performing unsafe actions.



2 Threat landscape

4.Denial of Service (DoS) and Distributed Denial of Service (DDoS)

- An attack that attempts to render an online service unavailable by sending a large amount of traffic to a targeted server.

2 Threat landscape

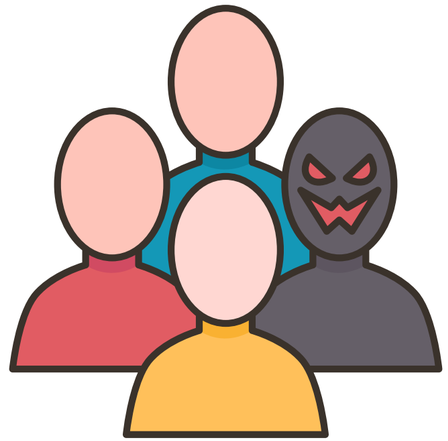
5.Advanced Persistent Threats (APTs)

- APTs are sophisticated, long-term attacks often carried out by nation-states or well-funded groups. They target specific organizations or industries with the intent to steal information or disrupt operations.

2 Threat landscape

6.Insider Threats

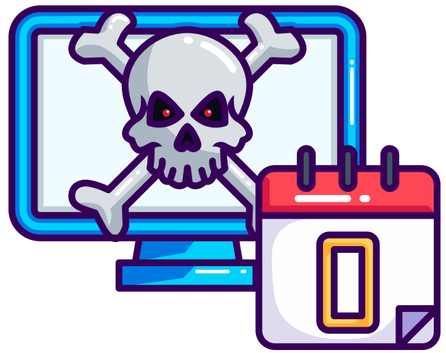
- Threats from insiders, such as employees with malicious intent or unintentionally committing unsafe acts.



2 Threat landscape

7.Zero-Day Exploits

- Attacks that use vulnerabilities that have not been patched or publicly announced, which makes it difficult to prevent. Security executives should exchange information with security agencies such as Thai CERT, CSIRT of various agencies to be aware of threats, etc.



2 Threat landscape

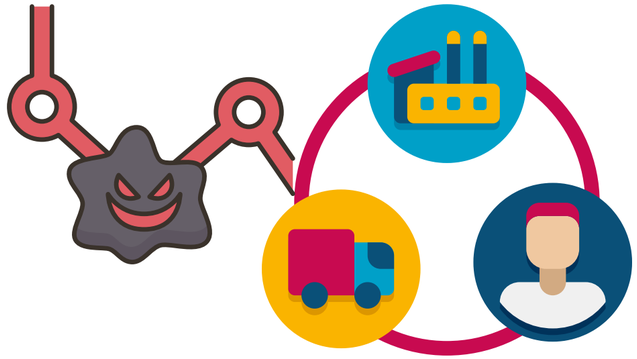
8.IoT Attacks

- Attacks targeting internet-connected devices such as CCTV, smart home devices, industrial OT (Operational Technology) systems, automation systems, PLC devices, SCADA systems, Industrial Internet of Things systems.

2 Threat landscape

9.Supply Chain Attacks

- Attacks that target service providers or suppliers to gain access to an organization's systems by exploiting vulnerabilities in the supply chain.



2 Threat landscape

10.Cryptojacking

- Using another person's computer resources to mine cryptocurrency without permission.

