Updating Cybersecurity Regulations

for the Next Wave of Health Threats

วันที่ 25 กันยายน 2568 เวลา 09.30 – 10.00 น.
ณ ห้อง Mayfair Ballroom B (ชั้น11) โรงแรมเดอะเบอร์เคลีย์ ประตูน้ำ กรุงเทพฯ

Air Vice Marshal Jadet Khuhakongkit

Assistant Secretary General & Deputy Director of ThaiCERT

ประสบการณ์ด้านไซเบอร์ที่เกี่ยวข้อง

ยุทธศาสตร์ทหารด้านสงครามไซเบอร์กองทัพไทย พ.ศ.2558 • หลักนิยมการปฏิบัติการร่วมทางไซเบอร์กองทัพไทย พ.ศ.2561 • นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ กองบัญชาการกองทัพไทย พ.ศ.2564 • การฝึกทางไซเบอร์ กองบัญชาการกองทัพไทย พ.ศ.2560, 2562 • การฝึกร่วมทางไซเบอร์ กองทัพไทย พ.ศ.2562-2563 • การแข่งขันทักษะทางไซเบอร์ในระดับ รร.ทหาร-ตำรวจ พ.ศ.2562-2563 • การแข่งขันทักษะทางไซเบอร์ กองทัพไทย พ.ศ.2562-2563 • ที่ปรึกษาในการจัดตั้ง สกมช. • ประกาศ กมช. เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศฯ พ.ศ.2564 • ประกาศ กกม. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ฯ พ.ศ.2564 • การฝึก Thailand's National Cyber Exercise 2022, 2023,2024

การศึกษา

โรงเรียนเตรียมทหาร • โรงเรียนนายเรืออากาศ • สถาบันบัณฑิตพัฒนบริหารศาสตร์ • Squadron Officer School (USA) • Air Force Command and Staff Course (China) • Harvard Kennedy School (USA)

CERTIFICATES

CQI | IRCA LEADING QUALITY SINCE 1919

พลอากาศตรี จเด็ด คูหะก้องกิจ

ผู้ช่วยเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เกี่ยวกับ สกมช.

วิสัยทัศน์ VISION

เป็นผู้นำในการขับเคลื่อนในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศที่มีประสิทธิภาพ พร้อมตอบสนองต่อภัยคุกคามไซเบอร์ทุกมิติ

พันธกิจ MISSIONS

เสนอแนะนโยบาย แผน ยุทธศาสตร์ และปรับปรุงกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งกำหนดแนวทาง มาตรฐาน มาตรการที่เกี่ยวข้องให้สอดคล้องกับสถานการณ์ทั้งในปัจจุบันและอนาคต

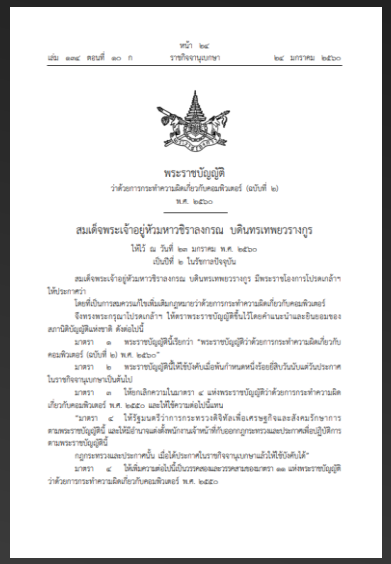
กำกับ ดูแล เฝ้าระวัง ติดตาม วิเคราะห์ ประมวลผล แจ้งเตือน และปฏิบัติการเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

เป็นศูนย์กลางในการประสานความร่วมมือ รวมทั้งส่งเสริม สนับสนุน และช่วยเหลือหน่วยงานภาครัฐและเอกชนทั้งในประเทศและต่างประเทศเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

เผยแพร่ความรู้ความเข้าใจ และสนับสนุนการพัฒนาบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

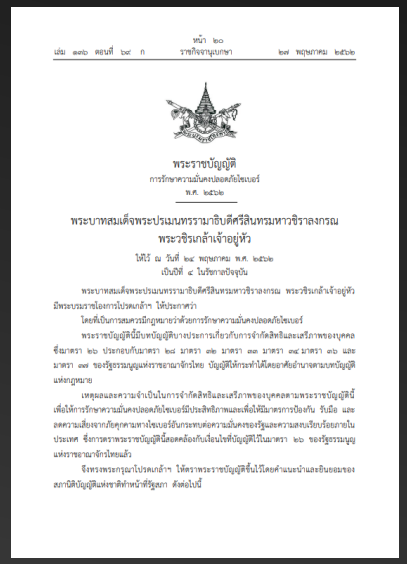
ประเทศไทยได้ออกกฎหมายและกำหนดหน่วยงานสำคัญหลายฉบับเพื่อเน้นการรักษาความมั่นคงทางไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล

SECURE & TRUSTED ENVIRONMENT



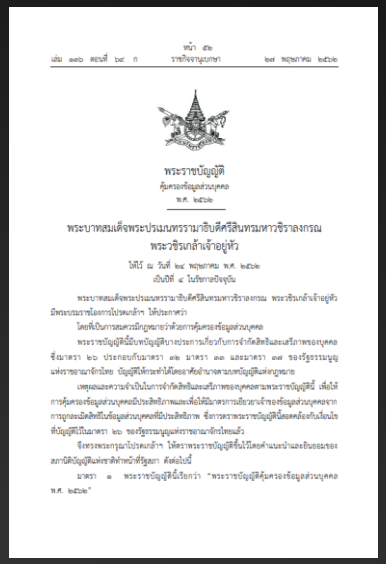
พระราชบัญญัติ
ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒)
พ.ศ. ๒๕๖๐

สมเด็จพระเจ้าอยู่หัวมหาวชิราลงกรณ บดินทรเทพยวรางกูร



พระราชบัญญัติ
การรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว



พระราชบัญญัติ
คุ้มครองข้อมูลส่วนบุคคล
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

pdpc สคส.
- มาตรการคุ้มครองข้อมูลส่วนบุคคล
- สิทธิเจ้าของข้อมูล
- ไกล่เกลี่ย ระงับข้อพิพาท

กำหนดความผิดและบทลงโทษ
- ความผิดที่ทำต่อข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์โดยตรง

NCSA สกมช
- Incident Response
- Critical Information Infrastructure Protection

หมายเหตุ : ระดับวิกฤตเป็นอำนาจหน้าที่ สำนักงานสภาความมั่นคงแห่งชาติ (สมช.)

พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และ 2560

กฎหมายฉบับนี้ครอบคลุมการเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต การแฮ็ก และการเผยแพร่ข้อมูลเท็จ เป็นกฎหมายพื้นฐานสำหรับการดำเนินคดีกับผู้กระทำผิดทางไซเบอร์

พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

กฎหมายที่มีเป้าหมายเพื่อความมั่นคงแห่งชาติในโลกไซเบอร์ กฎหมายฉบับนี้บังคับให้องค์กรในภาคส่วนสำคัญ (เช่น การเงิน พลังงาน คมนาคม และสุขภาพ) ต้องดำเนินมาตรการป้องกันโครงสร้างพื้นฐานสารสนเทศที่สำคัญ (Critical Information Infrastructure - CII) และให้สิทธิแก่รัฐบาลในการตรวจสอบและจัดการเหตุการณ์ทางไซเบอร์

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

มีเป้าหมายในการคุ้มครองข้อมูลส่วนบุคคลของประชาชน โดยกำหนดหลักเกณฑ์ในการเก็บรวบรวม ใช้ และจัดเก็บข้อมูล พร้อมทั้งให้สิทธิกับเจ้าของข้อมูลในการควบคุมข้อมูลส่วนตัว และกำหนดบทลงโทษกรณีละเมิด

"There are only two types of companies:
those that have been hacked,
and those that will be."

Robert Mueller
FBI Director, 2001-2013

The World's Current Threat Landscape
Public Health Sector

2024

1. **Ransomware**
2. Phishing
3. Compromised Credentials
4. **3rd Party** Credentials
5. **Data Breaches**

2025

1. **Ransomware** Deployment
2. **3rd Party** Breaches
3. **Data Breaches**
4. Supply Chain Attacks
5. Zero-Day Exploits

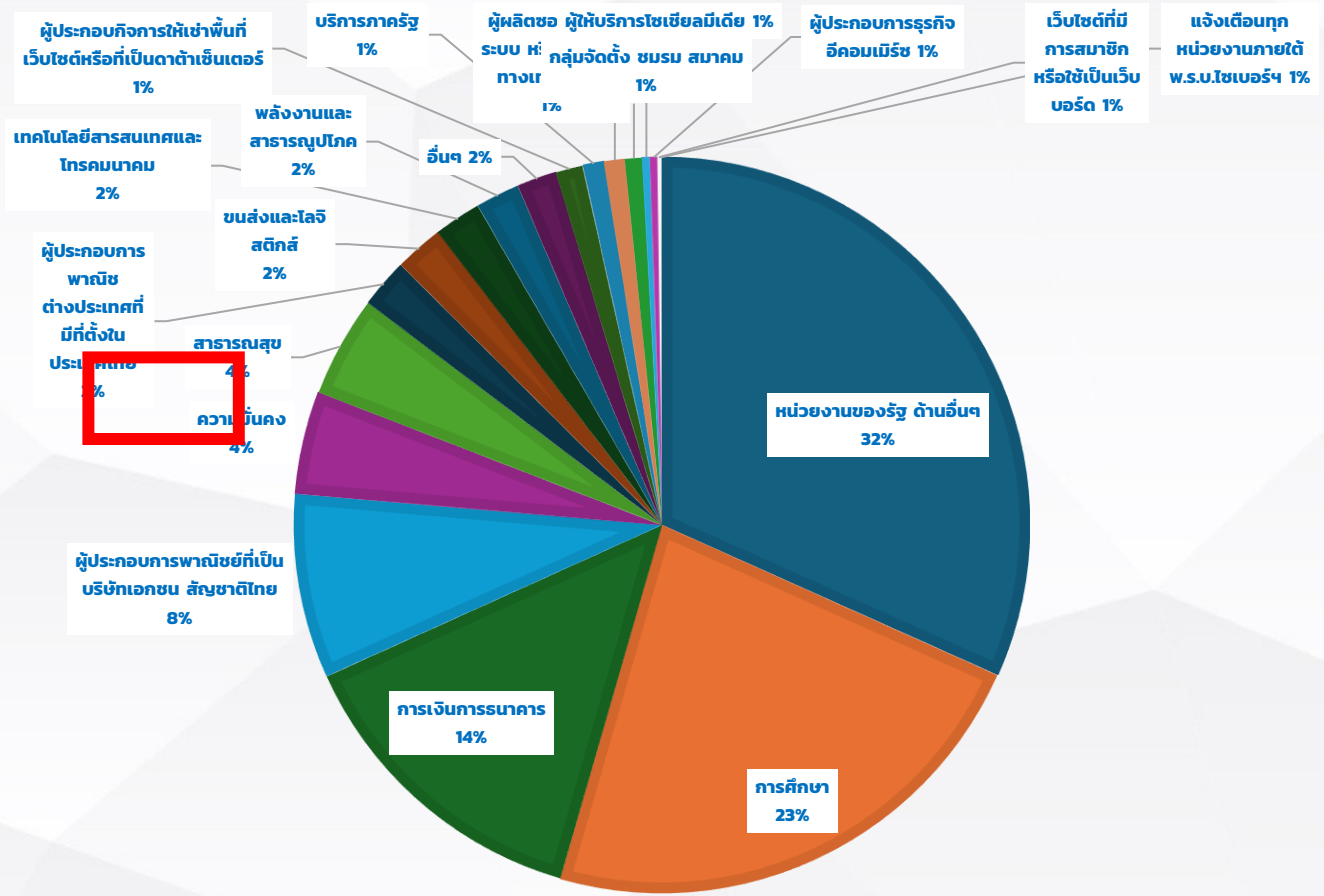
Source: Health-ISAC 2025-Annual-Threat-Report
Health-ISAC_2025-Annual-Threat-Report.pdf

