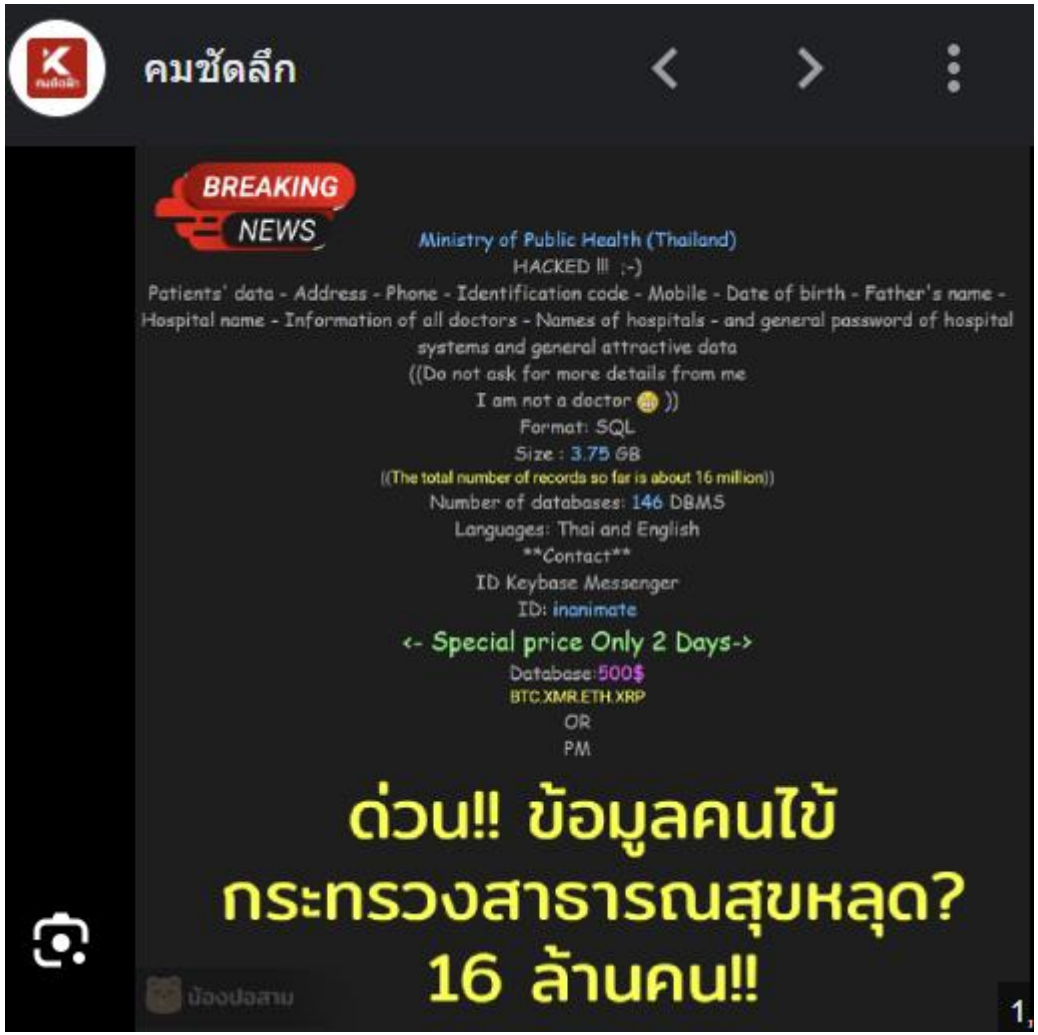
มนต์ศักดิ์ โซ่เจริญธรรม

- ที่ปรึกษา ในคณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ ของ สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.)
- ผู้ทรงคุณวุฒิ ด้านปัญญาประดิษฐ์ หน่วยบริหารและจัดการทุนด้านการพัฒนากำลังคนและทุนด้านการพัฒนาสถาบันอุดมศึกษา การวิจัยและการสร้างนวัตกรรม (บพค.) กระทรวง อว.
- ที่ปรึกษา คณะกรรมาธิการวิสามัญพิจารณาศึกษาแนวทางในการควบคุมและส่งเสริมการใช้เทคโนโลยีปัญญาประดิษฐ์เพื่อรองรับการเปลี่ยนแปลงในอนาคต (สภาผู้แทนราษฎร)
- ที่ปรึกษา อนุกรรมการด้านดิจิทัล สำนักงานอัยการสูงสุด
- ที่ปรึกษา (ด้านการใช้เทคโนโลยีดิจิทัลเพื่องานด้านสิทธิมนุษย์ชน) กรมคุ้มครองสิทธิและเสรีภาพ กระทรวงยุติธรรม
- ที่ปรึกษา คณะกรรมการธรรมาภิบาลข้อมูล (Data governance Council) กรมควบคุมโรค กระทรวงสาธารณะสุข
- อนุกรรมการ ด้านพัฒนาระบบเทคโนโลยีดิจิทัล สถาบันรับรองคุณภาพสถานพยาบาล (องค์การมหาชน)
- (อดีต) ที่ปรึกษาเลขาธิการ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)
- (อดีต) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) สำนักงานพัฒนารัฐบาลดิจิทัล (สพร. /DGA)
- (อดีต) ผู้บริหารข้อมูลระดับสูง (CDO) สำนักงานพัฒนารัฐบาลดิจิทัล (สพร./DGA)