Cyber Threat Case study that impact to the economy

3 Cyber Threat Case study that impact to the economy.

Case Study 1

Stuxnet OT cyber attack. Target Iran nuclear plant. 2010

- **Used by highly sophisticated worms to shoot exploited multiple zero-day**

ข้อมูลจาก https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet

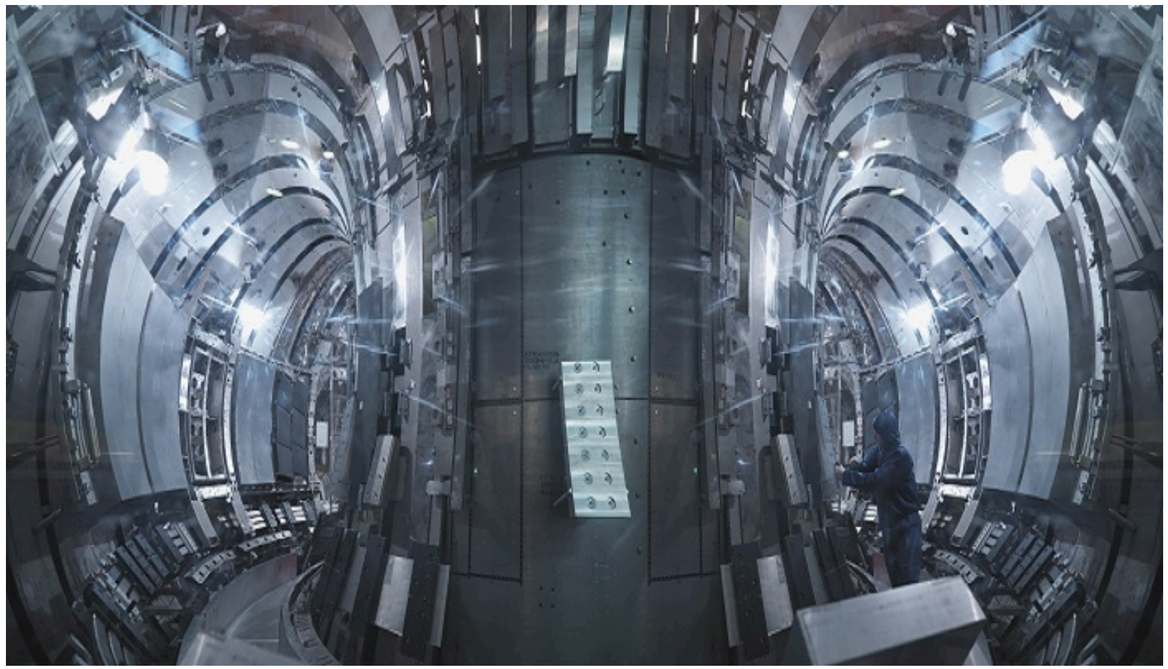
3 Cyber Threat Case study that impact to the economy.

Case Study 1

Stuxnet OT cyber attack. Target Iran nuclear plant. 2010

- Impact: Machinery in nuclear plants is damaged, slowing down the ability to enrich uranium.

- Objective of the attack: sabotage and disrupt the uranium enrichment process.