สถิติภัยคุกคามทางไซเบอร์ภาคสาธารณสุข

จากการดำเนินการเฝ้าระวังด้านความมั่นคงปลอดภัยทางไซเบอร์ สามารถจัดจำแนกประเภทของภารกิจหน่วยงาน ได้ดังนี้

หน่วยงานของรัฐ ด้านอื่นๆ	937
การศึกษา	673
การเงินการธนาคาร	407
ผู้ประกอบการพาณิชย์ที่เป็นบริษัทเอกชน สัญชาติไทย	240
ความมั่นคง	133
สาธารณสุข	131
ผู้ประกอบการพาณิชต่างประเทศที่มีที่ตั้งในประเทศไทย	64
ขนส่งและโลจิสติกส์	64
เทคโนโลยีสารสนเทศและโทรคมนาคม	61
พลังงานและสาธารณูปโภค	57
อื่นๆ	52
ผู้ประกอบกิจการให้เช่าพื้นที่เว็บไซต์หรือที่เป็นดาต้าเซ็นเตอร์	35
บริการภาครัฐ	28
ผู้ผลิตซอฟต์แวร์ ระบบ หรืออุปกรณ์ทางเทคโนโลยี	27
กลุ่มจัดตั้ง ชมรม สมาคม	22
ผู้ให้บริการโซเชียลมีเดีย	10
ผู้ประกอบการธุรกิจอีคอมเมิร์ซ	9
เว็บไซต์ที่มีการสมาชิกหรือใช้เป็นเว็บบอร์ด	4
แจ้งเตือนทุกหน่วยงานภายใต้ พ.ร.บ.ไซเบอร์ฯ	2

- 75 เหตุการณ์ ในปี 2024
- 131 เหตุการณ์ตั้งแต่วันที่ 1 มกราคมถึง 31 สิงหาคม 2025



https://www.ncsa.or.th/news/47eeaf5b61373614bc00004b?category=news

ทำไมภาคสาธารณสุขจึงตกเป็นเป้าหมาย

จำนวนโรงพยาบาล: > 1,400 แห่งทั่วประเทศ

- ระบบสารสนเทศหลายระบบ เช่น ระบบ Hospital Information System (HIS), ระบบสารสนเทศกรมควบคุมโรค (DPIS), ระบบสารสนเทศบุคลากรสาธารณสุข (HROPS), ระบบสารสนเทศทรัพยากรสุขภาพ (GIS Health), ระบบนัดหมาย, ระบบเวชระเบียนอิเล็กทรอนิกส์ ฯลฯ

ข้อมูลที่จัดเก็บ:

- ข้อมูลส่วนบุคคล (PII): ชื่อ, เลขบัตรประชาชน, เบอร์โทร, ที่อยู่
- ข้อมูลสุขภาพ (PHI): ประวัติการรักษา, ผลตรวจ, ยาที่ใช้, การวินิจฉัย

Source: สถาบันรับรองคุณภาพสถานพยาบาล (องค์การมหาชน)

ไทย ติด 1 ใน 10 ประเทศที่มีข้อมูลรั่วไหลบนดาร์กเว็บมากที่สุด

ไทย ติด 1 ใน 10 ประเทศที่มีข้อมูลรั่วไหลบนดาร์กเว็บมากที่สุด
รายงาน High-Tech Crime Trends โดย Group-IB พบว่าปี 2024 พบข้อมูลรั่วไหลสู่สาธารณะ 1,107 เคสทั่วโลก ทำให้ข้อมูลผู้ใช้มากกว่า 6.4 พันล้านรายการถูกบุกรุก โดยในบรรดาข้อมูลที่รั่วไหล อีเมล หมายเลขโทรศัพท์ และรหัสผ่านมีความเสี่ยงสูงสุด เนื่องจากผู้คุกคามสามารถใช้ข้อมูลตรงนี้โจมตีได้
จากข้อมูลที่รั่วไหลทั้งหมด กว่า 6.5 พันล้านรายการ เป็นข้อมูลที่มีอีเมลเป็นส่วนประกอบ ในขณะที่ 3.3 พันล้านรายการมีหมายเลขโทรศัพท์เป็นส่วนประกอบ และรหัสผ่านที่ถูกเปิดเผยกว่า 460 ล้านรายการ

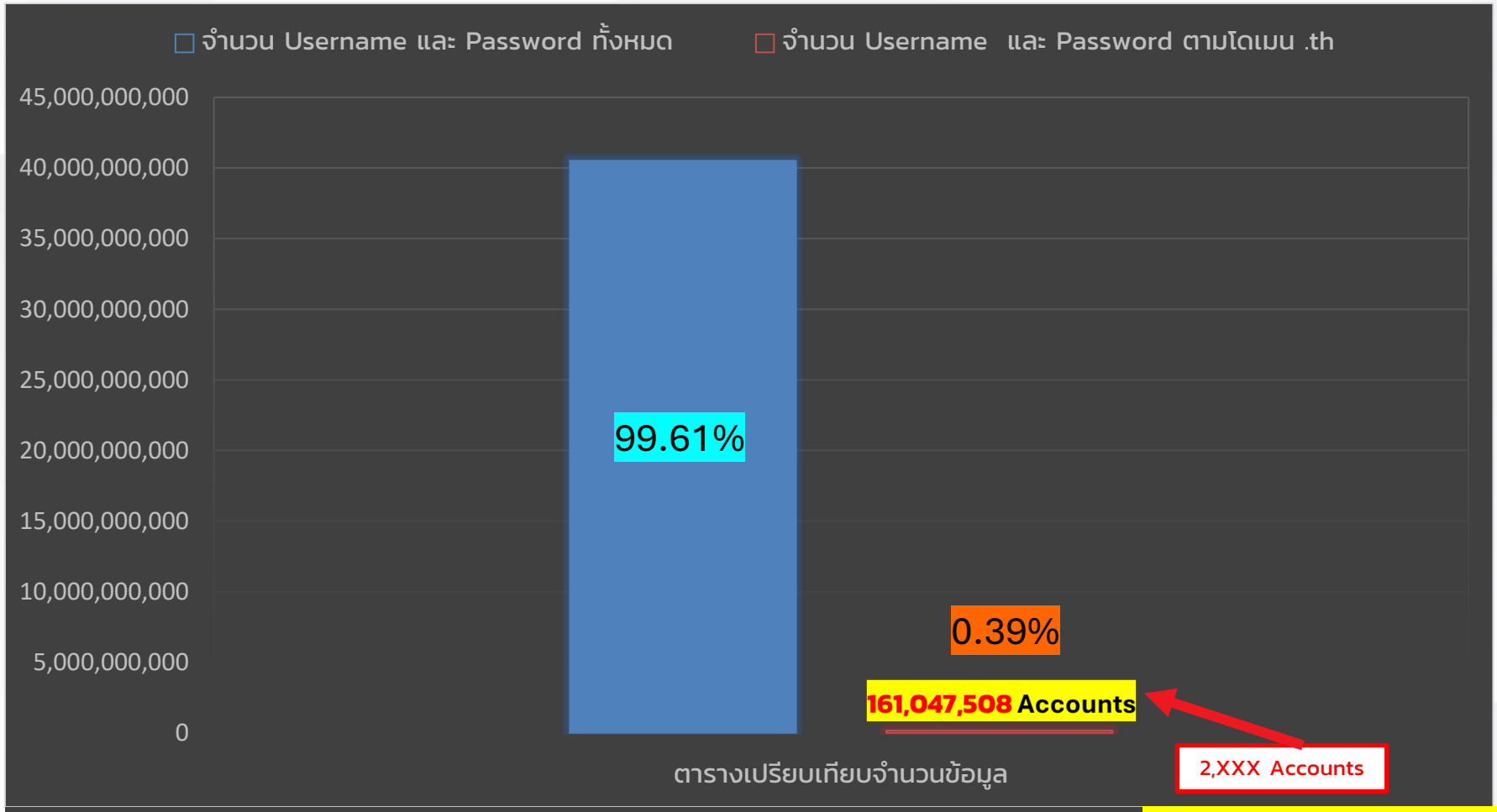
.