- (อดีต) ผู้อำนวยสถาบันนวัตกรรมและธรรมาภิบาลข้อมูล สำนักงานพัฒนารัฐบาลดิจิทัล (สพร. /DGA)
- (อดีต) ผู้อำนวยการฝ่ายส่งเสริมเมืองอัจฉริยะ (Smart City) สำนักงานส่งเสริมเศรษฐกิจดิจิทัล (depa)
- (อดีต) ผู้อำนวยการสถาบันไอโอที และนวัตกรรมดิจิทัล สำนักงานส่งเสริมเศรษฐกิจดิจิทัล (depa)
- (อดีต) ผู้เชี่ยวชาญอาวุโสด้านดิจิทัลและนวัตกรรม สำนักงานส่งเสริมเศรษฐกิจดิจิทัล (depa)

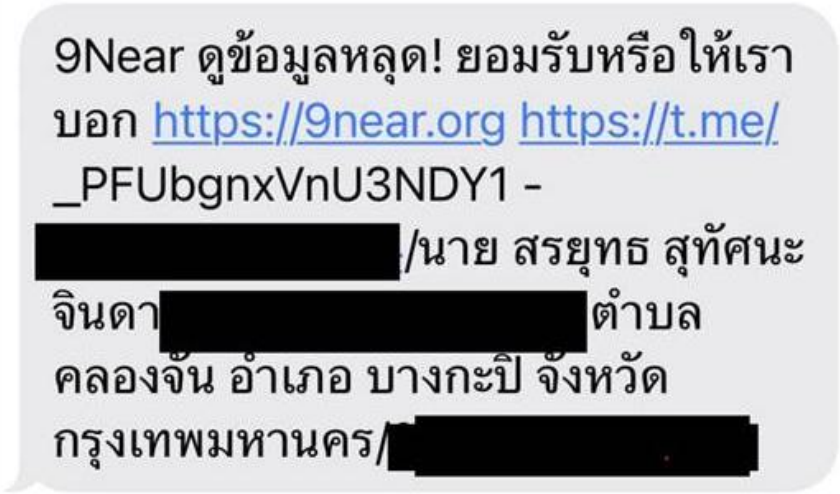
Module 1: บทสรุปผู้บริหาร
ภาพรวมของ Cybersecurity ในประเทศไทย
ผลกระทบที่เกิดขึ้นกับองค์กร และ
ข้อสำคัญที่ผู้บริหารองค์กรควรรู้และตระหนัก
ในการกำหนดนโยบายและลงทุนป้องกันได้อย่างถูกต้อง


PPTV HD 36
Thailand DOPgo.th Leaked
กรมกิจการผู้สูงอายุ
Department of Older Persons (DOP)
Hello BF 2.0 Members
I want to leak database backup of Thailand Department of Older Persons (https://dop.go.th).
file size compressed : 690.8 MB
file size uncompressed : 6.9 GB
total rows : 19718687
Download here :
Hidden Content
database tables :
PID
FULL NAME
PHONE
ADDRESS
IDCARD
BIRTHDAY
GENDER
ข้อมูลคนไทยรั่วไหล
ถูกประกาศขายกว่า 20 ล้านบัญชี!