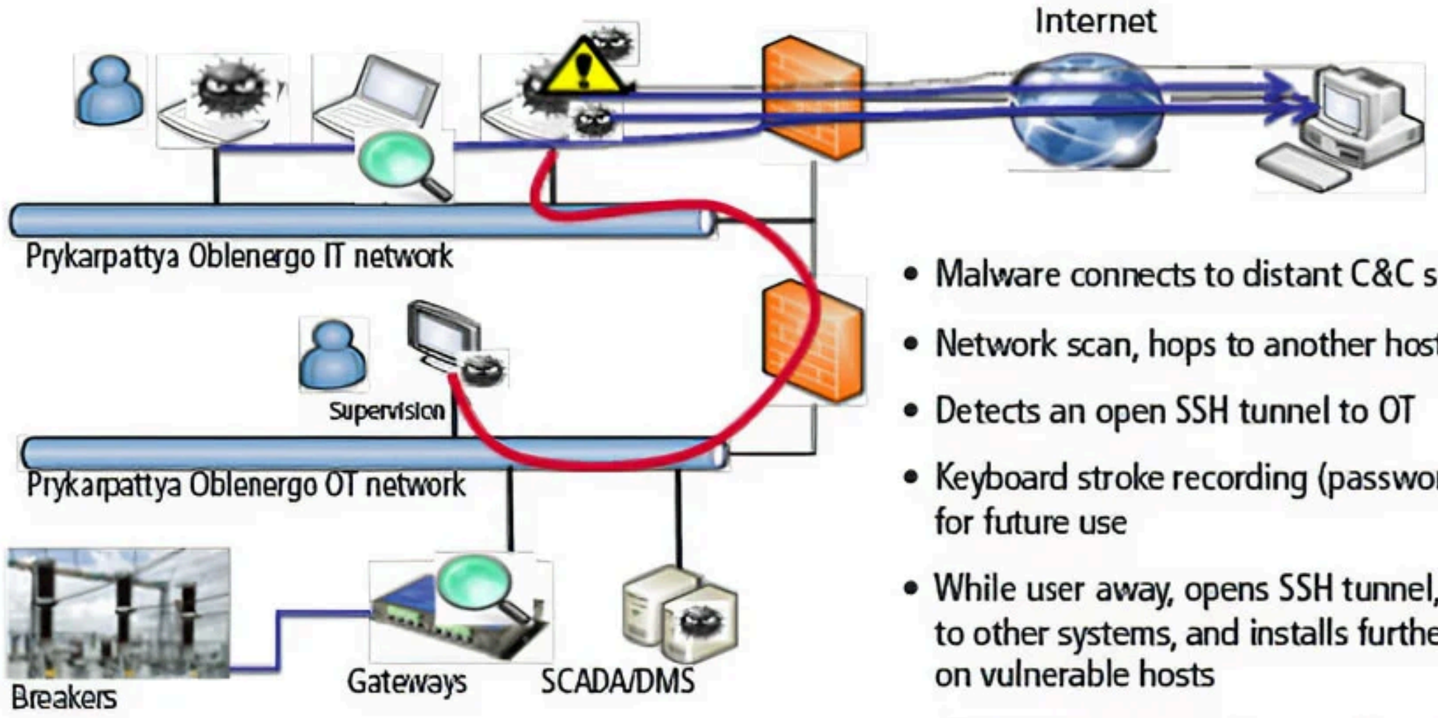


ข้อมูลจาก https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet

3 Cyber Threat Case study that impact to the economy.

Case Study 2

2015 and 2016 ; Ukraine Power Grid Attacks



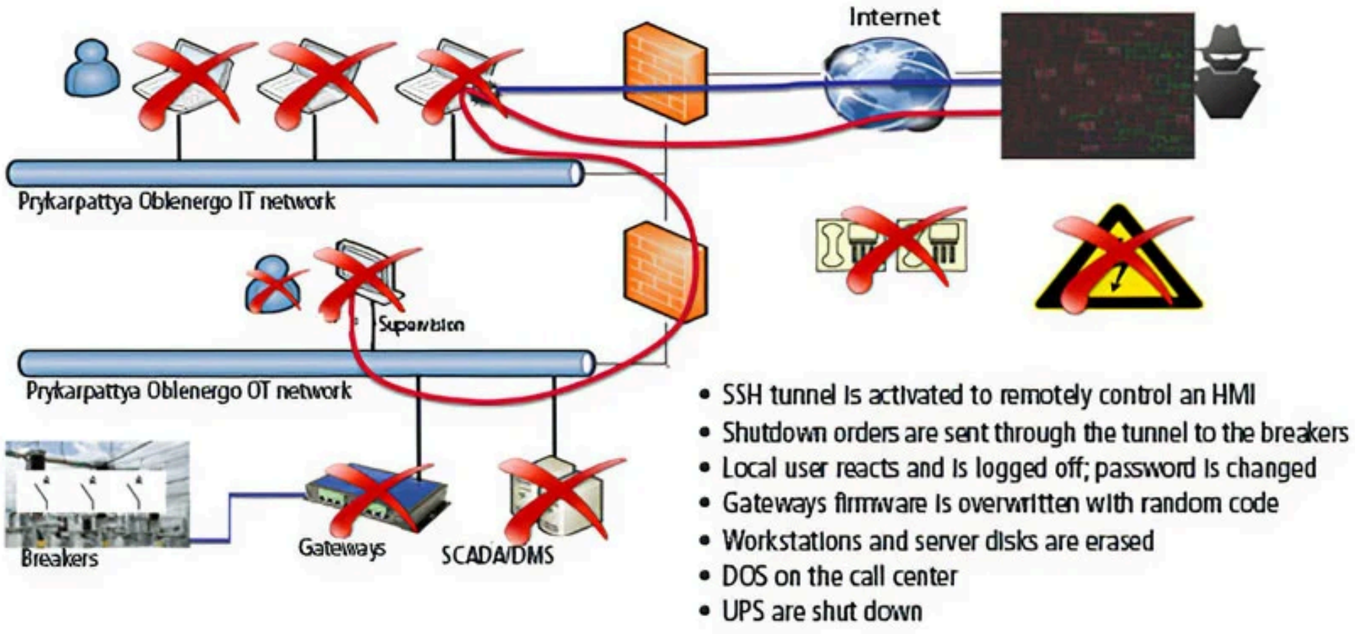
- Malware connects to distant C&C server
- Network scan, hops to another host
- Detects an open SSH tunnel to OT
- Keyboard stroke recording (passwords, etc.) for future use
- While user away, opens SSH tunnel, connects to other systems, and installs further malware on vulnerable hosts
- Cleanup and installation on a low-profile persistent threat, ready for activation

3 Cyber Threat Case study that impact to the economy.

Case Study 2

2015 and 2016 ; Ukraine Power Grid Attacks

- OT cyber attack. Targeted Ukrainian power grid in Dec2015 and Dec2016 using malware called BlackEnergy and KillDisk.