ซึ่งอินโดนีเซีย และไทย ติด 1 ใน 10 ตลาดทั่วโลกที่ได้รับผลกระทบจากการรั่วไหลของข้อมูลบนดาร์กเว็บมากที่สุด

https://www.facebook.com/blognone/posts/pfbid0sZkZUirixNiCrSaNe1AfY625MWqLc18k6BR5CJB66mGNGgRT2C71wDbbvtg5Asgwl?rdid=ZrJHRGak5eOgdbRq#

สถิติภัยคุกคามทางไซเบอร์Credential Leaks Trends

ตารางเปรียบเทียบจำนวนข้อมูล




```
Credential Leak all
batch 1 : 11298979814
batch 2 : 11194362311
batch 3 : 12023374050
batch 4 : 5995918056
all sum = 40,512,634,231 records

Only Top Level Domain .th
batch 1 : 50547776
batch 2 : 42239381
batch 3 : 41541102
batch 4 : 26719249
all th sum = 161,047,508 records
```

ค่าจำนวนของ credential leak ทั้งหมดจะได้มาจากแบ่งการทำงานเป็น 4 รอบ โดยแต่ละรอบจะแยกเป็นกลุ่ม(batch) แต่ละกลุ่มจะมีไฟล์ที่ไม่ซ้ำกัน เมื่อคำนวณเสร็จ
จะนำค่าทั้งหมดมารวมกัน และออกมาเป็นจำนวนของ credential leak ทั้งหมด

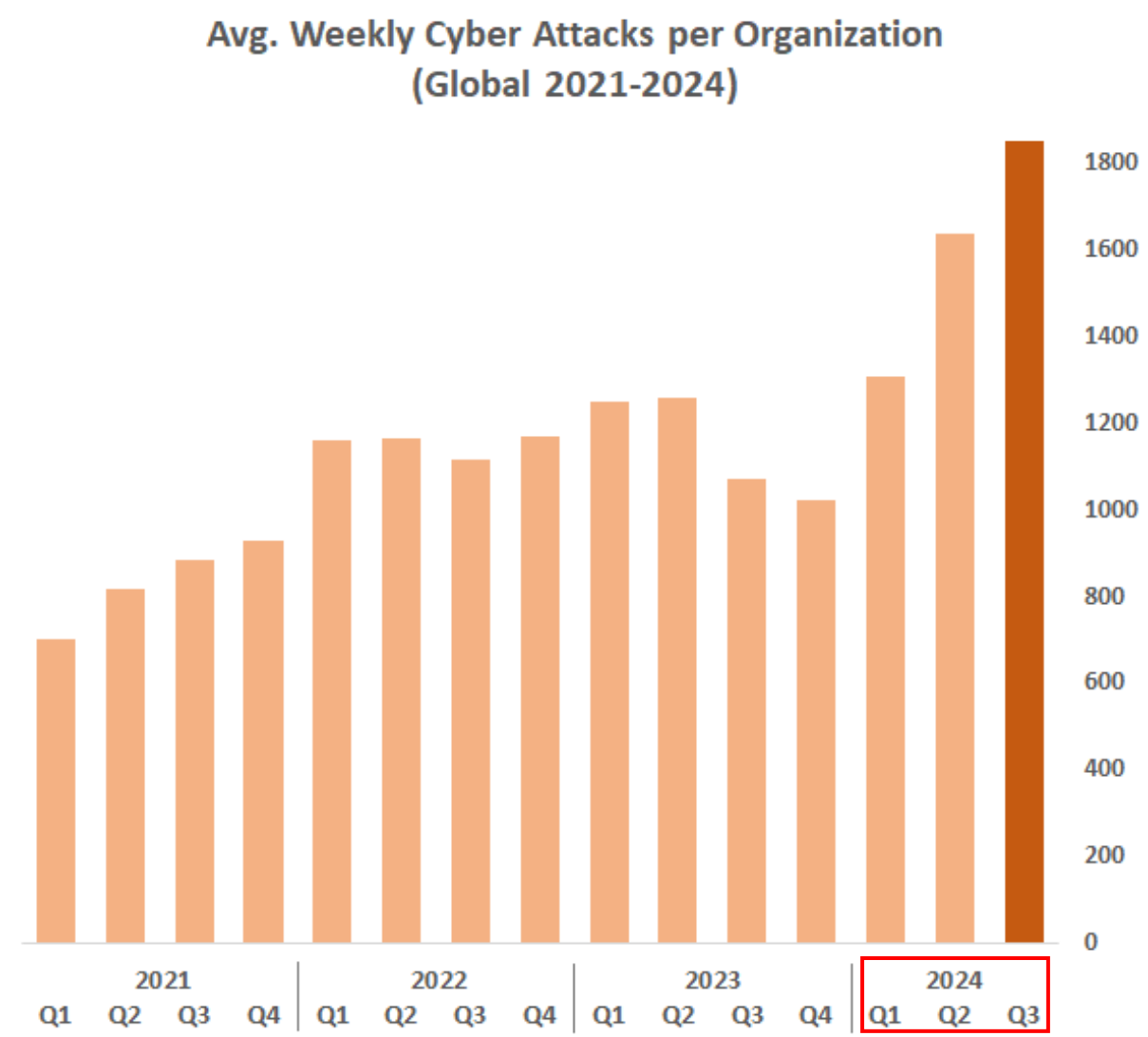
จำนวนไฟล์ทั้งหมด 6,209 ไฟล์

จำนวน Username และ Password ทั้งหมด 40,512,634,231 Accounts

จำนวน Username และ Password ตามโดเมน .th 161,047,508 Accounts

จำนวนข้อมูลที่รั่วไหลในปี 2025 **มากกว่าปี 2024 ประมาณ 80,524 เท่า**

2024: การโจมตีทางไซเบอร์ทั่วโลกพุ่งสูงขึ้น 75%



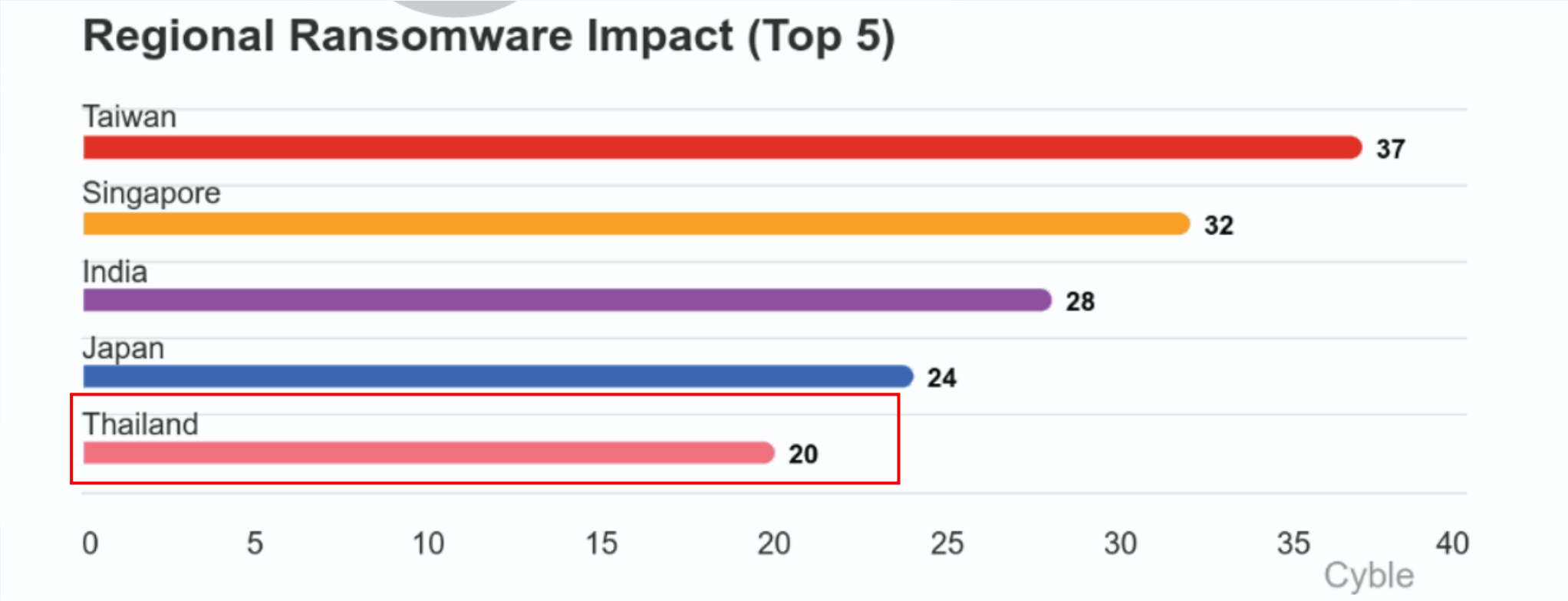
- **จำนวนการโจมตีที่พุ่งสูงเป็นประวัติการณ์:** ในไตรมาสที่ 3 ปี 2567 มีการบันทึกการโจมตีทางไซเบอร์เฉลี่ย 1,876 ครั้งต่อองค์กร ซึ่งเพิ่มขึ้น 75% เมื่อเทียบกับช่วงเวลาเดียวกันในปี 2566 และเพิ่มขึ้น 15% เมื่อเทียบกับไตรมาสก่อนหน้า
- **การแยกย่อยตามอุตสาหกรรม:** ภาคการศึกษา/การวิจัยเป็นเป้าหมายมากที่สุด โดยมีการโจมตีรายสัปดาห์จำนวน 3,828 ครั้ง รองลงมาคือภาครัฐบาล/ทหาร และภาคการดูแลสุขภาพ โดยมีการโจมตี 2,553 และ 2,434 ครั้ง ตามลำดับ
- **ระดับภูมิภาค:** แอฟริกาเผชิญกับการโจมตีเฉลี่ยสูงสุดที่ 3,370 ครั้งต่อสัปดาห์ (+90% เมื่อเทียบกับปีที่แล้ว) ในขณะที่ยุโรปและละตินอเมริกาก็พบว่าเพิ่มขึ้นอย่างมีนัยสำคัญเช่นกัน
- **Ransomware:** ภัยคุกคามที่คงอยู่: มีรายงานเหตุการณ์ ransomware มากกว่า 1,230 ครั้ง โดยอเมริกาเหนือได้รับผลกระทบมากที่สุด (57% ของเหตุการณ์) รองลงมาคือยุโรป (24%)