06 : 34 : 36
ฝีมือแฮกเกอร์ไทย
ขู่ข้อมูลหลุด 55 ล้านรายชื่อ ชี้เพื่อดิสเครดิตหน่วยงาน
@naewna_news
naewnanews
naewna
@naewna
Naewnanews - แนวหน้าออนไลน์


คมชัดลึก
BREAKING
NEWS
Ministry of Public Health (Thailand)
HACKED !!! ;-)
Patients' data - Address - Phone - Identification code - Mobile - Date of birth - Father's name - Hospital name - Information of all doctors - Names of hospitals - and general password of hospital systems and general attractive data
((Do not ask for more details from me
I am not a doctor))
Format: SQL
Size : 3.75 GB
((The total number of records so far is about 16 million))
Number of databases: 146 DBMS
Languages: Thai and English
Contact
ID Keybase Messenger
ID: inanimate
<- Special price Only 2 Days->
Database:500$
BTC,XMR,ETH,XRP
OR
PM
ด่วน!! ข้อมูลคนไข้
กระทรวงสาธารณสุขหลุด?
16 ล้านคน!!


เลือกตั้ง 66
THE STATES TIMES
CRIMES
สรยุทธ สุทัศนะจินดา กรรมกรข่าว
5 ชม. ·
เฮ่ย! ข้อมูลหลุดจริงๆ มีครบ ทั้ง เลขบัตรประชาชน 13 หลัก, วันเดือนปีเกิด , ที่อยู่ , เบอร์มือถือ
76
9N-Group
ข้อความ
เมื่อวาน 14:58
9Near ดูข้อมูลหลุด! ยอมรับหรือให้เราบอก https://9near.org https://t.me/_PFUbgnxVnU3NDY1 -
/นาย สรยุทธ สุทัศนะจินดา
ตำบลคลองจัน
กรุงเทพม
หลุดหมดครบถ้วน!!
‘สรยุทธ’ ยังโดน! แฮกเกอร์ ส่ง SMS ข้อมูลหลุดจริง
ซ้ำ! แฮกเกอร์ประกาศขาย 55 ล้านรายชื่อ อ้างได้มาจากรัฐ


9Near ดูข้อมูลหลุด! ยอมรับหรือให้เราบอก https://9near.org https://t.me/_PFUbgnxVnU3NDY1 -
/นาย สรยุทธ สุทัศนะจินดา
ตำบลคลองจัน อำเภอ บางกะปิ จังหวัดกรุงเทพมหานคร/


Thai PBS 3
หมอพร้อม
ผบ.ตร.ยืนยันข้อมูลหลุด
จาก “หมอพร้อม”


3PlusNews @3Plusnews · 17h
หลุดอีกแล้ว! ดาร์กเว็บโพสต์ขายข้อมูล
จาก สธ. 2 ล้านชื่อ ราคาเหมาๆ 1 หมื่นเ
อ่านต่อได้ที่ :
ch3...
#3PlusNews #ข่าวช่อง3
Ministry of Public Health of Thailand
กระทรวงสาธารณสุข
MINISTRY OF PUBLIC HEALTH
หลุดอีกแล้ว !
ดาร์กเว็บโพสต์ขายข้อ
2 ล้านชื่อ ราคา 1 หมื่นเหรียญ
B1 @b_B1B2B3 · 4m
แต่มีคนพบข้อมูลการรั่วไหล มีการขายข้อมูลนะ
หลุดอีกแล้ว! เพจ 'ชมรมแพทย์ชนบท' หวั่นซ้ำ
9near ขายข้อมูลคนไทย หลังพบว่า มี
โพสต์ขายข้อมูลอ้างมาจาก สธ. 2
เหมาๆ 1 หมื่นเหรียญ
เหวดกันค่ะ ว่า รมต. ท่านใดจะมาตอบประเด็นนี้
ก. หมอชลน่าน
ข. คุณประเสริฐ จันทรรวงทอง (AKA รมต.DE)
ค. สองท่านช่วยกันตอบ
ง. ไม่มีใครตอบ
หลุดอีกแล้ว! ดาร์กเว็บโพสต์ขายข้อมูลอ้างมา
จาก สธ. 2 ล้านชื่อ ราคาเหมาๆ 1 หมื่นเหรียญ
อ่านต่อได้ที่ : ch3plus.com/news/crime/
ch3...
#3PlusNews #ข่าวช่อง3
หลุดอีกแล้ว !
ดาร์กเว็บโพสต์ขายข้อมูล สธ.
สธ.ยืนยัน
ข้อมูลด้านสาธารณสุข ไม่รั่วไหล!!
19 มีนาคม 2567