3 Cyber Threat Case study that impact to the economy.

Case Study 3

Ransomware WannaCry Attack (May 2017)

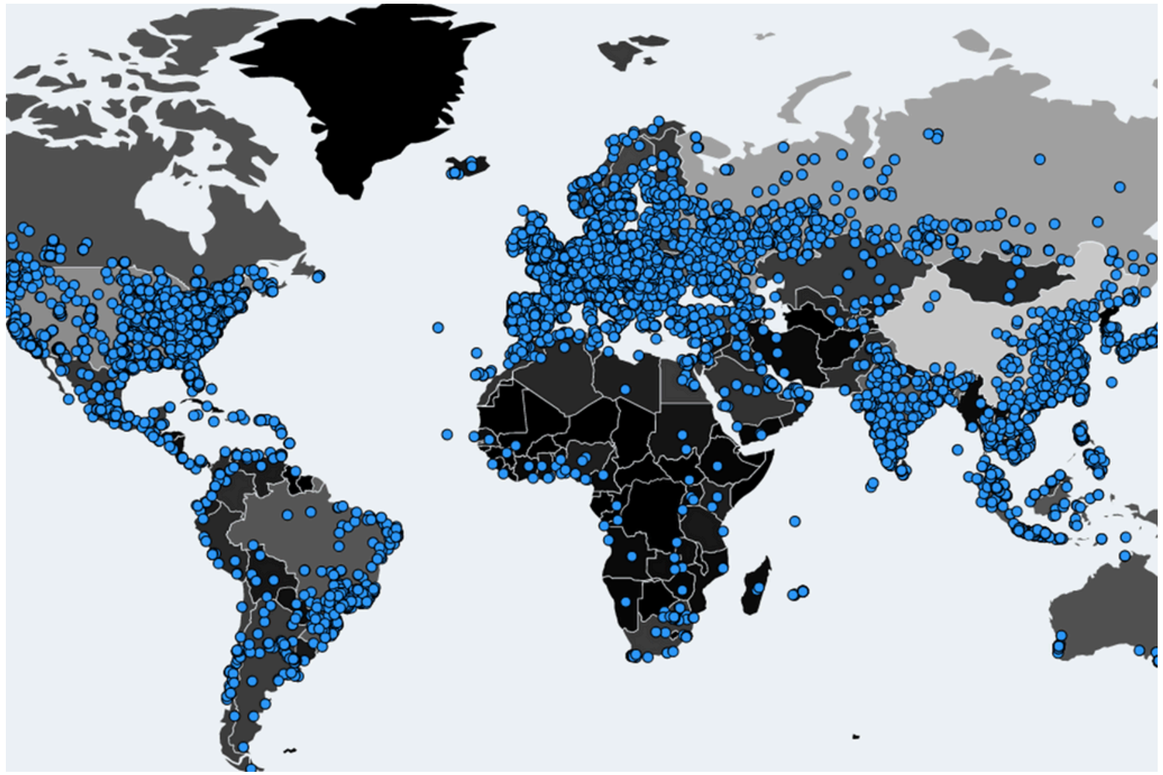
 ข้อมูลจาก https://blog.isa.org/lessons-learned-forensic-analysis-ukrainian-power-grid-cyberattack-malware

3 Cyber Threat Case study that impact to the economy.

Case Study 3

Ransomware WannaCry Attack (May 2017)

- A worldwide cyberattack that affected more than 200,000 computers in 150 countries.