https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/

World Top 10 industry attacked by Ransomware group

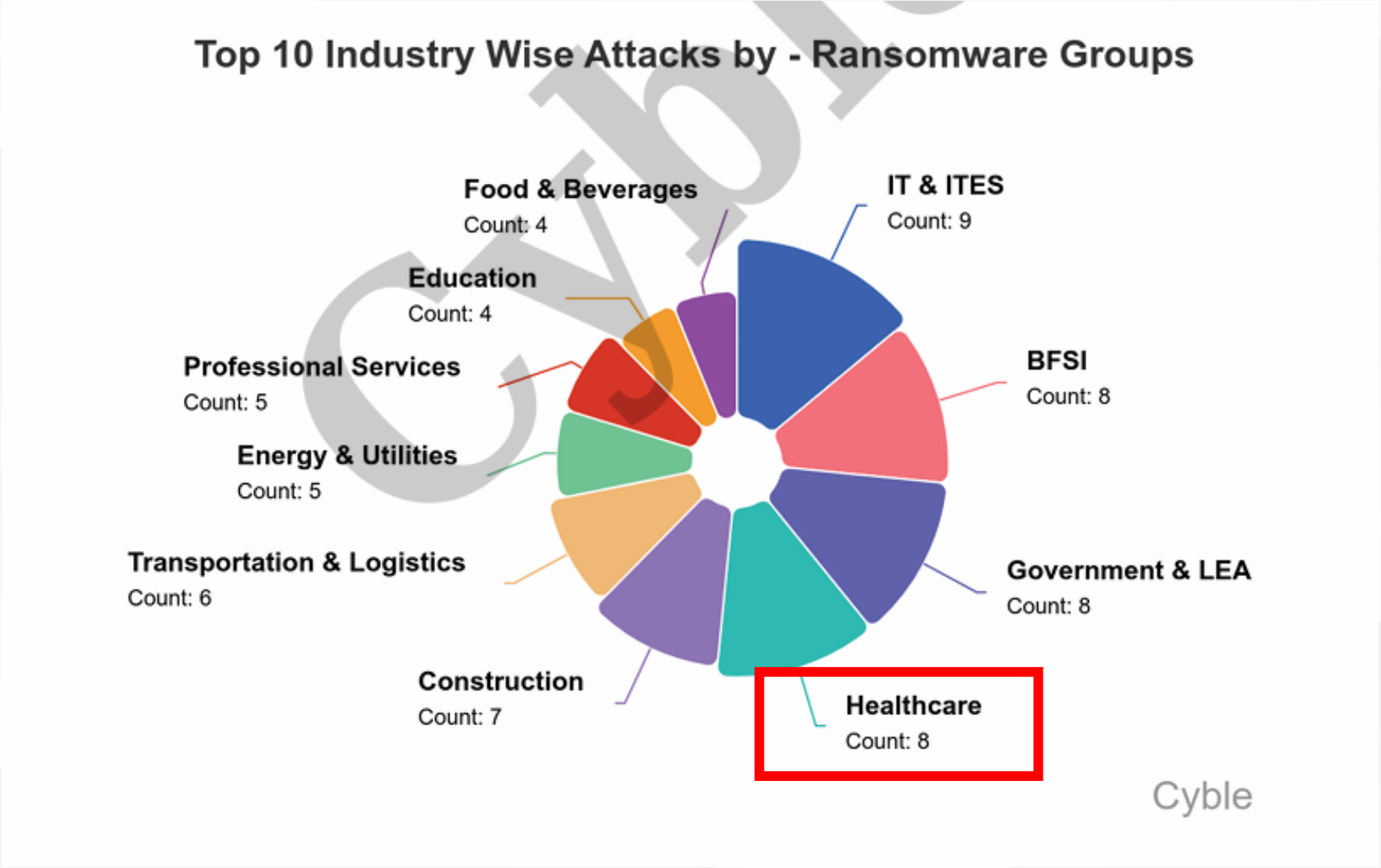
APAC

In Asia and Pacific, Taiwan was the most targeted country with 37 recorded incidents followed by Singapore (32), India (28), and Japan (24). The geopolitical tension in the South-East Asian countries seems to being leveraged by opportune ransomware actorsin this region.



Source: Cyble Global Ransomware Threat Landscape Report - H1-2025

World Top 10 industry attacked by Ransomware group

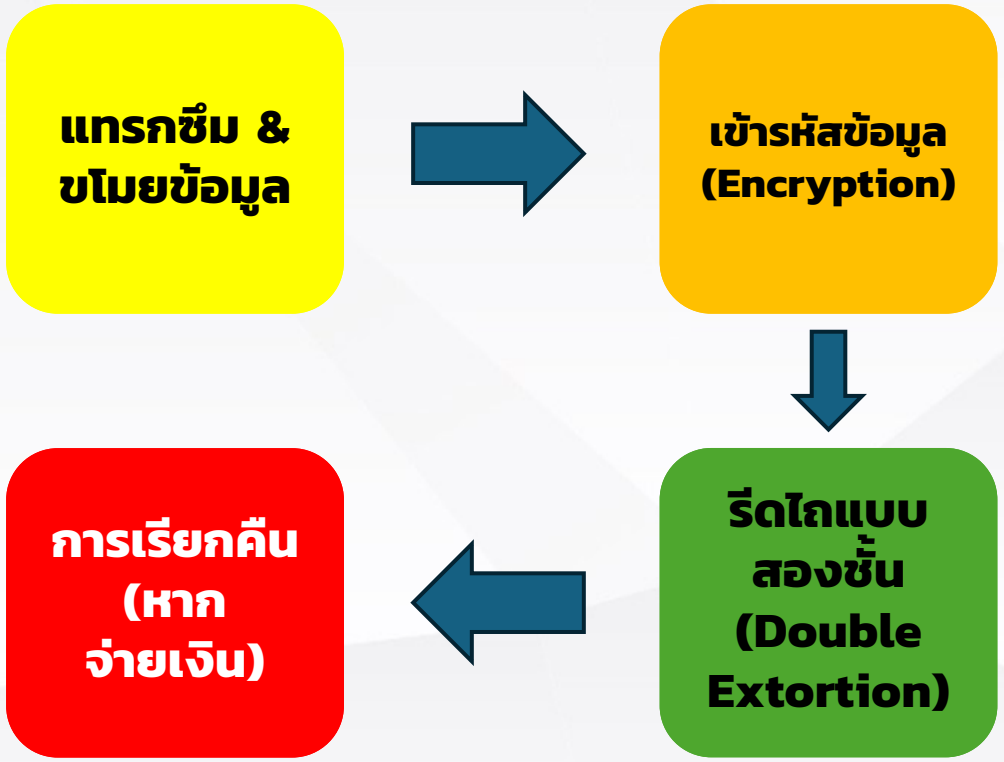


Source: Cyble Global Ransomware Threat Landscape Report - H1-2025

แรนซัมแวร์ 2.0 (Ransomware 2.0)

Ransomware 2.0 คือวิวัฒนาการของแรนซัมแวร์ยุคใหม่ที่ไม่ได้แค่เข้ารหัสข้อมูลเพื่อเรียกค่าไถ่ แต่ยังขโมยข้อมูลก่อน เพื่อ **รีดไถสองชั้น (Double Extortion)** เพิ่มแรงกดดันต่อเหยื่อ และเพิ่มผลกำไรให้ผู้โจมตี

กลไกการทำงานของ Ransomware 2.0 (4 ระยะ)



https://www.secoda.co/learn/data-trends-ransomware-2-0

แนวโน้มสำคัญของ Ransomware 2.0

1. **Double- Triple Extortion** – รีดไถข้อมูลก่อนล็อกไฟล์
2. **โจมตีระบบ Cloud & SaaS** – เป้าหมายใหม่ขององค์กรยุคดิจิทัล
3. **เจาะห่วงโซ่อุปทาน (Supply Chain Attack)** – ฝังมัลแวร์ในซอฟต์แวร์จาก Third-Party
4. **RaaS (Ransomware-as-a-Service)** – เปิดตลาดมืดให้คนทั่วไปเข้าถึงเครื่องมือแรนซัมแวร์
5. **โจมตีแบบเจาะจงเป้าหมาย (Targeted Attacks)** – ศึกษาเหยื่อ ปรับแต่งกลยุทธ์เฉพาะ
6. **ระบบอัตโนมัติขั้นสูง** – ใช้ AI/Automation ในการแพร่กระจายและหลบเลี่ยง
7. **การร่วมมือระหว่างกลุ่มแฮกเกอร์** – สร้างเครือข่ายอาชญากรรมไซเบอร์

วิธีการป้องกันภัยคุกคามทางไซเบอร์

การป้องกัน Ransomware,2.0 และภัยคุกคามทางไซเบอร์อื่นๆ ต้องใช้แนวทางแบบองค์รวม การฝึกอบรมด้านความปลอดภัยทางไซเบอร์เป็นประจำสำหรับพนักงานเพื่อให้สามารถระบุความพยายามฟิชชิ่งได้ การตรวจสอบให้แน่ใจว่าซอฟต์แวร์ได้รับการอัปเดตด้วยแพตช์ล่าสุด การนำการควบคุมการเข้าถึงที่มีประสิทธิภาพมาใช้ และการปรับใช้การป้องกันปลายทางขั้นสูง ถือเป็นกลยุทธ์พื้นฐาน นอกจากนี้ การตรวจหาภัยคุกคามเชิงรุก
การวางแผนการตอบสนองต่อเหตุการณ์ และการตรวจสอบอย่างต่อเนื่อง ถือเป็นองค์ประกอบสำคัญของแนวทางด้านความปลอดภัยทางไซเบอร์ที่ยืดหยุ่น

การรับมือ

- ใช้แนวคิด **Zero Trust**
- อัปเดตระบบและแพตช์ช่องโหว่สม่ำเสมอ
- สำรองข้อมูลแยกจากระบบหลัก (Offline/Immutable Backup)
- ติดตั้ง EDR/XDR และระบบตรวจจับภัยคุกคาม
- ฝึกอบรมพนักงานเรื่องฟิชชิ่งและภัยทางไซเบอร์
- จัดทำและซ้อมแผนรับมือเหตุการณ์ (Incident Response Plan)

การหลอกลวง (Phishing)

การหลอกลวง (Phishing) เป็นการหลอกลวงของผู้โจมตีผ่านทางอีเมล หรือเว็บไซต์ที่คล้ายกับของจริง เพื่อให้เหยื่อเป้าหมาย กรอกข้อมูลส่วนตัวลงไป โดยส่วนใหญ่จะเป็นข้อมูลเกี่ยวกับการทำธุรกรรมกับธนาคาร หรือที่เกี่ยวข้องกับการใช้ข้อมูลส่วนตัว

วิธีสังเกตว่าอีเมลหรือเว็บไซต์เป็น phishing สังเกตุดังนี้

ตรวจสอบที่อยู่อีเมลว่าใครเป็นคนส่ง เป็นอีเมลที่รู้จักหรือไม่ หากพบว่าเป็นอีเมลที่ไม่รู้แหล่งที่มา ไม่ควรคลิกลิงก์ หรือเปิดไฟล์แนบในอีเมลนั้น

ตรวจสอบ URL ของเว็บไซต์นั้นว่าเป็น URL ของเว็บไซต์ทางการหรือไม่ หากไม่ใช่ ไม่ควรกรอกข้อมูลลงในเว็บไซต์นั้น

