CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

MYSURACHET.COM

Information Security Managment Systems(ISMS)

ระบบมาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ

ตามแนวทาง ISO/IEC 27001

Part 1/2

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

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

MYSURACHET.COM

Surachet Suchaiya, PhD.

ประวัติการศึกษา ประวัติการทำงาน ความเชี่ยวชาญ ประสบการณ์ ประกาศนียบัตรการฝึกอบรมที่ได้รับ และงานวิจัยของอาจารย์

Information Security Managment Systems(ISMS)
ตามแนวทาง ISO/IEC 27001

Agenda

1. ภัยคุกคามทางไซเบอร์ในยุค AI
2. ประเภทของภัยคุกคาม
3. กรณีศึกษาภัยคุกคามทางไซเบอร์ที่สร้างผลกระทบต่อระบบเศรษฐกิจ
4. การสร้างมั่นคงปลอดภัยระบบสารสนเทศตามแนวทาง ISO/IEC 27001
5. บทบาทหน้าที่และการมีส่วนร่วม
6. สรุปและตอบคำถาม
7. **Quiz and Exercise**

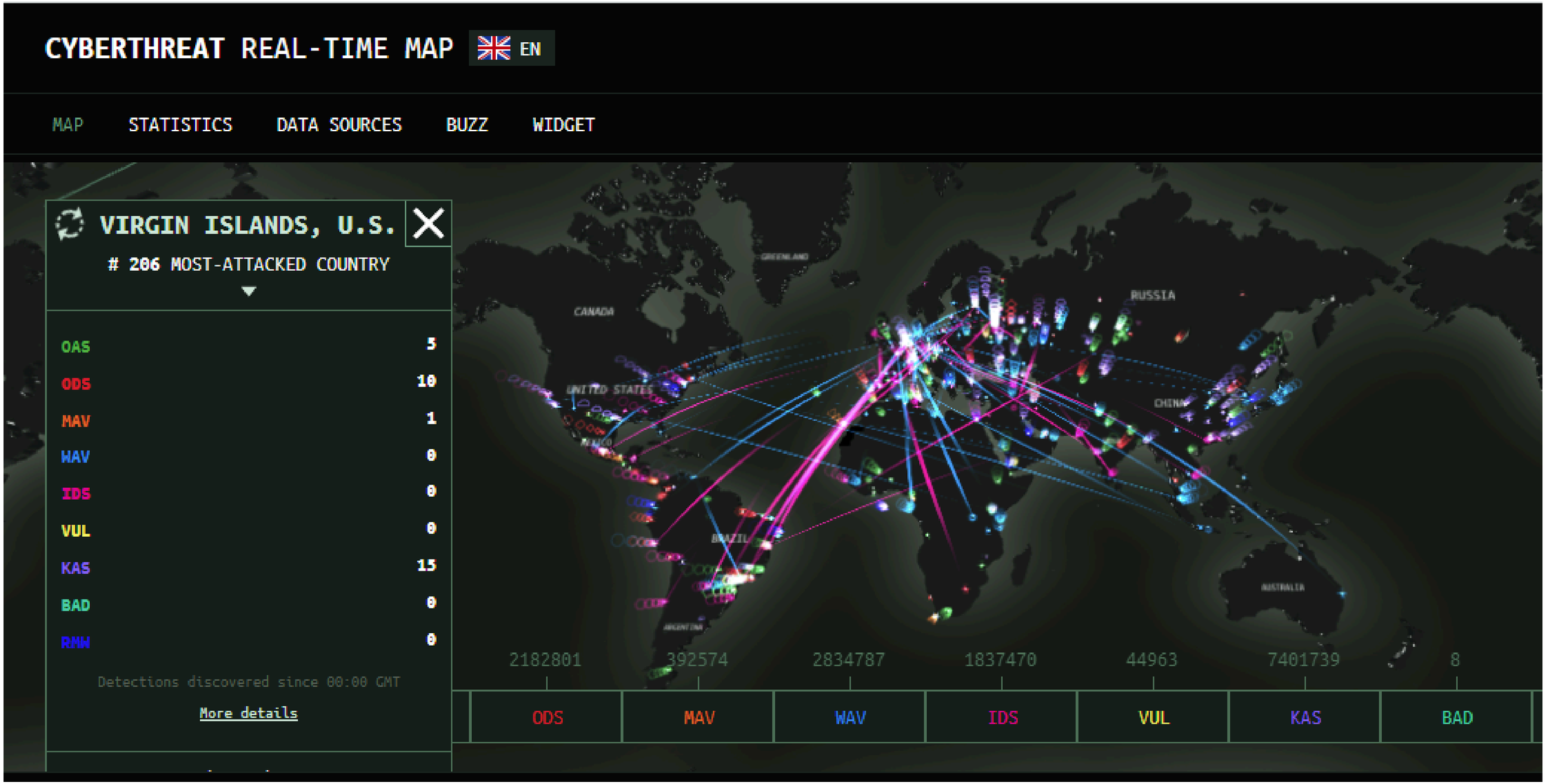
MYSURACHET.COM

1 ภัยคุกคามทางไซเบอร์ในยุค AI

MYSURACHET.COM

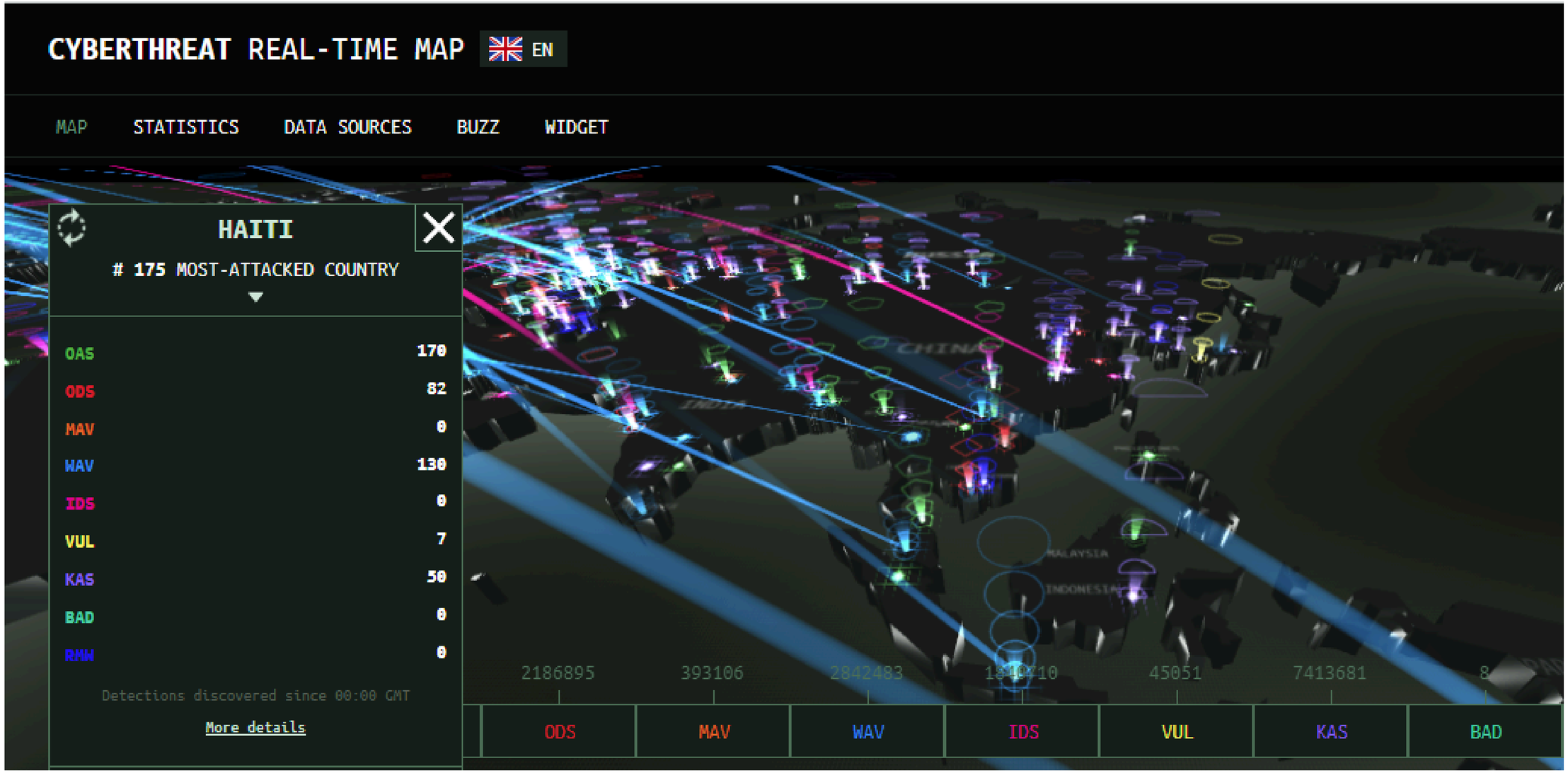
1 ภัยคุกคามทางไซเบอร์ในยุค AI

MYSURACHET.COM



1 ภัยคุกคามทางไซเบอร์ในยุค AI

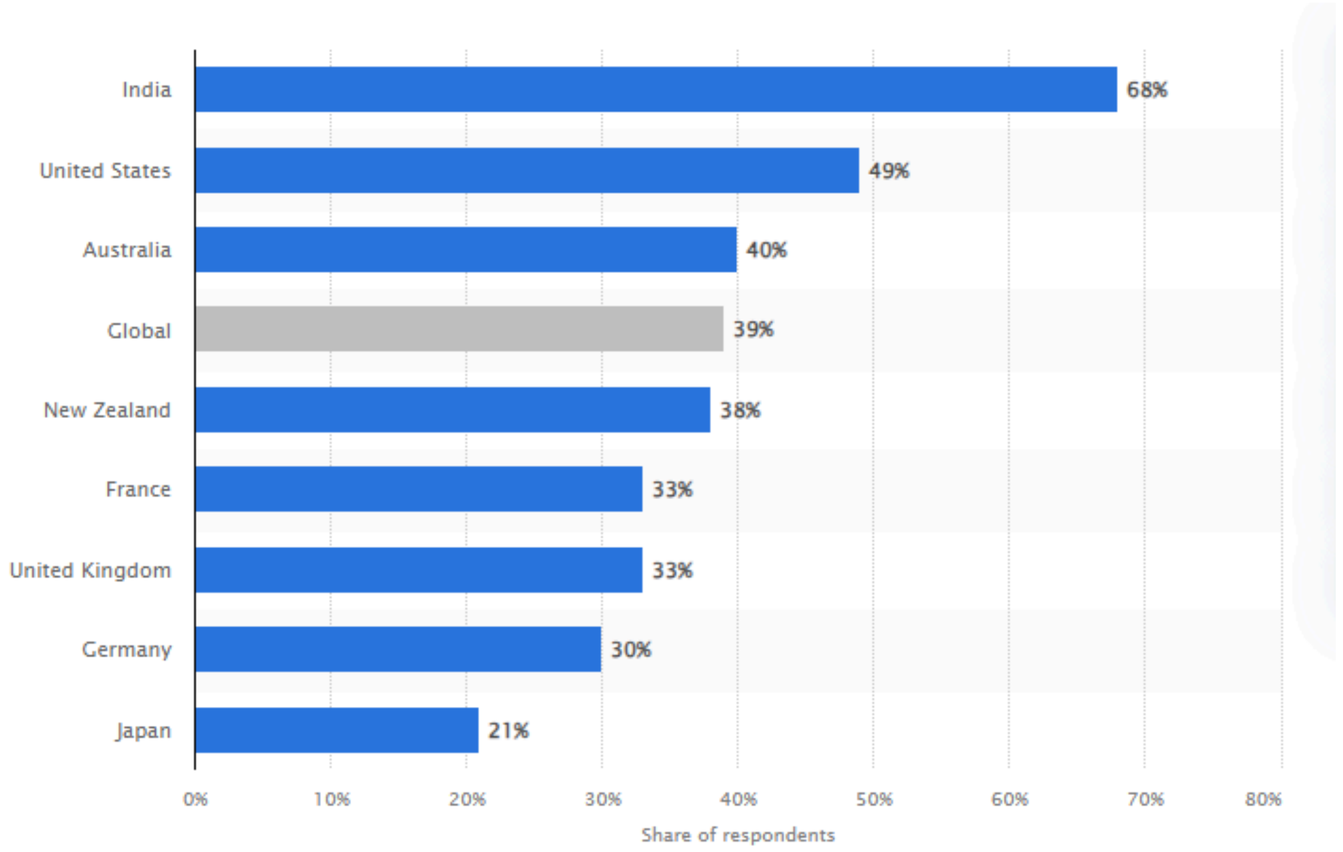
MYSURACHET.COM



1 ภัยคุกคามทางไซเบอร์ในยุค **AI : Economic Review**

แนวโน้มและอันตรายที่เกิดขึ้นจากภัยคุกคามทางโลกไซเบอร์

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

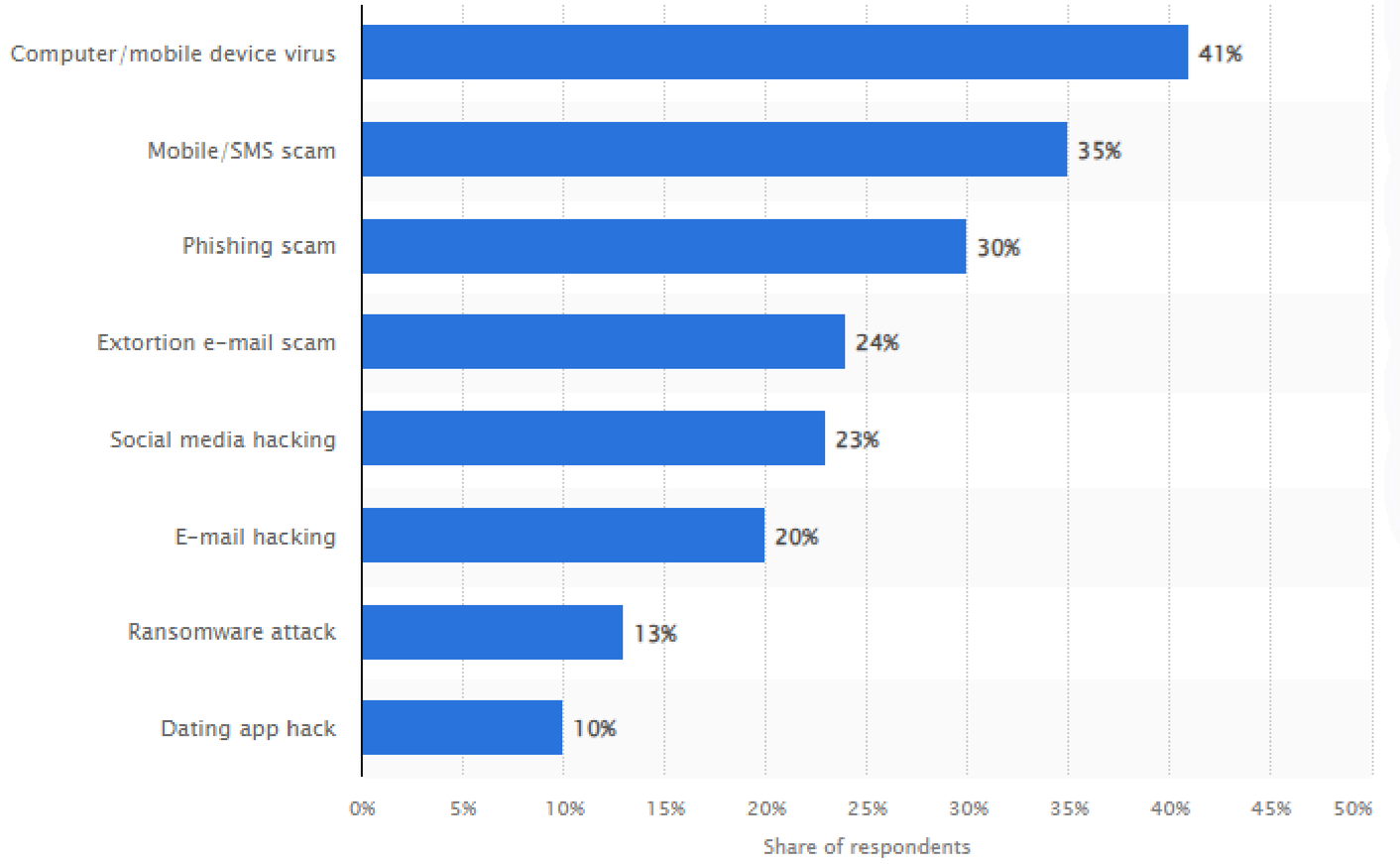


ข้อมูลจาก https://www.statista.com/statistics/194133/cybercrime-rate-in-selected-countries/