ข้อมูลจาก https://thehackernews.com/2017/05/how-to-wannacry-ransomware.html

3 Cyber Threat Case study that impact to the economy.

Case Study 3

Ransomware WannaCry Attack (May 2017)

ข้อมูลจาก https://thehackernews.com/2017/05/how-to-wannacry-ransomware.html

3 Cyber Threat Case study that impact to the economy.

Case Study 4

SingHealth cyber attack July 2018
1.5 million patient data stolen

SingHealth

Defining Tomorrow's Medicine

ข้อมูลจาก https://www.secnia.go.th/2018/07/21/เครือข่ายสาธารณสุขสิงตโปร์/

3 Cyber Threat Case study that impact to the economy.

Case Study 4

SingHealth cyber attack July 2018
1.5 million patient data stolen

SingHealth
Defining Tomorrow's Medicine

Attack pattern

- Hacker uses Advanced Persistent Threat (APT) to attack Front-End Workstation to access the central database
- Hacker intends to steal data of Singapore Prime Minister ('Lee Hsien Loong')

Impact

Around 1.5 million patient data of SingHealth Specialist Outpatient Clinics and Polyclinics from 1 May 2015 to 4 July 2018 were stolen. Demographic data (ID Card, name, address, gender, date of birth) was stolen.

- OPD prescription data was stolen.

ข้อมูลจาก https://www.secnia.go.th/2018/07/21/เครือข่ายสาธารณสุขสิงตโปร์/

3 Cyber Threat Case study that impact to the economy.

Case Study 4

Example : Advanced Persistent Threat (APT)

Suspected attribution	APT	Target sectors
Iran	APT33-34,39	The travel industry and IT firms that support it and the high-tech industry,military,commercial
Russia	APT 28-29	Government and Military, Political Organizations, Media, Aerospace, Energy Government and Diplomatic Institutions, Healthcare and Pharmaceutical, Think Tanks and Research Institutions, Technology:
North Korea	APT37-38	industry verticals, including chemicals, electronics, manufacturing, aerospace, automotive, and healthcare.

3 Cyber Threat Case study that impact to the economy.

Case Study 5

PEA Ransomware cyber attack
Causing system shutdown for several days June 2020

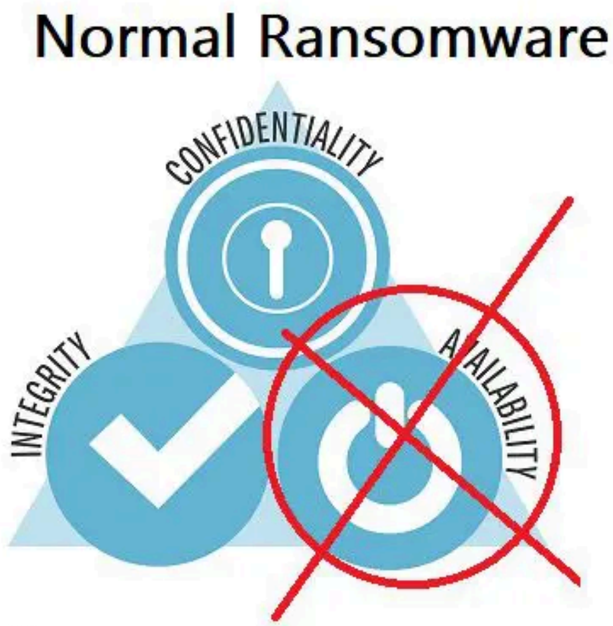
ข้อมูลอ้างอิง https://www.nia.go.th/cyber/cyberpage/89/

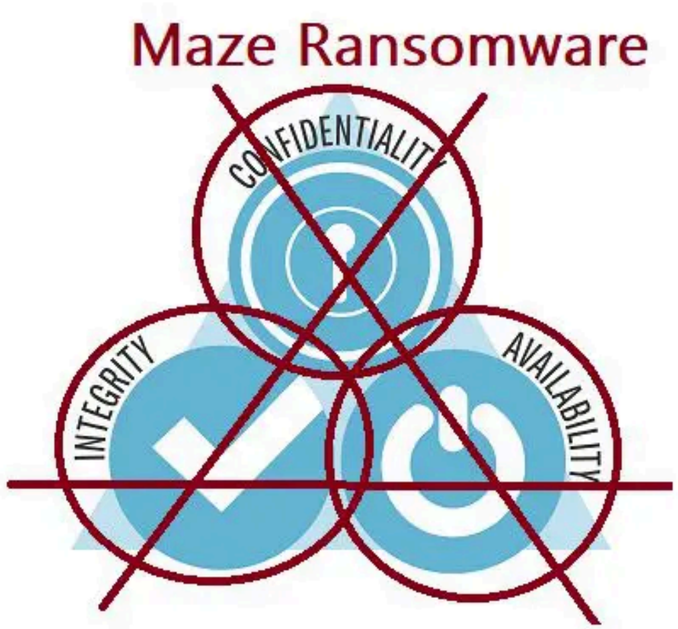
3 Cyber Threat Case study that impact to the economy.