กรมกิจการผู้สูงอายุ
กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์
Department of Older Persons
Ministry of Social Development and Human Security
Ch7HD NEWS
ข่าวออนไลน์
ดูทีวีกด 35
สดออนไลน์
BUGABOO TV
ขอโทษ "ผู้สูงอายุ"
ข้อมูลหลุดขายว่อนเน็ต

JIB เข้าชี้แจงแล้ว เคสข้อมูลลูกค้ารั่ว คาดเป็นฝีมืออดีตพนักงาน

สรุปกรณี True ทำข้อมูลผู้ใช้หลุด 46,000 ราย สื่อนอกชี้สะเพร่า 1 เดือนเต็ม กสทช. เรียกพบ 17 เมษาฯ นี้

โดย THE STANDARD TEAM
15.04.2018

AWN

Press Statement
6 กันยายน 2566

เอดับบลิวเอ็น ในกลุ่ม เอไอเอส ชี้แจง กรณีมีผู้ละเมิดข้อมูลสารสนเทศลูกค้านิติบุคคล ที่ใช้บริการ Mobile PBX

ตามที่ บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด (เอดับบลิวเอ็น) ในกลุ่ม ของ เอไอเอส ได้รับแจ้งจาก บริษัท ไอซอฟเทล (ประเทศไทย) จำกัด (ไอซอฟเทล) ผู้ให้บริการระบบ Mobile PBX แก่ลูกค้าบริษัทนิติบุคคลของ เอดับบลิวเอ็นว่ามีการเข้าถึงข้อมูลสารสนเทศในระบบดังกล่าว โดยไม่ชอบด้วยกฎหมายและโดยไม่ได้รับอนุญาต ซึ่งหลังจากได้รับแจ้ง เอดับบลิวเอ็นไม่ได้นิ่งนอนใจกับเหตุการณ์ที่เกิดขึ้น และได้เร่งทำงานร่วมกับ ไอซอฟเทล และผู้เชี่ยวชาญ ในการตรวจสอบข้อมูลที่ถูกอ้างถึงอย่างเร่งด่วน ซึ่งในเบื้องต้นกรณีนี้ ไม่เกี่ยวข้องกับระบบฐานข้อมูลและบริการของลูกค้าทั่วไป รวมทั้งลูกค้านิติบุคคลอื่นๆ ของเอดับบลิวเอ็นที่ไม่ได้ใช้บริการ Mobile PBX

โดยหลังจากพบกรณีดังกล่าว ไอซอฟเทลได้ทำการปิดกั้นการเข้าถึงข้อมูลสารสนเทศบนบริการ Mobile PBX ทั้งหมดแล้วทันที พร้อมกับพัฒนาระบบ Mobile PBX เวอร์ชั่นใหม่ ให้มีมาตรฐานความปลอดภัยที่สูงขึ้น โดยลูกค้านิติบุคคลยังคงสามารถใช้งาน Mobile PBX ได้ตามปกติ

ทั้งนี้ หน่วยงานภาครัฐที่เกี่ยวข้อง ประกอบด้วยสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) และ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้รับแจ้งเหตุการณ์ดังกล่าวจากเอดับบลิวเอ็น, ไอซอฟเทลเรียบร้อยแล้ว รวมถึงไอซอฟเทลได้ดำเนินการแจ้งความกับเจ้าพนักงานตำรวจ

Crowdstrike ล่มทั่วโลก

ผู้ใช้หลายคนถูกล็อกเอาต์ออกจากระบบ

CYBERTRON

รายละเอียด

- เซิร์ฟเวอร์ CrowdStrike ล่มและเกิดข้อผิดพลาด BSOD ข้อผิดพลาด BSOD หมายถึงข้อผิดพลาดหน้าจอสีน้ำเงินแห่งความตาย (blue screen of death error) ซึ่งเป็นที่รู้จักกันอีกชื่อว่า stop error และเป็นข้อผิดพลาดที่รุนแรง
- CrowdStrike ได้ยอมรับข้อผิดพลาดนี้และกล่าวว่า **“วิศวกรของเรากำลังทำงานอย่างขยันขันแข็งเพื่อแก้ไขปัญหานี้และไม่จำเป็นต้องเปิดตั๋วสนับสนุน”** นอกจากนี้ พวกเขายังกล่าวว่าจะมีการแจ้งให้ทราบเมื่อปัญหาได้รับการแก้ไขแล้ว