1 ภัยคุกคามทางไซเบอร์ในยุค **AI : Economic Review**

แนวโน้มและอันตรายที่เกิดขึ้นจากภัยคุกคามทางโลกไซเบอร์

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



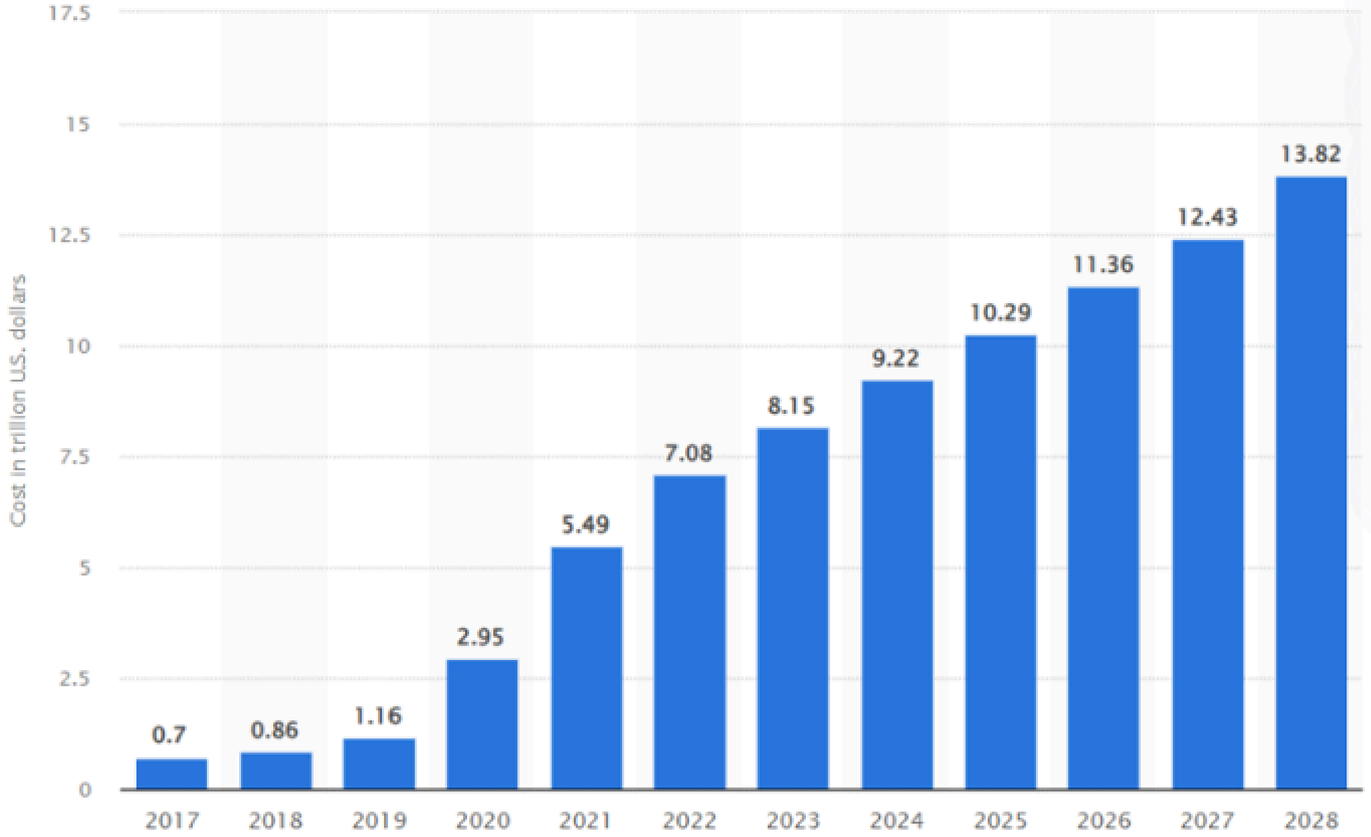
MYSURACHET.COM

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

1 ภัยคุกคามทางไซเบอร์ในยุค AI : Economic Review

แนวโน้มและอันตรายที่เกิดขึ้นจากภัยคุกคามทางโลกไซเบอร์

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



MYSURACHET.COM

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

1 ภัยคุกคามทางไซเบอร์ในยุค AI : Economic Review

งบประมาณด้านความมั่นคงปลอดภัยไซเบอร์แต่ละประเทศ

Percentage of IT budget allocated to security, by country.

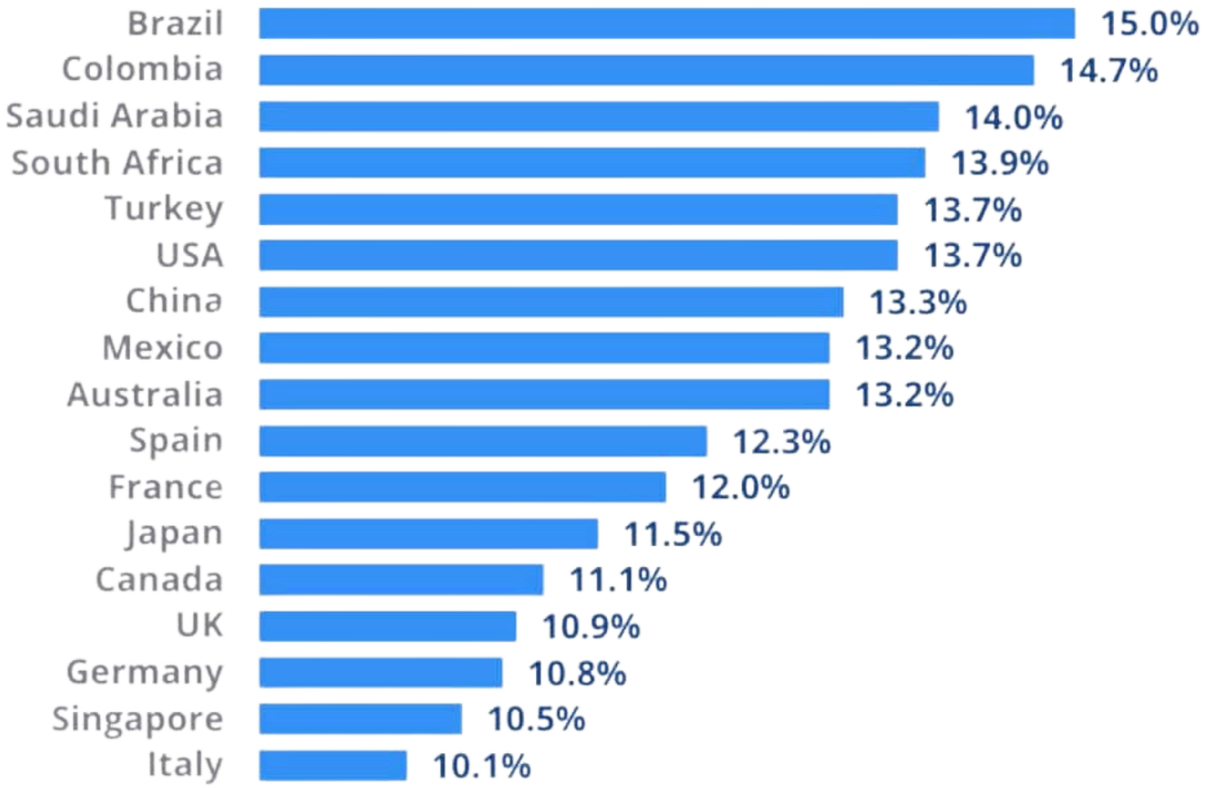


Figure 24: Percentage of IT budget allocated to security, by country.