Case Study 5

PEA Ransomware cyber attack
Causing system shutdown for several days June 2020

Maze Ransomware Triple Threat





ข้อมูลอ้างอิง https://www.nia.go.th/cyber/cyberpage/89/

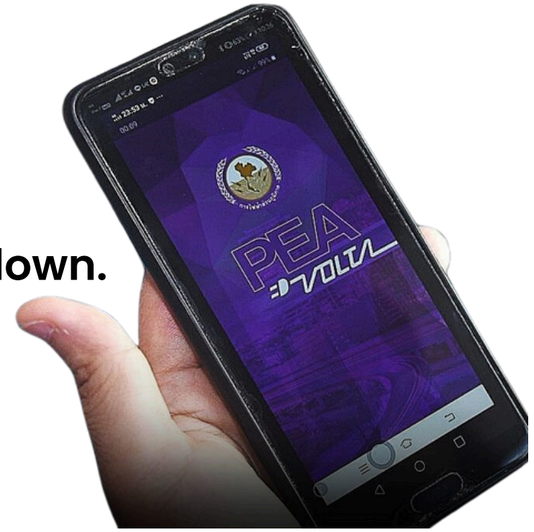
3 Cyber Threat Case study that impact to the economy.

Case Study 5

PEA Ransomware cyber attack
Causing system shutdown for several days June 2020

Damage

- Files are compressed and encrypted to demand ransom
- Hackers disseminate stolen data online



The service recipients were affected by the cyber attack as follows:

- Some information technology systems must be temporarily shut down.
- Temporarily shut down the online payment system.
- Temporarily shut down the PEA Smart Plus application.

ข้อมูลอ้างอิง https://www.nia.go.th/cyber/cyberpage/89/

3 Cyber Threat Case study that impact to the economy.

Case Study 6

JBS Foods Cyber Attack May 2021
REvil Ransomware Demands Files

ข้อมูลอ้างอิง https://claroty.com/blog/jbs-attack-puts-food-and-beverage-cybersecurity-to-the-test/

3 Cyber Threat Case study that impact to the economy.

Case Study 6

JBS Foods Cyber Attack May 2021

JBS Foods is the world's largest meat processor, exporting meat from Brazil to the United States. It has 230,000 employees and sales of more than $5.2 billion.

Attack Pattern

- **Hackers used REvil Ransomware to lock down access to the company’s systems. The incident lasted more than a month, causing disruption to JBS Foods’ business.**

Impact

- **JBS had to close several plants around the world**
- **Delayed or disrupted meat shipments**
- **Global meat prices soar**
- **JBS lost revenue and reputation**

ข้อมูลอ้างอิง https://claroty.com/blog/jbs-attack-puts-food-and-beverage-cybersecurity-to-the-test/

3 Cyber Threat Case study that impact to the economy.

Case Study 6

JBS Foods Cyber Attack May 2021

Response

- **JBS decided to pay a ransom of 11 million USD to REvil group**
- **JBS coordinated with several government agencies to jointly investigate the perpetrators**
- **This incident raised concerns about food security**

ข้อมูลอ้างอิง https://claroty.com/blog/jbs-attack-puts-food-and-beverage-cybersecurity-to-the-test/

3 Cyber Threat Case study that impact to the economy.

Case Study 7

CNA Financial Cyber Attack May 2021
REvil Ransomware Demands Files

ข้อมูลอ้างอิง https://www.insurancejournal.com/news/national/2021/11/29/643569.htm

3 Cyber Threat Case study that impact to the economy.

Case Study 7

CNA Financial Cyber Attack May 2021

CNA is a major insurance company in the United States with 4,500 employees and sales of over $7 billion.

Attack Pattern

- **Hackers use REvil Ransomware to lock access to company systems and sensitive company data.**

Impact

- **CNA Financial had to suspend some operations**
- **CNA Financial customers lost access to their insurance information**
- **The company lost revenue and reputation**

ข้อมูลอ้างอิง https://www.insurancejournal.com/news/national/2021/11/29/643569.htm

3 Cyber Threat Case study that impact to the economy.

Case Study 7

JBS Foods Cyber Attack May 2021

Response

- CNA decided to pay a ransom of 40 million USD to the REvil group.
- CNA coordinated with government agencies in several countries to cooperate in investigating the perpetrators.
- This incident raised concerns about trust and financial stability.