ขั้นตอนการแก้ไขปัญหา

- บูต Windows เข้าสู่ Safe Mode หรือ Windows Recovery Environment
- ไปที่ไดเรกทอรี C:\Windows\System32\drivers\CrowdStrike
- ค้นหาไฟล์ที่ตรงกับ "C-00000291*.sys" และลบไฟล์นั้น
- บูตเครื่องตามปกติ


มิติหุ้น
crowdstrikeล่ม
SETไม่ล่ม?
Microsoft
ระบบคอมพิวเตอร์ล่มเกือบทั่วโลก
กระทบสายการบิน การเดินเรือต้องหยุดชะงัก
ทั้ง แบงก์, สนามบิน,การเดินเรือ ตลาดหุ้น
อาทิ Cathay Pacific, Delta Air Lines , American Airlines สายการบินใหญ่สุดในโลก
London Stock Exchange ด้านระบบข่าว
รวมทั้ง รพ.และ สายการบินในไทย อาทิ รพ.ศิริราช, สายการบินแอร์เอเชีย เป็นต้น
ปัญหาที่เกิดขึ้น เกิดจาก cybersecurity software
ของบริษัท crowdstrike. ส่งผลให้การบริการของ Microsoft ล่มทั้งหมด
ขณะที่ SET ระบบซื้อขาย และระบบข่าวในบริษัทจดทะเบียน ไม่ล่ม
SET
เหตุไม่ได้เลือกใช้บริการค่ายที่เป็นปัญหา โดย SET ใช้ระบบ trading engine ของ Nasdag
ส่วนระบบข่าว SET พัฒนาขึ้นมาเอง
นอกจากนี้ SET ยังมีมีทีม ไอที,คณะกรรมการดูแลเรื่องดังกล่าว และยังมีทำงานร่วมเวนเดอร์จากต่างประเทศ
เพื่อรองรับการเปลี่ยนแปลงในอนาคตรวมถึง AIครั้งใหญ่ด้วย
www.mitihoon.com
mitihoon
mitihoon
@mitihoon


tech hub
KNOWLEDGE
UPDATE
HOWTO
:(
Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.
65% complete
CROWDSTRIKE
TRENDING
‘ล่มทั่วโลก Windows ขึ้นจอฟ้า’
หลังอัปเดต CrowdStrike


SPOTLIGHT
:(
Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.
20% complete
For more information about this issue and possible fixes, visit https://www.windows.com/stopcode
If you call a support person, give them this info.
Stop code: CRITICAL_PROCESS_DIED
CROWDSTRIKE
Windows ล่มกันทั่วโลก
CrowdStrike ต้นเหตุของปัญหา

ยกเลิก 2,692 เที่ยวบิน
7 ข้อสรุป ระบบไอทีล่มทั่วโลก

Stuxnet is a malicious computer worm first uncovered in 2010 and thought to have been in development since at least 2005.

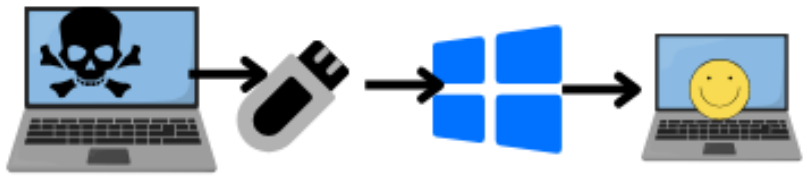
Iranian President Mahmoud Ahmadinejad during a tour of centrifuges at Natanz in 2008. OFFICE OF THE PRESIDENCY OF THE ISLAMIC REPUBLIC OF IRAN

This recent undated satellite image provided by Space Imaging/Inta SpaceTurk shows the once-secret Natanz nuclear complex in Natanz, Iran, about 150 miles south of Tehran.AP PHOTO/SPACE IMAGING/INTA SPACETURK, HO

Iranian President Mahmoud Ahmadinejad observes computer monitors at the Natanz uranium enrichment plant in central Iran, where Stuxnet was believed to have infected PCs and damaged centrifuges. OFFICE OF THE PRESIDENCY OF THE ISLAMIC REPUBLIC OF IRAN