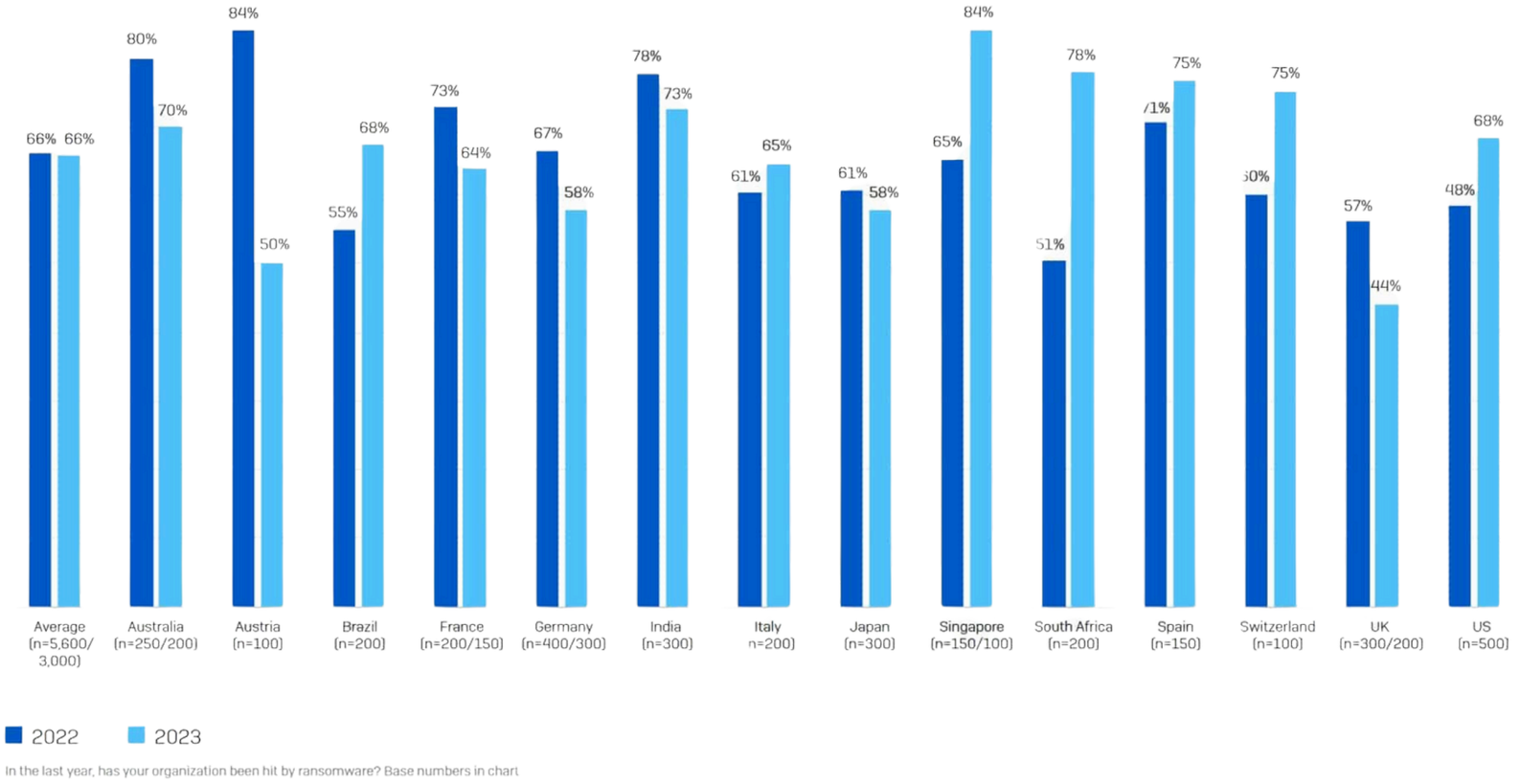
MYSURACHET.COM

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

1 ภัยคุกคามทางไซเบอร์ในยุค AI : Economic Review

อัตราการโจมตีจากการเรียกค่าไถ่ข้อมูลในปี 2022 และ ปี2023

Rate of Ransomware Attacks by Country : 2022 vs 2023

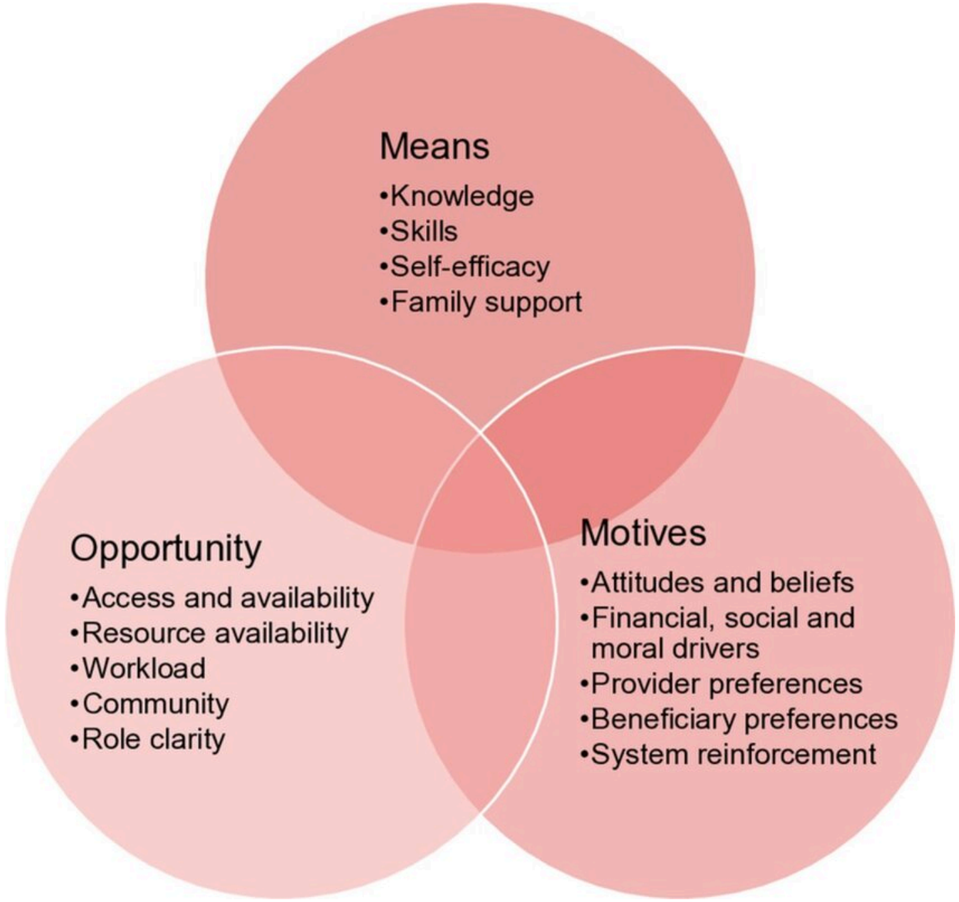


MYSURACHET.COM

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

1 ภัยคุกคามทางไซเบอร์ในยุค **AI : Economic Review**

ปัจจัยที่ก่อให้เกิดอาชญากรรมทางไซเบอร์ **(Cyber Crime)**

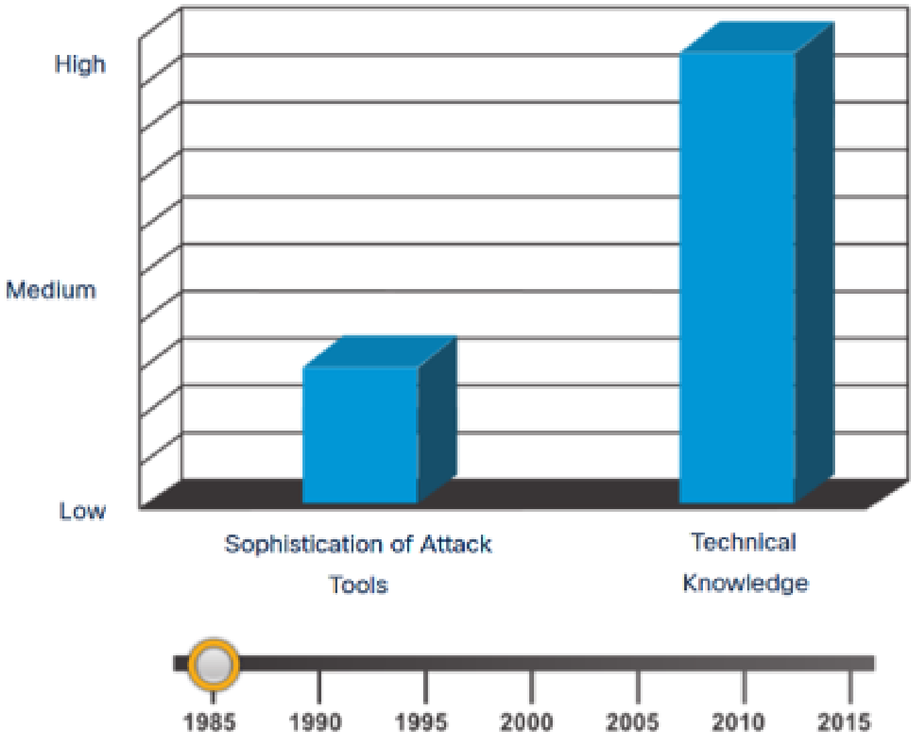


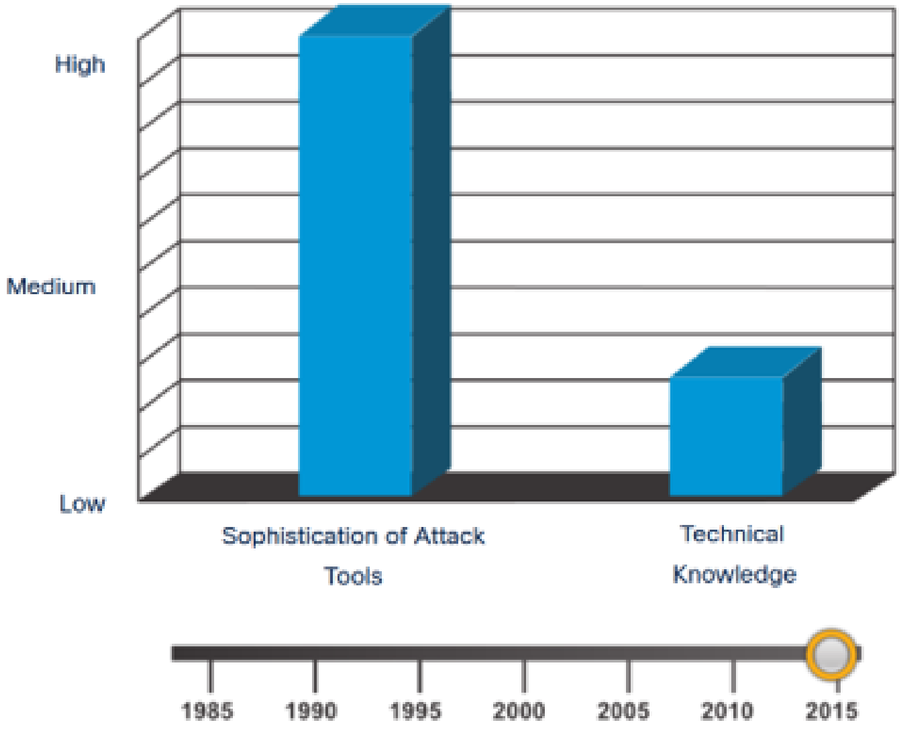
MYSURACHET.COM

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

1 ภัยคุกคามทางไซเบอร์ในยุค AI