ข้อมูลอ้างอิง https://www.insurancejournal.com/news/national/2021/11/29/643569.htm

3 Cyber Threat Case study that impact to the economy.

Case Study 8

Kaseya VSA was cyber attacked July 2021

ข้อมูลอ้างอิง https://www.kaseya.com/press-release/kaseya-responds-swiftly-to-sophisticated-cyberattack-mitigating-global-disruption-to-customers/

3 Cyber Threat Case study that impact to the economy.

Case Study 8

Kaseya VSA was cyber attacked July 2021

Kaseya VSA is a business that provides remote monitoring and manage (Remote Monitoring and Management - RMM).

Attack pattern

- **Inject malicious code into Kaseya VSA vulnerability to control customer computer systems**
- **Use controlled customer computers to distribute REvil Ransomware, encrypt files and demand ransom**

Response

- **When attacked, Kaseya shuts down all its own servers.**
- **Customers using On-Premise VSA are advised to shut down their servers as well.**

ข้อมูลอ้างอิง https://www.kaseya.com/press-release/kaseya-responds-swiftly-to-sophisticated-cyberattack-mitigating-global-disruption-to-customers/

3 Cyber Threat Case study that impact to the economy.

Case Study 8

Kaseya VSA was cyber attacked July 2021

Impact

- Affected over 1,000 organizations worldwide, files were encrypted
- Caused financial and reputational damage to Kaseya VSA and the affected organizations

Response

- When attacked, Kaseya shut down all of its servers.
- Kaseya On-Premise customers are advised to shut down their servers as well.
- Kaseya did not pay the ransom, but was able to decrypt and restore the system.
- Kaseya updated its software to fix the vulnerability.
- Kaseya is coordinating with government agencies in several countries to jointly investigate the perpetrators.

ข้อมูลอ้างอิง https://www.kaseya.com/press-release/kaseya-responds-swiftly-to-sophisticated-cyberattack-mitigating-global-disruption-to-customers/

3 Cyber Threat Case study that impact to the economy.

Case Study 9

Patient data in the public health system, September 2021

ข้อมูลอ้างอิง https://www.hfocus.org/content/2024/03/30032

3 Cyber Threat Case study that impact to the economy.

Case Study 9

Patient data in the public health system, September 2021

On September 6, 2021, there were reports of more than one million basic patient data in the public health system.

Attack pattern

- Hackers attacked the hospital database system, both government and private sectors.
- Stealing more than a million patient records
- The stolen data includes names, surnames, addresses, phone numbers, dates of birth, names of attending physicians, and hospital names.

Impact

- Patients are at risk of personal data being hacked
- May be used for fraud or illegal transactions
- Damage to the reputation of the healthcare system
- Create concerns for the public

ข้อมูลอ้างอิง https://www.hfocus.org/content/2024/03/30032

3 Cyber Threat Case study that impact to the economy.

Case Study 10 (Not Cyber Attack)

CrowdStrike Software Glitch July 19, 2024

ข้อมูลอ้างอิง https://www.techradar.com/news/live/windows-outage-july-2024-live

3 Cyber Threat Case study that impact to the economy.

Case Study 10 (Not Cyber Attack)

CrowdStrike Software Glitch July 19, 2024

Cause

- CrowdStrike Falcon fan-caused crashes that may have resulted from external CrowdStrike platforms. Cause: "Failure-causing factors" impact customer systems worldwide.

Impact

- Millions of CrowdStrike users worldwide experienced a system outage, were unable to use their security platform, and impacted businesses, organizations, and agencies at scale. Some organizations had to temporarily stop operations.
- Financial damage from this incident: some businesses lost revenue, lost business opportunities, and incurred additional costs to fix the issue.
- Impact on CrowdStrike's reputation: decreased credibility with customers, loss of confidence, and possible loss of customers.

ข้อมูลอ้างอิง https://www.techradar.com/news/live/windows-outage-july-2024-live

8 สรุปและตอบคำถาม

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

MYSURACHET.COM

Questions & Answer

www.MySurachet.com

085 636 2551

surachet@catinfonet.com

Thank you

LINE

LINE