Natanz Nuclear Facility
تأسیسات هسته‌ای نطنز
665
665
Google

HOW STUXNET WORKED



1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

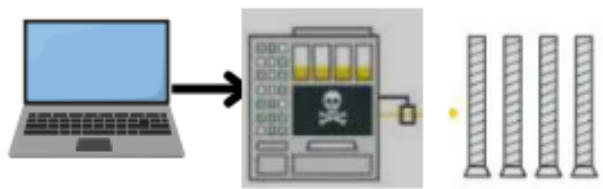
Stuxnet then checks whether a given machine is part of the targeted industry- trial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself

4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities- software weaknesses that haven't been identified by security experts.



5. control

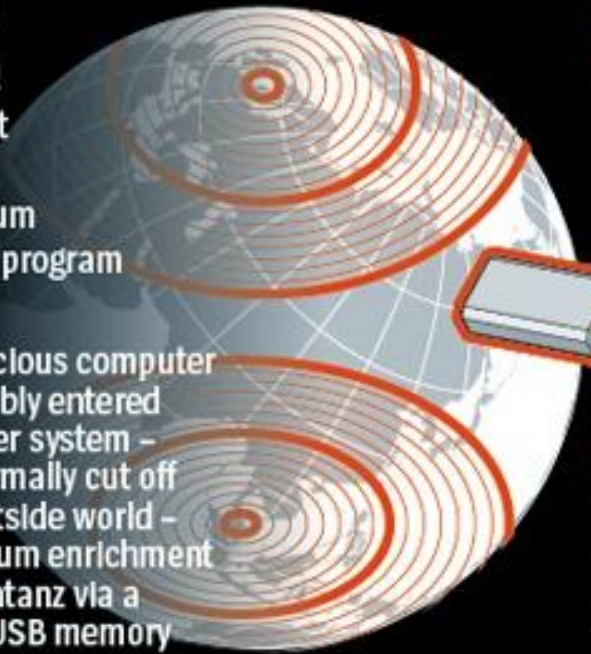
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy

Meanwhile, it provides false feed- back to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it

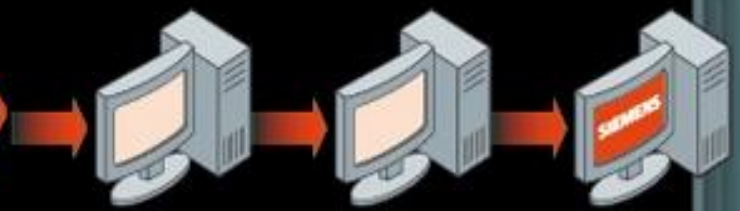
Software Sabotage

How Stuxnet disrupted Iran's uranium enrichment program



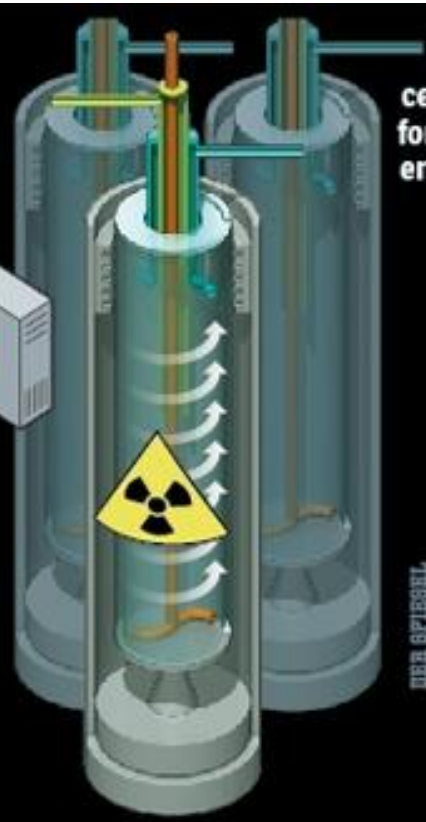
1 The malicious computer worm probably entered the computer system – which is normally cut off from the outside world – at the uranium enrichment facility in Natanz via a removable USB memory stick.

2 The virus is controlled from servers in Denmark and Malaysia with the help of two Internet addresses, both registered to false names. The virus infects some 100,000 computers around the world.