Attack Tools (เครื่องมือที่ใช้ในการโจมตี)



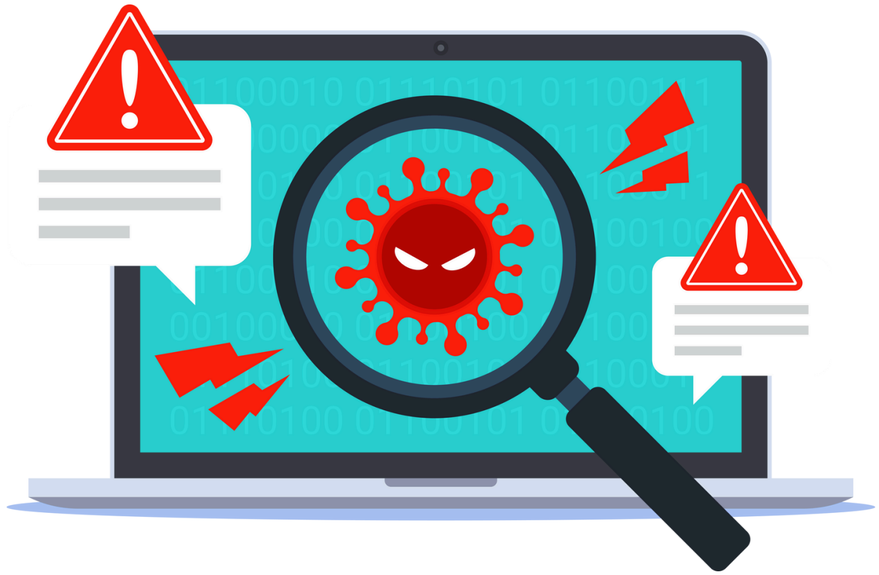



Threat Landscape

2 ประเภทของภัยคุกคาม

1.Malware (มัลแวร์)

- **Virus:** โค้ดที่แฝงตัวในโปรแกรมอื่นๆ และแพร่กระจายไปยังโปรแกรมอื่นๆ เมื่อถูกเรียกใช้งาน
- **Worms:** มัลแวร์ที่แพร่กระจายไปทั่วเครือข่ายโดยไม่ต้องพึ่งพาโฮสต์โปรแกรม
- **Trojans:** มัลแวร์ที่ปลอมตัวเป็นซอฟต์แวร์ที่ไม่เป็นอันตราย แต่ทำการโจมตีเมื่อถูกติดตั้ง
- **Ransomware:** มัลแวร์ที่เข้ารหัสไฟล์ของผู้ใช้และเรียกค่าไถ่เพื่อปลดล็อกไฟล์
- **Spyware:** มัลแวร์ที่คอยสอดส่องและเก็บข้อมูลของผู้ใช้โดยไม่ได้รับอนุญาต



2

ประเภทของภัยคุกคาม

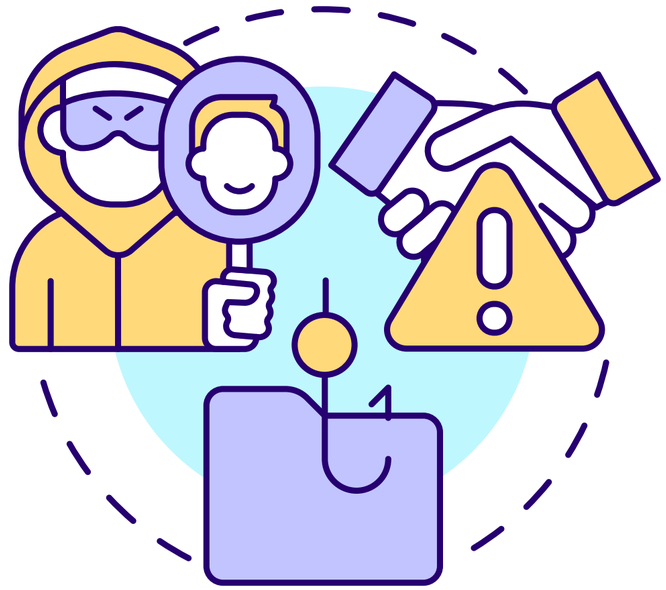
2.Phishing (ฟิชชิ่ง)