วิธีป้องกันการโจมตีแบบ Phishing

- **ตรวจสอบอีเมลอย่างละเอียด** – อย่าเปิดลิงก์หรือดาวน์โหลดไฟล์แนบจากอีเมลที่น่าสงสัย
- **ใช้ Multi-Factor Authentication (MFA)** – แม้รหัสผ่านรั่วไหลก็ยังมีการป้องกันเพิ่มเติม
- **หลีกเลี่ยงการให้ข้อมูลทางโทรศัพท์หรือ SMS** – ธนาคารและองค์กรจริงจะไม่ขอข้อมูลผ่านช่องทางเหล่านี้
- **อัปเดตซอฟต์แวร์และแอนตี้ไวรัสสม่ำเสมอ** – เพื่อป้องกันมัลแวร์ที่อาจมาพร้อมกับ Phishing
- **ฝึกอบรมพนักงานเกี่ยวกับ Social Engineering** – ลดโอกาสที่องค์กรจะถูกโจมตี

Phishing เป็นหนึ่งในภัยคุกคามที่พบได้บ่อยที่สุดและยังคงพัฒนาอย่างต่อเนื่อง การเพิ่มความระมัดระวังและใช้มาตรการรักษาความปลอดภัยที่เหมาะสมจะช่วยลดความเสี่ยงของการถูกโจมตีได้

รู้หรือไม่ องค์กรไทยเกือบ 58% เคยโดนภัยคุกคามจาก AI

บริษัทวิจัย IDC เผยผลสำรวจหัวข้อ “State of Cybersecurity in APJC: From Constant Risk to Platform-Driven Resilience” พบว่า **เกือบ 58% ขององค์กรในไทยเคยเผชิญภัยคุกคามที่ขับเคลื่อนด้วย AI** โดยเฉพาะการโจมตีที่ใช้เทคนิค Deepfake, Phishing อัจฉริยะ และการวิเคราะห์ข้อมูลรั่วไหล ส่วนภัยที่พบมากที่สุดยังคงเป็น **“ฟิชชิ่ง”** ซึ่งครองอันดับหนึ่งในภูมิภาค **เอเชีย-แปซิฟิก** สะท้อนความท้าทายขององค์กรในการรับมือภัยไซเบอร์ยุคใหม่ที่ซับซ้อนและเน้นอัตโนมัติยิ่งขึ้น.

ผลการศึกษาสะท้อนสถานการณ์เกี่ยวกับความปลอดภัยทางไซเบอร์ของประเทศไทยใน 5 ประเด็น

1.AI กลายเป็นอาวุธใหม่ของผู้โจมตี
2.ความเสี่ยงทางไซเบอร์ในปัจจุบัน คือเรื่องปกติ
3.ทีมงานอยู่ภายใต้ความกดดัน แต่คนมีไม่พอ
4.แม้การลงทุนจะเพิ่มขึ้น แต่ก็ยังไม่ทันต่อความเสี่ยง
5.ใช้แพลตฟอร์มสร้างความมั่นคงทางไซเบอร์

https://www.prachachat.net/ict/news-1820786

Mega Trend: Quantum Computer

Problem Statement

- Shor's Algorithm **breaks asymmetric crypto**
  - Breaks **RSA** by quickly factoring large numbers
  - Breaks **Elliptic Curve** Cryptography and **Diffie-Hellman** by solving the discrete log problem
- Grover's Algorithm **weakens symmetric crypto**
  - Square-root speedup on search algorithms
  - **Weakens** symmetric encryption and hashing **by 50%**

Type	Algorithm	Key Strength Classic (bits)	Key Strength Quantum (bits)	Quantum Attack
Asymmetric	RSA 2048	112	0	Shor's Algorithm
	RSA 3072	128		
	ECC 256	128		
	ECC 521	256		
Symmetric	AES 128	128	64	Grover's Algorithm
	AES 256	256	128	

https://utimaco.com/market-trends/2025-utimaco-pqc-readiness-report

Main Challenges of the Post Quantum Age

Impact of Quantum Computing on Applications and Use Cases

Future decryption

- Sensitive data gets tapped
- Stored for future decryption
- Relevant for data with a long confidentiality span

Impersonation

- Attacker "calculates" credentials from public information
- Attacker approves requests or signs documents as you

Fake identities

- Issuance of fake certificates (e. g. identities) in the name of your organization's PKI

https://utimaco.com/market-trends/2025-utimaco-pqc-readiness-report

Regulatory Initiatives Around the World on PQC

Country	PQC Algorithms Under Consideration	Published Guidance	Timeline (summary)
Australia	NIST	ACSC-2023 ACSC-2024	Start planning for transition to quantum resistant cryprography.
Canada	NIST	CAN-01 CAN-02	Start planning, wait for standards. CSE is updating detailed PQC guidance.
China	China Specific	CAICT-2023	Start Planning
Czech Republic	NIST (but not restricted to)	NÚKIB-2023	Migrate by 2027 (key establishment, encryption). As soon as possible for firmware & software signing.
European Union	NIST Plan to select PQC EU algorithms	ENISA-2022 EC-2024	Start planning Define a coordinated PQC roadmap for Member States by 2026
France	NIST (but not restricted to)	ANSSI (2022, 2023)	Start planning; Transition from 2024
Germany	NIST (but not restricted to)	BSI-2021 BSI-2023 BSI-2024	Start planning
Italy	NIST	CAN-2024	
Japan	Monitoring NIST	JAPAN-2022	Start planning; initial timeline. CRYPTREC is preparing detailed PQC guidelines.
Netherlands	ML-KEM, Classic McEliece and FrodoKEM recommended in hybrid mode for TLS.	NL-2022 AIVD-2023 NL-2024	Draft action plan with timeframes
New Zealand	NIST	NZISM-2024	Start planning. Transition from 2026-27.
Singapore	Monitoring NIST	SG-2022 MAS-2024	No timeline available. Financial services firms required to prepare plan.
South Korea	KpqC	MSIT (2022) MSIT (2024)	Start competition First round (Nov.'22-Nov.'23). PQC Roadmap published
Spain	NIST and FrodoKEM.	CCN.ES-2022	Four phase approach today to post-2030.
United Kingdom	NIST	NCSC-2024a NCSC-2024b	Start planning; use only standards in production. NCSC is preparing detailed PQC guidance.
United States	NIST	NSM-10 CISA-2021 CNSA20 HR7375 CISA-2023 CISA-2024	Implement 2023-2033

*https://www.gsma.com/newsroom/post-quantum-government-initiatives-by-country-and-region/

https://utimaco.com/market-trends/2025-utimaco-pqc-readiness-report

Year to Quantum (Y2Q) Countdown Clock

https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security/

ข้อมูลวันที่ 24 กันยายน พ.ศ. 2568

Guidelines for Post-Quantum Readiness

คำแนะนำเรื่องแนวทางปฏิบัติการเตรียมความพร้อมสำหรับยุคควอนตัม

สำนักงานคณะกรรมการการรักษา
ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

คำแนะนำเรื่องแนวทางการปฏิบัติ
การเตรียมความพร้อมสำหรับยุคควอนตัม
Guidelines for Post-Quantum Readiness

ศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์

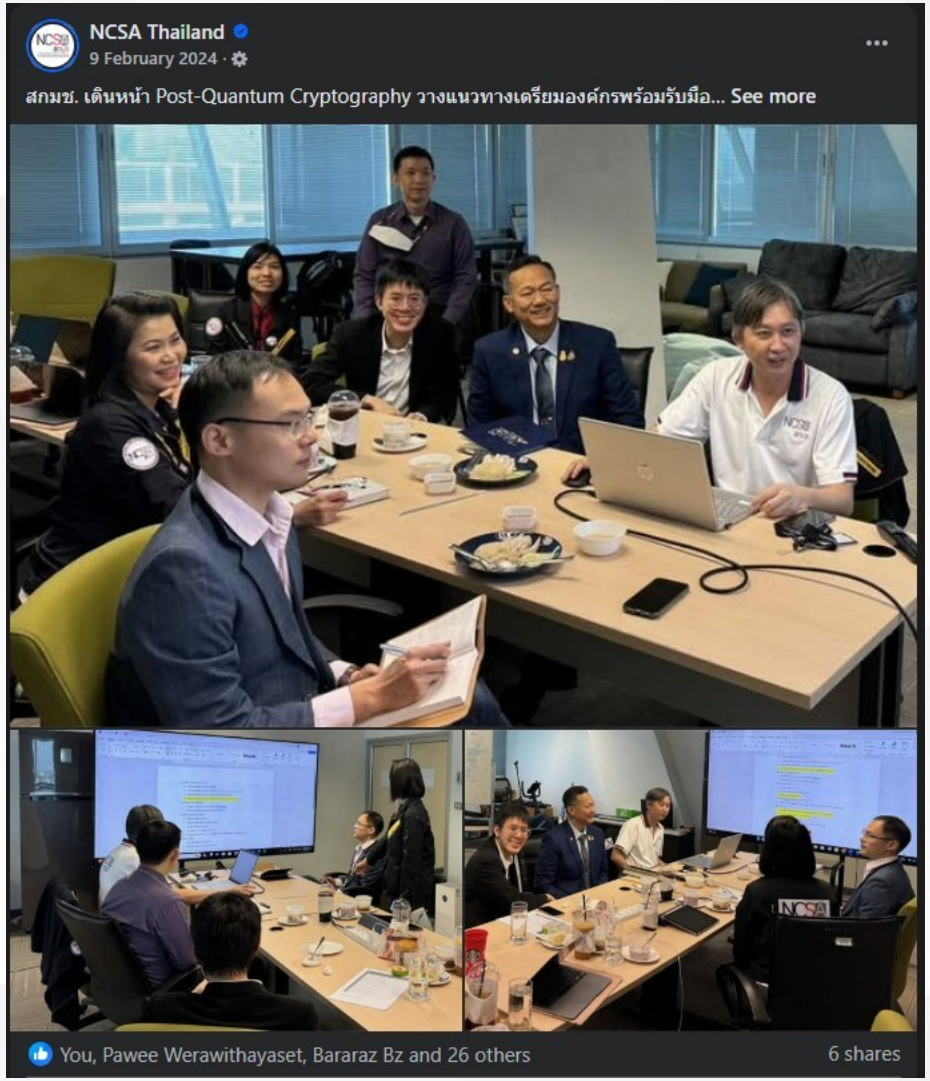
สารบัญ

รูปที่ ๔ เตรียมความพร้อมสำหรับยุคควอนตัม[๒๕]

คำแนะนำเรื่องแนวทาง
ปฏิบัติการเตรียมความ
พร้อมสำหรับยุคควอนตัม

https://drive.ncsa.or.th/s/52GYxAqMfDNZjEZ

NCSA VS Quantum Computing



NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

แนวปฏิบัติขั้นตอนการเตรียมความพร้อม PQC

1. จัดทำแผนงาน (Roadmap):
กำหนดบุคลากรเพื่อจัดทำแผนงาน (Roadmap) เตรียมความพร้อมรับมือภัยคุกคามจากคอมพิวเตอร์ควอนตัมตั้งแต่เนิ่นๆ เพื่อให้การเปลี่ยนแปลงเป็นไปอย่างราบรื่นและประเมินค่าใช้จ่ายในการลงทุนได้