3 Stuxnet spreads through the system until it finds computers running the Siemens control software Step 7, which is responsible for regulating the rotational speed of the centrifuges.

4 The computer worm varies the rotational speed of the centrifuges. This can destroy the centrifuges and impair uranium enrichment.



Iranian centrifuges for uranium enrichment

5 The Stuxnet attacks start in June 2009. From this point on, the number of inoperative centrifuges increases sharply.

Source: IAEA, ISIS, FAS, World Nuclear Association, FT research

องค์ประกอบของ Malware

1. Dropper (Code ส่วนที่ทำหน้าที่ให้เครื่องติดเชื้อ เช่น ใช้วิธีการ Zero-day)
2. Payload (ส่วนการทำงานที่สร้างความเสียหาย)

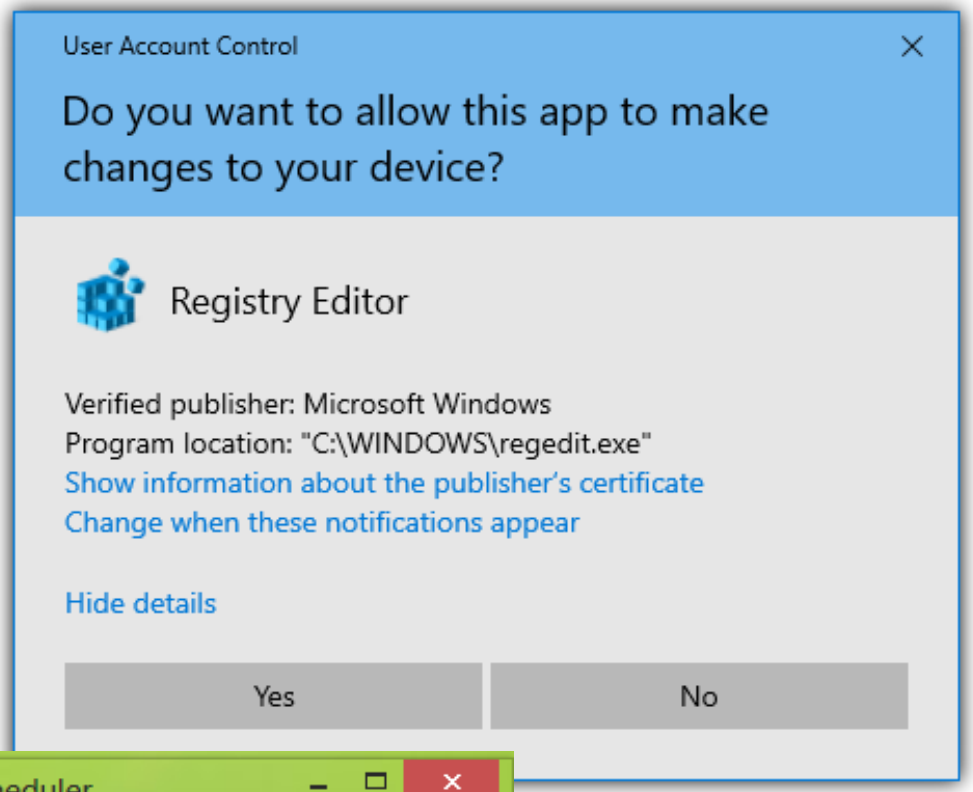
องค์ประกอบของ Operating System (OS)