- การส่งอีเมลหรือข้อความที่ปลอมแปลงเป็นแหล่งข้อมูลที่น่าเชื่อถือเพื่อหลอกให้ผู้ใช้เปิดเผยข้อมูลส่วนตัว เช่น รหัสผ่านหรือข้อมูลบัตรเครดิต

2 ประเภทของภัยคุกคาม

3.Social Engineering (วิศวกรรมสังคม)

- การใช้วิธีทางจิตวิทยาในการหลอกลวงบุคคลให้เปิดเผยข้อมูลที่เป็นความลับหรือดำเนินการที่ไม่ปลอดภัย



2

ประเภทของภัยคุกคาม

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

- การโจมตีที่พยายามทำให้บริการออนไลน์ไม่สามารถให้บริการได้โดยการส่งปริมาณการใช้งานจำนวนมากไปยังเซิร์ฟเวอร์เป้าหมาย

2

ประเภทของภัยคุกคาม

5.Advanced Persistent Threats (APTs)

- การโจมตีที่พยายามทำให้บริการออนไลน์ไม่สามารถให้บริการได้โดยการส่งปริมาณการใช้งานจำนวนมากไปยังเซิร์ฟเวอร์เป้าหมาย

2 ประเภทของภัยคุกคาม

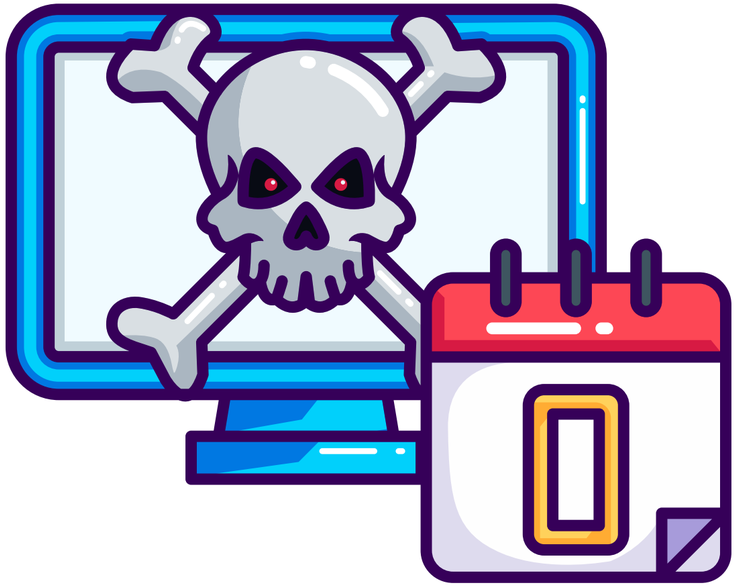
6.Insider Threats (ภัยคุกคามจากคนในองค์กร)

- การคุกคามที่มาจากบุคคลภายในองค์กร เช่น พนักงานที่มีความประสงค์ร้ายหรือทำการกระทำที่ไม่ปลอดภัยโดยไม่ได้ตั้งใจ

2 ประเภทของภัยคุกคาม

7.Zero-Day Exploits

- การโจมตีที่ใช้ช่องโหว่ที่ยังไม่มีการแก้ไขหรือประกาศต่อสาธารณะ ซึ่งทำให้การป้องกันเป็นไปได้ยาก ผู้บริหารด้านความมั่นคงปลอดภัยควรมีการแลกเปลี่ยนข้อมูลกับหน่วยงานที่ดูแลด้านความมั่นคงปลอดภัย เช่น **Thai CERT , CSIRT** ของหน่วยงานต่างๆ เพื่อทราบถึงภัยคุกคามเป็นต้น



2 ประเภทของภัยคุกคาม

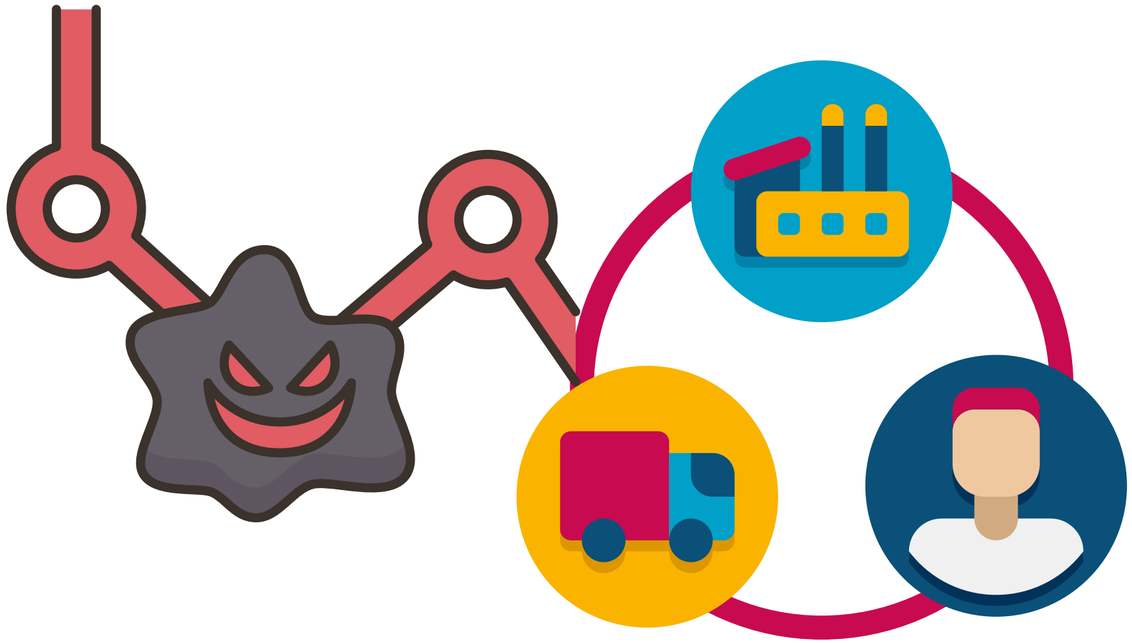
8.IoT Attacks (การโจมตีอุปกรณ์ IoT : Internet of Things)

- การโจมตีที่มุ่งเป้าไปยังอุปกรณ์ที่เชื่อมต่ออินเทอร์เน็ต เช่น กล้องวงจรปิด, อุปกรณ์สมาร์ทโฮม, ระบบ **OT (Operational Technology)**ในภาคอุตสาหกรรม, ระบบ **Automation System**, อุปกรณ์ **PLC**, ระบบ **SCADA**, ระบบ **Industrial Internet of Things**

2 ประเภทของภัยคุกคาม

9.Supply Chain Attacks (การโจมตีห่วงโซ่อุปทาน)

- การโจมตีที่มุ่งเป้าไปที่ผู้ให้บริการหรือซัพพลายเออร์เพื่อเข้าถึงระบบขององค์กรผ่านการโจมตีช่องโหว่ในห่วงโซ่อุปทาน



2 ประเภทของภัยคุกคาม

10.Cryptojacking (การใช้ทรัพยากรของผู้อื่นในการขุดคริปโต)

- การใช้ทรัพยากรของคอมพิวเตอร์ของผู้อื่นเพื่อขุดคริปโตเคอร์เรนซีโดยไม่ได้รับอนุญาต

3

กรณีศึกษาภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

MYSURACHET.COM

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

MYSURACHET.COM

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่1

SingHealth ถูกโจมตีทางไซเบอร์ กรกฎาคม **2018**
โจรกรรมข้อมูลผู้ป่วย **1.5**ล้านคน

SingHealth

Defining Tomorrow's Medicine

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

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

MYSURACHET.COM

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่1

SingHealth ถูกโจมตีทางไซเบอร์ กรกฎาคม **2018** โจรกรรมข้อมูลผู้ป่วย **1.5**ล้านคน