2. เสริมสร้างความตระหนักรู้:
ศึกษาและสร้างความรู้ความเข้าใจเกี่ยวกับภัยคุกคามจากคอมพิวเตอร์ควอนตัมให้แก่พนักงานในทุกฝ่าย เพื่อให้สามารถเลือกใช้ซอฟต์แวร์หรือฮาร์ดแวร์ที่มีความปลอดภัยต่อการโจมตีจากควอนตัมได้

3. กำหนดหน้าที่ความรับผิดชอบ:
มอบหมายหน้าที่และความรับผิดชอบให้แก่บุคลากรที่เกี่ยวข้องในแต่ละส่วนงาน เพื่อให้มีความรู้ความเข้าใจเกี่ยวกับเทคโนโลยีระบบรหัสลับที่องค์กรเลือกใช้

4. จัดทำรายการสินทรัพย์ทางสารสนเทศ:
จัดทำรายการสินทรัพย์ไอที (IT asset inventory) ทั้งซอฟต์แวร์และฮาร์ดแวร์ที่เกี่ยวข้องกับระบบรหัสลับ เพื่อทำความเข้าใจวิธีการสร้าง จัดเก็บ และใช้งานกุญแจเข้ารหัสลับในปัจจุบัน

5. ประเมินเทคโนโลยีทางเลือก:
ประเมินและเปรียบเทียบข้อดีข้อเสียของเทคโนโลยี PQC (Post-Quantum Cryptography) หรือ QKD (Quantum Key Distribution) เพื่อเลือกใช้ให้เหมาะสมกับระบบสารสนเทศขององค์กร หรืออาจใช้ระบบความปลอดภัยแบบผสมผสาน (Hybrid Security Approach)

6. ทำการทดลองและทดสอบ:
เริ่มทดลองและทดสอบระบบและเทคโนโลยีที่เกี่ยวข้องได้เลย แม้ว่ามาตรฐานจะยังไม่สมบูรณ์ เพื่อเตรียมความพร้อมสำหรับการเปลี่ยนแปลงในอนาคต และทำความเข้าใจปัญหาที่อาจเกิดขึ้น

7. ติดตามความก้าวหน้าอย่างต่อเนื่อง:
ติดตามความคืบหน้าของแผนงานอย่างต่อเนื่อง พร้อมทั้งประเมินความเสี่ยงและระยะเวลาที่อาจเกิดภัยคุกคามใหม่อยู่เป็นระยะ

https://drive.ncsa.or.th/s/52GYxAqMfDNZjEZ

ปัจจุบันทั่วโลกกำลังให้ความสำคัญและเร่งพัฒนาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในทุกมิติ

International Laws and Regulation

กฎหมาย Cyber Solidarity Act ของ EU

- **วัตถุประสงค์หลัก:** เสริมสร้างขีดความสามารถของสหภาพยุโรปในการตรวจจับ เตรียมความพร้อม และรับมือกับภัยคุกคามทางไซเบอร์ขนาดใหญ่ ผ่านยุทธศาสตร์สามเสาหลักที่เน้นความร่วมมือและการป้องกันเชิงรุก
- **3 เสาหลัก**
  - เสาหลักที่ 1: ระบบแจ้งเตือนความปลอดภัยทางไซเบอร์แห่งยุโรป (European Cybersecurity Alert System)
  - เสาหลักที่ 2: กลไกฉุกเฉินด้านความปลอดภัยไซเบอร์ (Cybersecurity Emergency Mechanism)
  - เสาหลักที่ 3: กลไกทบทวนเหตุการณ์ความปลอดภัยไซเบอร์ (European Cybersecurity Incident Review Mechanism)

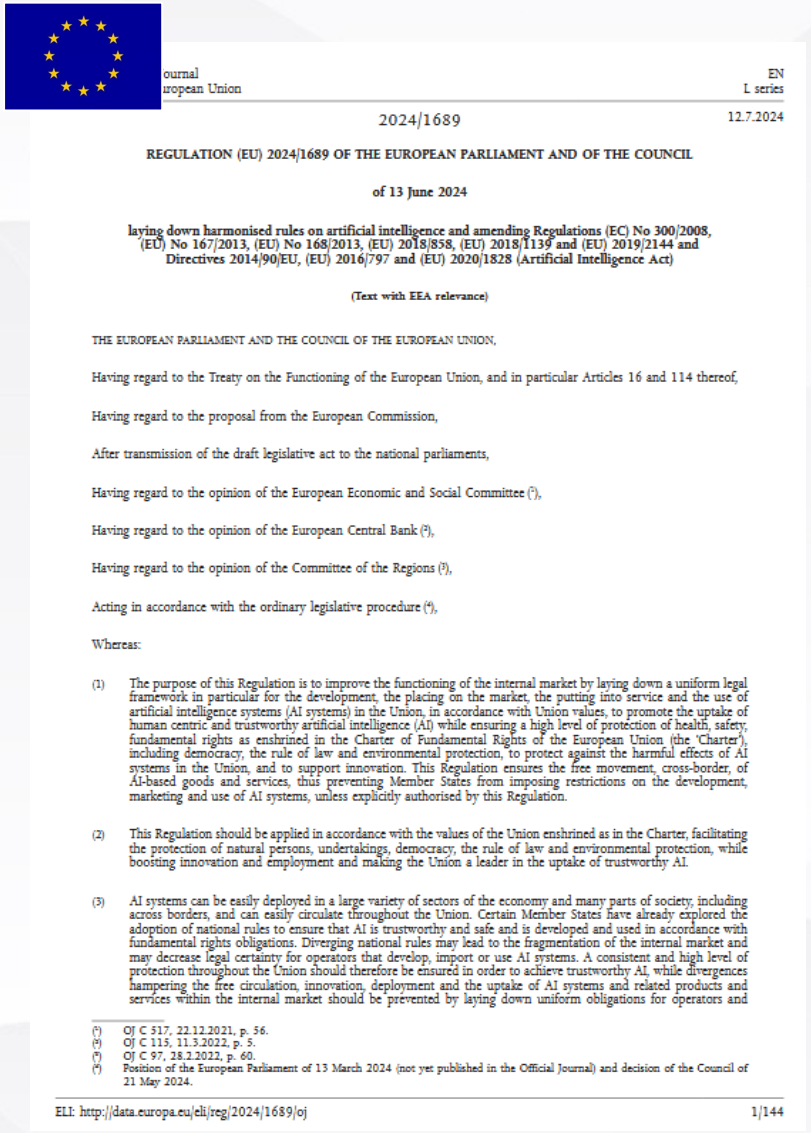
https://eur-lex.europa.eu/eli/reg/2025/38/oj

FDA U.S. FOOD & DRUG ADMINISTRATION

แนวทาง FDA สหรัฐฯ: ความปลอดภัยไซเบอร์ในอุปกรณ์การแพทย์

- วัตถุประสงค์หลัก: กำหนดให้ความมั่นคงปลอดภัยไซเบอร์เป็นส่วนสำคัญของความปลอดภัยผู้ป่วยตลอดวงจรชีวิตผลิตภัณฑ์ (Total Product Lifecycle - TPLC) และบังคับใช้กับผู้ผลิตอุปกรณ์การแพทย์
- **หลักการสำคัญ:**
  - **ความปลอดภัยไซเบอร์เป็นส่วนหนึ่งของความปลอดภัย:** เชื่อมโยงความปลอดภัยไซเบอร์เข้ากับกฎระเบียบระบบคุณภาพ (QS) ของ FDA อย่างชัดเจน
  - **กรอบการพัฒนาผลิตภัณฑ์ที่ปลอดภัย (SPDF):** สนับสนุนให้ผู้ผลิตใช้แนวทาง "Secure by Design" คือการฝังความปลอดภัยเข้าไปในทุกขั้นตอนตั้งแต่การออกแบบ
  - **การประเมินความเสี่ยงที่เน้นการถูกโจมตี (Exploitability):** ประเมินความเสี่ยงโดยพิจารณาจากโอกาสที่ช่องโหว่จะถูกโจมตีได้จริง
  - **รายการส่วนประกอบซอฟต์แวร์ (SBOM):** เป็นข้อบังคับทางกฎหมายสำหรับ "Cyber Devices" ที่ต้องส่งรายการซอฟต์แวร์ทั้งหมดเพื่อความโปร่งใสและง่ายต่อการจัดการช่องโหว่
  - **ความโปร่งใสและการจัดทำเอกสาร:** ผู้ผลิตต้องจัดทำเอกสารทางเทคนิคที่ครอบคลุม ตั้งแต่สถาปัตยกรรมความปลอดภัยไปจนถึงผลการทดสอบเจาะระบบ (Penetration Testing)

กฎหมาย AI Act ของสหภาพยุโรป: กรอบกำกับดูแลปัญญาประดิษฐ์ฉบับแรกของโลก



journal
uropean Union
EN
L series

2024/1689
12.7.2024

REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 13 June 2024

laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Having regard to the opinion of the European Central Bank (2),

Having regard to the opinion of the Committee of the Regions (3),

Acting in accordance with the ordinary legislative procedure (4),

Whereas:

(1) The purpose of this Regulation is to improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, the placing on the market, the putting into service and the use of artificial intelligence systems (AI systems) in the Union, in accordance with Union values, to promote the uptake of human centric and trustworthy artificial intelligence (AI) while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union (the 'Charter'), including democracy, the rule of law and environmental protection, to protect against the harmful effects of AI systems in the Union, and to support innovation. This Regulation ensures the free movement, cross-border, of AI-based goods and services, thus preventing Member States from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by this Regulation.

(2) This Regulation should be applied in accordance with the values of the Union enshrined as in the Charter, facilitating the protection of natural persons, undertakings, democracy, the rule of law and environmental protection, while boosting innovation and employment and making the Union a leader in the uptake of trustworthy AI.

(3) AI systems can be easily deployed in a large variety of sectors of the economy and many parts of society, including across borders, and can easily circulate throughout the Union. Certain Member States have already explored the adoption of national rules to ensure that AI is trustworthy and safe and is developed and used in accordance with fundamental rights obligations. Diverging national rules may lead to the fragmentation of the internal market and may decrease legal certainty for operators that develop, import or use AI systems. A consistent and high level of protection throughout the Union should therefore be ensured in order to achieve trustworthy AI, while divergences hampering the free circulation, innovation, deployment and the uptake of AI systems and related products and services within the internal market should be prevented by laying down uniform obligations for operators and

(1) OJ C 517, 22.12.2021, p. 56.
(2) OJ C 115, 11.3.2022, p. 5.
(3) OJ C 97, 28.2.2022, p. 60.
(4) Position of the European Parliament of 13 March 2024 (not yet published in the Official Journal) and decision of the Council of 21 May 2024.