SingHealth
Defining Tomorrow's Medicine

รูปแบบการโจมตี

- **Hacker** ใช้ **Advanced Persistent Threat (APT)** โจมตี **Front-End Workstation** เพื่อเข้าสู่ฐานข้อมูลกลาง
- **Hacker** มีเจตนาขโมยข้อมูลนายกรัฐมนตรีสิงคโปร์ ('ลี เซียนลุง')

ผลกระทบ

ข้อมูลผู้ป่วยราว **1.5**ล้านคน ที่เคยเข้ารับบริการที่ **Specialist Outpatient Clinics** และ **Polyclinics** ของ **SingHealth** ตั้งแต่ **1** พฤษภาคม **2015** ถึง **4** กรกฎาคม **2018** ถูกขโมยข้อมูล **Demographic (ID Card,** ชื่อ ที่อยู่ เพศ วันเกิด**)**

- ถูกขโมยข้อมูลการสั่งยาจาก **OPD**

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

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

MYSURACHET.COM

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่1

ตัวอย่าง **Advanced Persistent Threat (APT)** แยกตามประเทศ

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
China	APT1-8,10-27,30-31,40-41	government, international financial organization, and aerospace and defense organizations, as well as high tech, construction and engineering, telecommunications, media, and insurance.
North Korea	APT37-38	industry verticals, including chemicals, electronics, manufacturing, aerospace, automotive, and healthcare.

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

MYSURACHET.COM

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่2

กฟภ. ถูกโจมตีทางไซเบอร์ด้วยมัลแวร์เรียกค่าไถ่
จนต้องปิดให้บริการระบบหลายวัน มิถุนายน 2020

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

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

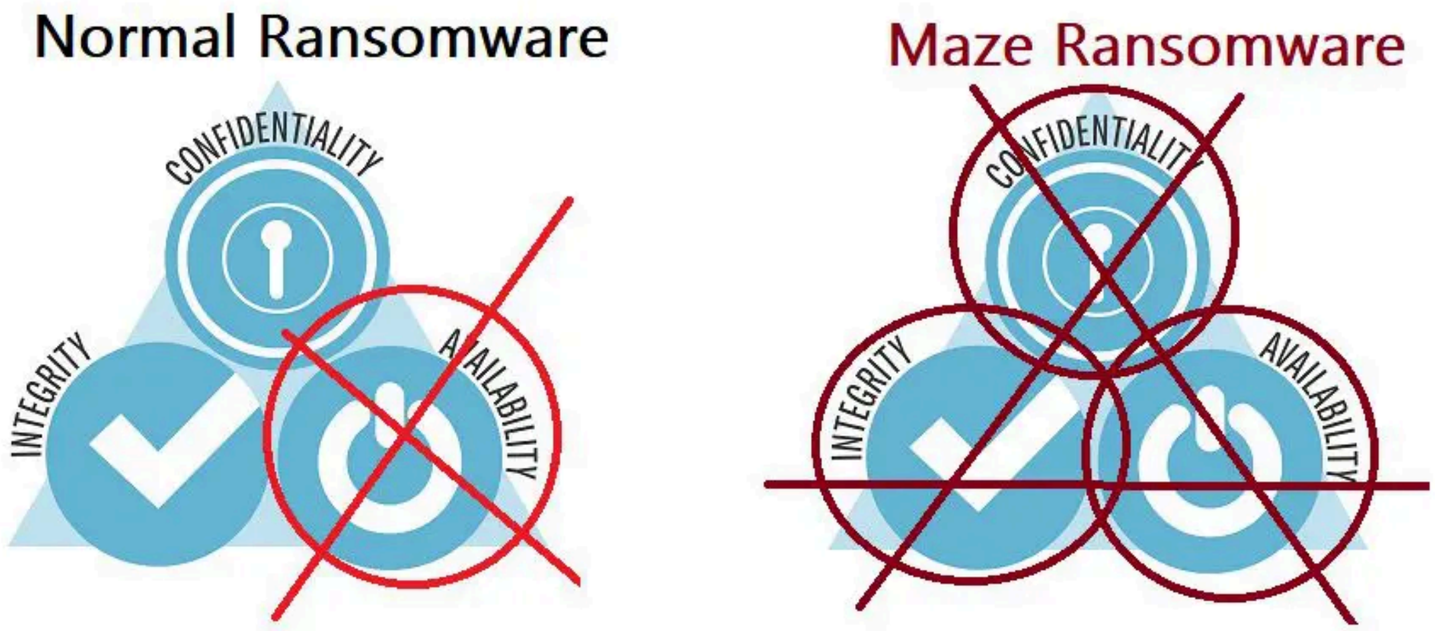
MYSURACHET.COM

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่2

กฟภ. ถูกโจมตีทางไซเบอร์ด้วยมัลแวร์เรียกค่าไถ่
จนต้องปิดให้บริการระบบหลายวัน มิถุนายน **2020**

Maze Ransomware

Maze Ransomware Triple Threat



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

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

MYSURACHET.COM

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่2

กฟภ. ถูกโจมตีทางไซเบอร์ด้วยมัลแวร์เรียกค่าไถ่ จนต้องปิดให้บริการระบบหลายวัน มิถุนายน 2020

ความเสียหาย

- ไฟล์ถูกบีบอัดและเข้ารหัสเพื่อเรียกค่าไถ่ไฟล์
- **Hacker** เผยแพร่ข้อมูลที่ขโมยมาในโลกออนไลน์

ประชาชนผู้รับบริการได้รับผลกระทบจากการโจมตีทางไซเบอร์ดังนี้

- ต้องปิดระบบเทคโนโลยีสารสนเทศบางส่วน ชั่วคราว
- ปิดบริการระบบชำระค่าบริการแบบออนไลน์ ชั่วคราว
- ปิดบริการแอปพลิเคชัน **PEA Smart Plus** ชั่วคราว

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

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

MYSURACHET.COM

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่3

JBS Foods ถูกโจมตีทางไซเบอร์ พฤษภาคม **2021**
REvil Ransomware เรียกค่าไถ่ไฟล์

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

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

MYSURACHET.COM

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่3

JBS Foods ถูกโจมตีทางไซเบอร์ พฤษภาคม 2021

JBS Foods ดำเนินธุรกิจเกี่ยวกับแปรรูปเนื้อสัตว์รายใหญ่ที่สุดในโลก ส่งออกเนื้อสัตว์จากบราซิลไปยังสหรัฐอเมริกา มีพนักงาน **230,000**คน ยอดขายมากกว่า **5,200**ล้าน**USD.**

รูปแบบการโจมตี

- **Hacker** ใช้ **REvil Ransomware** เพื่อล๊อคการเข้าถึงระบบของบริษัท เหตุการณ์นี้เกิดขึ้นกว่า **1** เดือน ทำให้ธุรกิจของ **JBS Foods** หยุดชะงัก

ผลกระทบ

- **JBS** ต้องปิดโรงงานหลายแห่งทั่วโลก
- การส่งสินค้าเนื้อสัตว์ล่าช้าหรือหยุดชะงัก
- ราคาเนื้อสัตว์ทั่วโลกเพิ่มสูงขึ้น
- **JBS** สูญเสียรายได้และเสียชื่อเสียง

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

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

MYSURACHET.COM

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่3

JBS Foods ถูกโจมตีทางไซเบอร์ พฤษภาคม **2021**

การตอบสนอง

- **JBS** ตัดสินใจจ่ายค่าไถ่ จำนวน **11** ล้าน**USD** ให้กับกลุ่ม **REvil**
- **JBS** ประสานไปยังหน่วยงานรัฐบาลหลายประเทศร่วมมือกันสืบสวนหาตัวผู้ก่อการ
- เหตุการณ์นี้สร้างความกังวลเกี่ยวกับความมั่นคงทางอาหาร

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

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

MYSURACHET.COM

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่4

CNA Financial ถูกโจมตีทางไซเบอร์ พฤษภาคม **2021**
REvil Ransomware เรียกค่าไถ่ไฟล์

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

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

MYSURACHET.COM

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่4

CNA Financial ถูกโจมตีทางไซเบอร์ พฤษภาคม **2021**

CNA เป็นบริษัทประกันภัยรายใหญ่ในสหรัฐอเมริกา มีพนักงาน **4,500**คน ยอดขายมากกว่า **7,000**ล้าน**USD.**

รูปแบบการโจมตี

- **Hacker** ใช้ **REvil Ransomware** เพื่อล๊อคการเข้าถึงระบบของบริษัท และข้อมูลสำคัญของบริษัท

ผลกระทบ

- **CNA Financial** ต้องหยุดการดำเนินงานบางส่วน
- ลูกค้าของ **CNA Financial** ไม่สามารถเข้าถึงข้อมูลประกันภัยของตน
- บริษัทต้องสูญเสียรายได้และเสียชื่อเสียง

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

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

MYSURACHET.COM

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่4

CNA Financial ถูกโจมตีทางไซเบอร์ พฤษภาคม **2021**

การตอบสนอง

- **CNA** ตัดสินใจจ่ายค่าไถ่ จำนวน **40** ล้าน**USD** ให้กับกลุ่ม **REvil**
- **CNA** ประสานไปยังหน่วยงานรัฐบาลหลายประเทศร่วมมือกันสืบสวนหาตัวผู้ก่อการ
- เหตุการณ์นี้สร้างความกังวลเกี่ยวกับความเชื่อมั่น และ ความมั่นคงทางการเงิน

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

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

MYSURACHET.COM

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่**5**

Kaseya VSA ถูกโจมตีทางไซเบอร์ กรกฎาคม **2021**

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

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

MYSURACHET.COM

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่5

Kaseya VSA ถูกโจมตีทางไซเบอร์ กรกฎาคม 2021

Kaseya VSA ดำเนินธุรกิจเกี่ยวกับให้บริการซอฟต์แวร์ควบคุมระบบระยะไกล **(Remote Monitoring and Management - RMM)**

กรกฎาคม **2021 Kaseya VSA** ถูก **Hacker** กลุ่ม **REvil** โจมตีช่องโหว่

รูปแบบการโจมตี

- แทรก **code** อันตรายในช่องโหว่ของ **Kaseya VSA** เพื่อควบคุมระบบคอมพิวเตอร์ของลูกค้าที่ใช้บริการ
- ใช้คอมพิวเตอร์ของลูกค้าที่ถูกควบคุมกระจาย **REvil Ransomware** เข้ารหัสไฟล์ข้อมูลเพื่อเรียกค่าไถ่

การตอบสนอง

- เมื่อถูกโจมตีทาง **Kaseya** ปิดระบบ **Server** ของตัวเองทั้งหมด
- แจ้งให้ลูกค้าที่ใช้งาน **VSA** แบบ **On-Premise** ปิด **Server** ด้วยเช่นกัน

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

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

MYSURACHET.COM

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่5

Kaseya VSA ถูกโจมตีทางไซเบอร์ กรกฎาคม 2021

ผลกระทบ

- ส่งผลกระทบต่อองค์กรทั่วโลกมากกว่า **1,000** แห่ง ถูกเข้ารหัสไฟล์
- สร้างความเสียหายทางการเงินและชื่อเสียงของ **Kaseya VSA** และองค์กรที่ถูกโจมตี

การตอบสนอง

- เมื่อถูกโจมตีทาง **Kaseya** ปิดระบบ **Server** ของตัวเองทั้งหมด
- แจ้งให้ลูกค้าที่ใช้งาน **Kaseya** แบบ **On-Premise** ปิด **Server** ด้วยเช่นกัน
- **Kaseya** ไม่ได้จ่ายค่าไถ่ไฟล์ สามารถถอดรหัสและกู้คืนระบบได้
- **Kaseya update software** เพื่อแก้ไขช่องโหว่
- **Kaseya** ประสานไปยังหน่วยงานของรัฐบาลหลายประเทศ เพื่อร่วมมือกันสืบสวนหาตัวผู้ก่อการในครั้งนี้

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

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

MYSURACHET.COM

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่6

ข้อมูลคนไข้ในระบบสาธารณสุขรั้วไหล กันยายน **2021**

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

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

MYSURACHET.COM

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่6

ข้อมูลคนไข้ในระบบสาธารณสุขรั้วไหล กันยายน 2021

วันที่ 6 กันยายน 2564 มีรายงานข้อมูลพื้นฐานของคนไข้ในระบบสาธารณสุขรั้วไหลกว่า ล้านรายชื่อ

รูปแบบการโจมตี

- แฮกเกอร์โจมตีระบบฐานข้อมูลของโรงพยาบาล เป็นไปได้ทั้งรัฐ-เอกชน
- ขโมยข้อมูลคนไข้กว่า ล้านรายชื่อ
- ข้อมูลที่ถูกขโมย ได้แก่ ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ วันเดือนปีเกิด ชื่อแพทย์เจ้าของไข้ และชื่อโรงพยาบาล

ผลกระทบ

- ผู้ป่วยมีความเสี่ยงต่อการถูกแฮกข้อมูลส่วนบุคคล
- อาจถูกนำไปใช้เพื่อหลอกลวง หรือทำธุรกรรมที่ผิดกฎหมาย
- เสียชื่อเสียงต่อระบบสาธารณสุข
- สร้างความกังวลให้กับประชาชน

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

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

MYSURACHET.COM

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่6

ข้อมูลคนไข้ในระบบสาธารณสุขรั้วไหล กันยายน 2021

วันที่ 6 กันยายน 2564 มีรายงานข้อมูลพื้นฐานของคนไข้ในระบบสาธารณสุขรั้วไหลกว่าล้านรายชื่อ

การตอบสนอง

- สธ.-สกมช. ยอมรับว่ามีข้อมูลรั่วไหล เป็นไปได้ทั้งรัฐ-เอกชน
- สั่งปิดระบบฐานข้อมูลที่ถูกโจมตี
- แจ้งความดำเนินคดีกับผู้กระทำผิด
- ตั้งคณะกรรมการสอบสวนหาสาเหตุ
- เตรียมเยียวยาผู้เสียหาย
- กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ร่วมตรวจสอบช่องโหว่
- เตรียมเสนอมาตรการป้องกันการโจมตีทางไซเบอร์ในอนาคต

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

3 ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

MYSURACHET.COM

กรณีศึกษาความผิดพลาดของซอฟต์แวร์

CrowdStrike Software Glitch 19 กรกฎาคม **2024**

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

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

MYSURACHET.COM

กรณีศึกษาความผิดพลาดของซอฟต์แวร์

CrowdStrike Software Glitch 19 กรกฎาคม **2024**

สาเหตุ

- เกิดจาก ข้อผิดพลาดของซอฟต์แวร์ **CrowdStrike Falcon** ซึ่งเป็นแพลตฟอร์มรักษาความปลอดภัย ไม่ได้เกิดจากการโจมตีทางไซเบอร์จากภายนอก ทาง **CrowdStrike** ระบุว่าสาเหตุเกิดจาก "การอัปเดตซอฟต์แวร์ที่ผิดพลาด" ส่งผลกระทบต่อระบบของลูกค้าทั่วโลก

ผลกระทบ

- ผู้ใช้ **CrowdStrike** หลายล้านคนทั่วโลกประสบปัญหาระบบล่ม ไม่สามารถใช้งานแพลตฟอร์มรักษาความปลอดภัย ส่งผลกระทบต่อธุรกิจ องค์กร และหน่วยงานต่างๆ เป็นวงกว้าง บางองค์กรต้องหยุดการดำเนินงานชั่วคราว
- เสียหายทางการเงินจากเหตุการณ์ครั้งนี้ **some businesses** สูญเสียรายได้ เสียโอกาสทางธุรกิจ และต้องเสียค่าใช้จ่ายเพิ่มเติมในการแก้ไขปัญหา
- ส่งผลต่อชื่อเสียงของ **CrowdStrike** ความน่าเชื่อถือของบริษัทลดลง ลูกค้าสูญเสียความมั่นใจ อาจสูญเสียลูกค้าบางส่วน

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