ELI: http://data.europa.eu/eli/reg/2024/1689/oj
1/144

- **วัตถุประสงค์หลัก:** สร้างกรอบกฎหมาย AI ที่เป็นมาตรฐานเดียวกัน ส่งเสริมนวัตกรรมที่เชื่อถือได้และมีมนุษย์เป็นศูนย์กลาง พร้อมปกป้องสิทธิขั้นพื้นฐาน สุขภาพ และความปลอดภัย โดยใช้ **แนวทางกำกับดูแลตามระดับความเสี่ยง (Risk-Based Approach)**
- **การแบ่งประเภทความเสี่ยงของ AI**
- **ความเสี่ยงที่ยอมรับไม่ได้ (Unacceptable Risk) – ห้ามใช้เด็ดขาด:**
  - ระบบที่บิดเบือนพฤติกรรมมนุษย์อย่างมีนัยสำคัญ (Manipulative AI)
  - ระบบให้คะแนนทางสังคม (Social Scoring) โดยภาครัฐหรือเอกชน
  - ระบบระบุตัวตนด้วยข้อมูลชีวมิติแบบเรียลไทม์ในที่สาธารณะ (มีข้อยกเว้นที่จำกัดมาก)
- **AI ความเสี่ยงสูง (High-Risk AI) – ข้อบังคับเข้มงวด:**
  - ระบบ AI ที่ใช้ในภาคส่วนสำคัญ เช่น โครงสร้างพื้นฐาน, การศึกษา, การจ้างงาน, การเข้าถึงบริการที่จำเป็น (เช่น สินเชื่อ), การบังคับใช้กฎหมาย, และกระบวนการยุติธรรม
  - **ข้อบังคับหลัก:** ต้องมีระบบบริหารความเสี่ยง, ใช้ข้อมูลคุณภาพสูง, มีเอกสารทางเทคนิคที่โปร่งใส, มีมนุษย์กำกับดูแล (Human Oversight), และมีความแม่นยำ-ปลอดภัยทางไซเบอร์สูง
- **AI ความเสี่ยงจำกัดและต่ำ (Limited & Minimal Risk):**
  - **ความเสี่ยงจำกัด:** อยู่ภายใต้กฎด้านความโปร่งใส เช่น AI ที่โต้ตอบกับมนุษย์ (Chatbot) ต้องแจ้งให้ผู้ใช้ทราบว่าเป็น AI
  - **ความเสี่ยงต่ำ:** ไม่มีข้อบังคับเพิ่มเติม สามารถพัฒนาและใช้งานได้อย่างเสรี

https://eur-lex.europa.eu/eli/reg/2024/1689/oj

กฎหมายที่เกี่ยวข้องกับไซเบอร์ Cyber Law

Thailand
ไทย

กฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์
- พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

กฎหมายธุรกรรมทางอิเล็กทรอนิกส์ เช่น
- พ.ร.บ. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2562
- พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม
- พ.ร.ก. การประกอบธุรกิจบริการแพลตฟอร์มดิจิทัล ที่ต้องแจ้งให้ทราบ พ.ศ. 2565

กฎหมายการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม
- พ.ร.ก .มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.2566

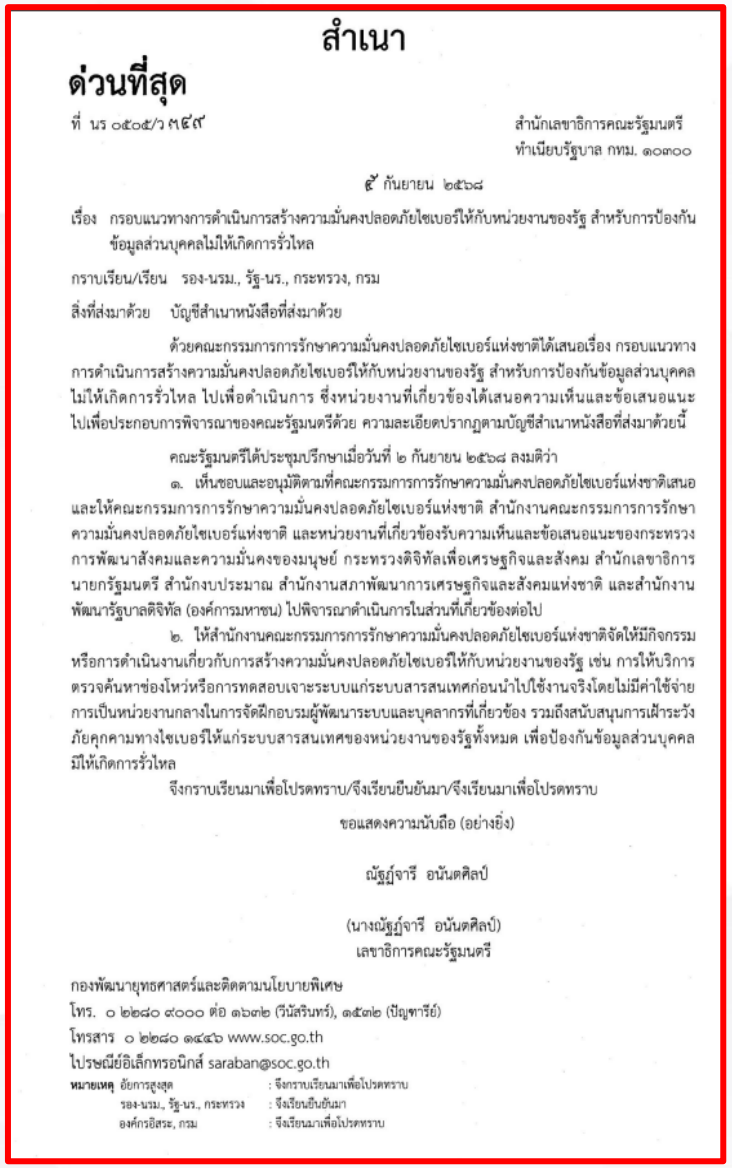
กฎหมายคุ้มครองข้อมูลส่วนบุคคล
- พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

กฎหมายโทรคมนาคม เช่น
- พ.ร.บ. องค์กรจัดสรรคลื่นความถี่และกำกับกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม พ.ศ. 2553 และที่แก้ไขเพิ่มเติม
- พ.ร.บ. การประกอบกิจการกระจายเสียงและกิจการโทรทัศน์ พ.ศ. 2551
- พ.ร.บ. การประกอบกิจการโทรคมนาคม พ.ศ. 2544 และที่แก้ไขเพิ่มเติม

กฎหมายพัฒนาเศรษฐกิจดิจิทัล
- พ.ร.บ. การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. 2560

กฎหมายริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล
- พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

มติ ครม.ตามหนังสือ ว349



สำเนา

ด่วนที่สุด

ที่ นร ๐๕๐๕/ว ๓๔๙ สำนักเลขาธิการคณะรัฐมนตรี
ทำเนียบรัฐบาล กทม. ๑๐๓๐๐

๕ กันยายน ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

กราบเรียน/เรียน รอง-นรม., รัฐ-นร., กระทรวง, กรม

สิ่งที่ส่งมาด้วย บัญชีสำเนาหนังสือที่ส่งมาด้วย

ด้วยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้เสนอเรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ไปเพื่อดำเนินการ ซึ่งหน่วยงานที่เกี่ยวข้องได้เสนอความเห็นและข้อเสนอแนะไปเพื่อประกอบการพิจารณาของคณะรัฐมนตรีด้วย ความละเอียดปรากฏตามบัญชีสำเนาหนังสือที่ส่งมาด้วยนี้

คณะรัฐมนตรีได้ประชุมปรึกษาเมื่อวันที่ ๒ กันยายน ๒๕๖๘ ลงมติว่า

๑. เห็นชอบและอนุมัติตามที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอและให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และหน่วยงานที่เกี่ยวข้องรับความเห็นและข้อเสนอแนะของกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักเลขาธิการนายกรัฐมนตรี สำนักงบประมาณ สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ และสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ไปพิจารณาดำเนินการในส่วนที่เกี่ยวข้องต่อไป

๒. ให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติจัดให้มีกิจกรรมหรือการดำเนินงานเกี่ยวกับการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ เช่น การให้บริการตรวจค้นหาช่องโหว่หรือการทดสอบเจาะระบบแก่ระบบสารสนเทศก่อนนำไปใช้งานจริงโดยไม่มีค่าใช้จ่าย การเป็นหน่วยงานกลางในการจัดฝึกอบรมผู้พัฒนาระบบและบุคลากรที่เกี่ยวข้อง รวมถึงสนับสนุนการเฝ้าระวังภัยคุกคามทางไซเบอร์ให้แก่ระบบสารสนเทศของหน่วยงานของรัฐทั้งหมด เพื่อป้องกันข้อมูลส่วนบุคคลมิให้เกิดการรั่วไหล

จึงกราบเรียนมาเพื่อโปรดทราบ/จึงเรียนยืนยันมา/จึงเรียนมาเพื่อโปรดทราบ

ขอแสดงความนับถือ (อย่างยิ่ง)

ณัฐฏ์จารี อนันตศิลป์

(นางณัฐฏ์จารี อนันตศิลป์)
เลขาธิการคณะรัฐมนตรี

กองพัฒนายุทธศาสตร์และติดตามนโยบายพิเศษ
โทร. ๐ ๒๒๘๐ ๙๐๐๐ ต่อ ๑๖๓๒ (วีนัสรินทร์), ๑๕๓๒ (ปัญฑารีย์)
โทรสาร ๐ ๒๒๘๐ ๑๔๔๖ www.soc.go.th
ไปรษณีย์อิเล็กทรอนิกส์ saraban@soc.go.th

หมายเหตุ ชั้นการสูงสุด : จึงกราบเรียนมาเพื่อโปรดทราบ
รอง-นรม., รัฐ-นร., กระทรวง : จึงเรียนยืนยันมา
องค์กรอิสระ, กรม : จึงเรียนมาเพื่อโปรดทราบ

คณะรัฐมนตรีมีมติ ดังนี้

1. เห็นชอบกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ซึ่งเป็นการขับเคลื่อนการแก้ไขปัญหาเชิงระบบสำหรับหน่วยงานของรัฐ หน่วยงานควบคุม หรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเพื่อเป็นกรอบแนวทางฯ .. และอนุมัติให้ทุกหน่วยงานนำไปดำเนินการเพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับระบบงานของหน่วยงานต่อไป ตามที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอ

ข้อ 1 การใช้มาตรฐานสากลในการออกแบบและพัฒนา
ข้อ 2 งดใช้ข้อมูลจริงในขั้นตอนการพัฒนาระบบ
ข้อ 3 กำหนดเกณฑ์การคัดเลือกบริษัทพัฒนาซอฟต์แวร์ที่มีประสบการณ์และมาตรฐานที่ผ่านการรับรองทางความปลอดภัย
ข้อ 4 กำหนดให้มีการกำกับดูแลติดตาม รวมทั้งการทดสอบความปลอดภัยระบบเป็นประจำ ทั้งในช่วงการพัฒนาและก่อนการใช้งานจริงเพื่อค้นหาช่องโหว่และแก้ไขทันที
ข้อ 5 จัดอบรมสำหรับผู้พัฒนาและบุคลากรที่เกี่ยวข้องในเรื่องการออกแบบและพัฒนาระบบให้ปลอดภัย
ข้อ 6 สร้างการรับรู้ในเรื่องภัยคุกคามไซเบอร์ที่อาจเกิดขึ้น
ข้อ 7 จัดให้มีการตรวจสอบและประเมินผลการทำงานของระบบอย่างสม่ำเสมอ
ข้อ 8 ตรวจสอบความสอดคล้องกับมาตรฐานความปลอดภัยที่กำหนด
ข้อ 9 กำหนดให้มีการระบุเงื่อนไขด้านความปลอดภัยในสัญญาว่าจ้างผู้พัฒนา โดยเน้นความรับผิดชอบต่อปัญหาด้านความปลอดภัยที่อาจเกิดขึ้นจากการพัฒนา
ข้อ 10 จัดให้มีกลไกการเฝ้าระวัง เพื่อแจ้งเตือนและตอบสนองต่อการโจมตีหรือช่องโหว่ที่เกิดขึ้นอย่างรวดเร็ว
ข้อ 11 มีแผนรับมือเมื่อเกิดเหตุการณ์ความปลอดภัยไซเบอร์
ข้อ 12 สนับสนุนการปรับปรุงระบบให้ทันสมัยอยู่เสมอ โดยอัปเดตซอฟต์แวร์และแพตช์ด้านความปลอดภัยเมื่อมีช่องโหว่ที่ถูกค้นพบ
ข้อ 13 ปิดระบบที่ไม่ได้ใช้งาน เพื่อป้องกันการเข้าถึงข้อมูล
ข้อ 14 ให้หน่วยงานของรัฐปฏิบัติตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

อัพเดต กฎหมายที่สำคัญล่าสุด

ประกาศ กมช. เรื่อง

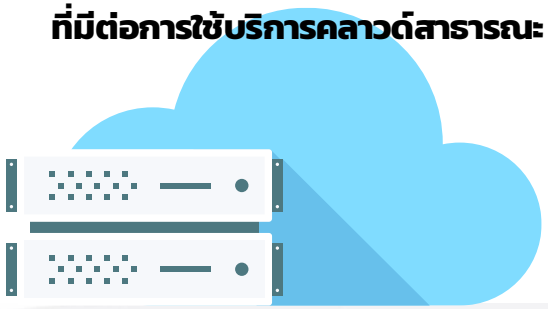
มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

พ.ศ. 2567

มีผลใช้บังคับตั้งแต่วันที่ 10 ก.ย. 69 เป็นต้นไป

สาระสำคัญ

เพื่อกำหนดมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ ให้แก่หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ **เพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีต่อการใช้บริการคลาวด์สาธารณะ**



ดาวน์โหลดเอกสารมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

ประกาศ กมช. เรื่อง

มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์

พ.ศ. 2568

อยู่ระหว่างประกาศในราชกิจจานุเบกษา

สาระสำคัญ

เพื่อเป็นการกำหนดและส่งเสริมให้ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานเอกชน **มีมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ของตน เป็นไปอย่างมีประสิทธิภาพ ปลอดภัย และให้บริการได้อย่างต่อเนื่อง**

ดาวน์โหลดเอกสารมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์

แต่ อย่าลืมกฎระเบียบในปัจจุบัน !!

HA-IT Plus แนวทางการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

สำหรับโรงพยาบาลของรัฐ

แนวทางการดำเนินงาน

ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

สำหรับโรงพยาบาลของรัฐ

พ.ศ. 2567

ตารางวิเคราะห์ผลกระทบทางธุรกิจหากเกิดภัยพิบัติไซเบอร์ต่อระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

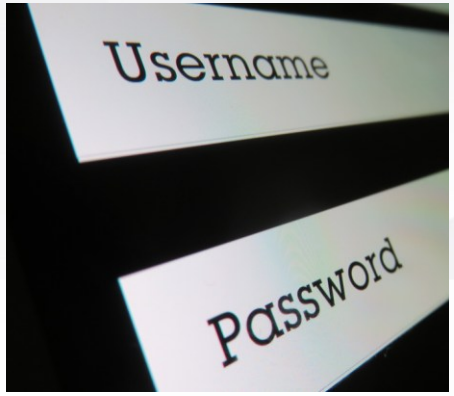
ระบบงาน	ความสำคัญ (สูง ปานกลาง ต่ำ)	ความเสียหายเมื่อเกิดภัยพิบัติที่ทำให้ไม่สามารถให้บริการระบบได้
1. ระบบ Hospital Information System (HIS)	สูง	ระบบงานตรวจรักษาผู้ป่วยนอกหยุดชะงัก การให้บริการผู้ป่วยที่มาตรวจต้องลงอย่างมาก กระทบต่อชีวิตและสุขภาพประชาชน
2. ระบบบริการภาพ X-Rays (PACS)	ปานกลาง	แพทย์ไม่สามารถเรียกดูภาพเอ็กซเรย์เดิมที่ผู้ป่วยเคยตรวจไว้ได้ อาจกระทบต่อคุณภาพการวินิจฉัยโรคและการรักษาผู้ป่วย
3. ระบบ Laboratory Information System (LIS)	ปานกลาง	แพทย์ไม่สามารถเรียกดูผลการตรวจทางห้องปฏิบัติการของผู้ป่วย อาจกระทบต่อคุณภาพการวินิจฉัยโรคและการรักษาผู้ป่วย
4. ระบบ Document Scan ของงานเวชระเบียน	ปานกลาง	ไม่สามารถเรียกดูภาพเอกสารเวชระเบียนที่ scan เก็บไว้ได้ อาจกระทบต่อคุณภาพการวินิจฉัยโรคและการรักษาผู้ป่วย
5. ระบบเชื่อมต่อข้อมูลจากเครื่องวัดความดันโลหิตเข้าสู่ระบบ HIS	ต่ำ	ไม่สามารถดึงข้อมูลจากเครื่องเข้าสู่ระบบ HIS ได้ เจ้าหน้าที่ต้องป้อนข้อมูลเข้าไปเอง อาจเกิดความผิดพลาดของข้อมูลได้ เกิดความล่าช้าของการให้บริการ
6. ระบบหน้าจอแสดงคิวอัตโนมัติ	ต่ำ	ไม่สามารถแสดงคิวผ่านหน้าจอให้ผู้ป่วยได้เห็นคิวได้ เจ้าหน้าที่ต้องดำเนินการเอง อาจเกิดความล่าช้าของการให้บริการ

Source: แนวทางการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับโรงพยาบาลของรัฐ พ.ศ.2567

จากการวิเคราะห์สาเหตุกรณีหน่วยงานรัฐและเอกชน ในประเทศไทยถูกโจมตีของ ThaiCERT ในปี 2567

ระบบของภาครัฐและเอกชนจำนวนมากทั้งที่จ้างพัฒนาและพัฒนาเอง มีความไม่ปลอดภัยและการเขียนโปรแกรมที่ไม่ปลอดภัย

การใช้ซอฟแวร์ที่มีช่องโหว่หรือล้าสมัย



การที่ผู้ดูแลระบบใช้ USERNAME และ PASSWORD เดิมที่ติดมากับอุปกรณ์หรือซอฟต์แวร์

ขาดระบบป้องกันและเฝ้าระวังการถูกโจมตี

การป้องกันการรั่วไหลของข้อมูลจากพนักงานภายใน (Insider Threat)

การใช้งานการเข้ารหัสที่ไม่ปลอดภัยหรือไม่มีการเข้ารหัส

หน่วยงานขาดบุคลากรที่มีความเชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

การขาดบุคลากรด้านการคุ้มครองข้อมูลส่วนบุคคล (DPO)

การจัดการสิทธิ์ของพนักงานที่ออกจากงาน (Offboarding)

ขาดมาตรการกำกับดูแลและการป้องกันการเข้าถึงระบบจากบุคคลภายนอก

NCSA สกมช. ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

คำแนะนำในการป้องกันองค์กรของ สกมช. ในปี 2568

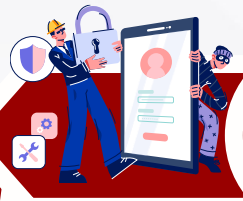
01 อัปเดตซอฟต์แวร์และระบบอยู่เสมอและ หลีกเลี่ยงการดาวน์โหลดและติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์ (Software Updates & Patching)

02 สำรองข้อมูลอย่างปลอดภัยและเป็นประจำ (Data Backup and Disaster Recovery)

03 ยกระดับความปลอดภัยด้วยการยืนยันตัวตน 2 ขั้นตอน (2FA)

04 แต่งตั้งและเสริมบทบาทของ DPO และ CISO

05 จัดตั้ง SOC ตลอดจนตรวจสอบและวิเคราะห์กิจกรรมในเครือข่ายอย่างสม่ำเสมอ



06 จัดการความเสี่ยงจากการใช้ AI อย่างมีจริยธรรม (AI Risk Management)

07 ส่งเสริมการใช้รหัสผ่านที่ปลอดภัยและนโยบาย Zero-Trust

08 มีการกำกับดูและคัดเลือกบริษัทที่มีประสบการณ์และมาตรฐานความปลอดภัย และหลีกเลี่ยงการใช้ข้อมูลจริงในขั้นตอนการพัฒนา

09 ป้องกัน Insider Threat และจัดการ Offboarding อย่างปลอดภัย

10 ให้ความรู้แก่พนักงานและปรับปรุงความรู้ด้านความปลอดภัยไซเบอร์


Q&A

Contact us

National Cyber Security Agency - NCSA

NCSA Thailand

Line ID : NCSA Thailand

E-Mail:

saraban@ncsa.or.th

4IoTus (สี่ แอล โอ ทีใหญ่ ยู เอส)