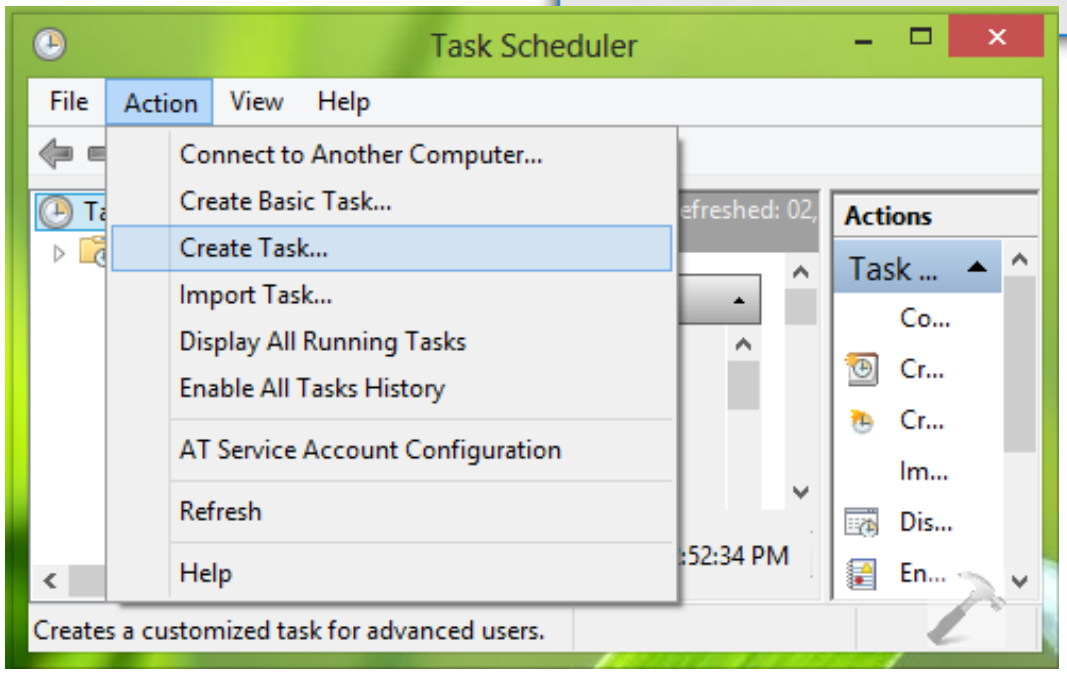
1. Kernel (ฝังอยู่ในส่วนที่ลึกสุดของ OS ทำหน้าที่ควบคุมและจัดการทรัพยากรของเครื่องคอมพิวเตอร์ เช่น คีย์บอร์ด จอภาพ เครื่องพิมพ์ CPU Memory Storage และ ช่อง port สื่อสารต่าง ๆ)
2. User (System, Admin, User) รองรับการใช้งาน (ทำงาน) ของมนุษย์ในระดับต่าง ๆ

รายการ Zero-day ที่ Dropper ของ Stuxnet นำไปใช้งาน (ตัว Dropper มีขนาด 500 KB* เป็นภาษา C++ และ assembly)

1. RPC (Remote Procedure Call)
2. Autorun (โปรแกรมที่ทำงานอัตโนมัติ)
3. Print Spooling (เก็บลงใน /system)
4. Keyboard Layout (ตัวควบคุมการแสดงผลเมื่อกดคีย์บอร์ด)
5. UAC task (ช่องโหว่ที่ทำให้สามารถรันโปรแกรมด้วยสิทธิ์ admin โดยไม่รู้ตัว)

**ขนาดของ dropper ปกติอยู่ที่ 50-100 KB*





การทำงานเพื่อแพร่เชื้อ (หน้าที่ของ dropper ใน Stuxnet)

1. จะตื่นขึ้นมาทุก 1 เดือน และทำการแพร่เชื้อ
2. จะแพร่เชื้อแค่ 3 ครั้ง แล้วหยุด
3. การอัพเดทเวอร์ชั่น จะทำใน Memory ไม่เขียนลงไฟล์
4. มี Doomsday Clock คือ ถ้าถึงวันที่เท่านี้ ทุกอย่างจะยกเลิก (วันส่งมอบนิวเคลียร์ของอิหร่าน)
    - มองหา DLL ของโปรแกรม Step7 ของ Siemens คือ เป็น DLL ที่ทำหน้าที่ควบคุมการทำงานของ PLC
    - ถ้าเจอ ก็จะแทน code ของตัวเองเข้าไปใน DLL ต้นฉบับนั้น
5. จะไม่ทำงานถ้าตรวจไม่พบการเชื่อมต่อของเครื่อง Centrifuge และ การใช้งาน Step7

ทั่วโลกทราบเรื่อง Stuxnet ได้อย่างไร

มีผู้ใช้ booth เครื่องไม่ขึ้น แล้วไปติดต่อบริษัท Antivirus ให้ช่วยดูให้หน่อย

ปัญหา คือ booth เครื่องไม่ขึ้น และแม้ติดตั้ง Windows ใหม่ แล้ว แต่ก็ยังไม่หาย
ซึ่งแปลกมาก ..... แล้วเรื่องทั้งหมด ก็เริ่มต้น

คำถาม เกี่ยวกับ Stuxnet

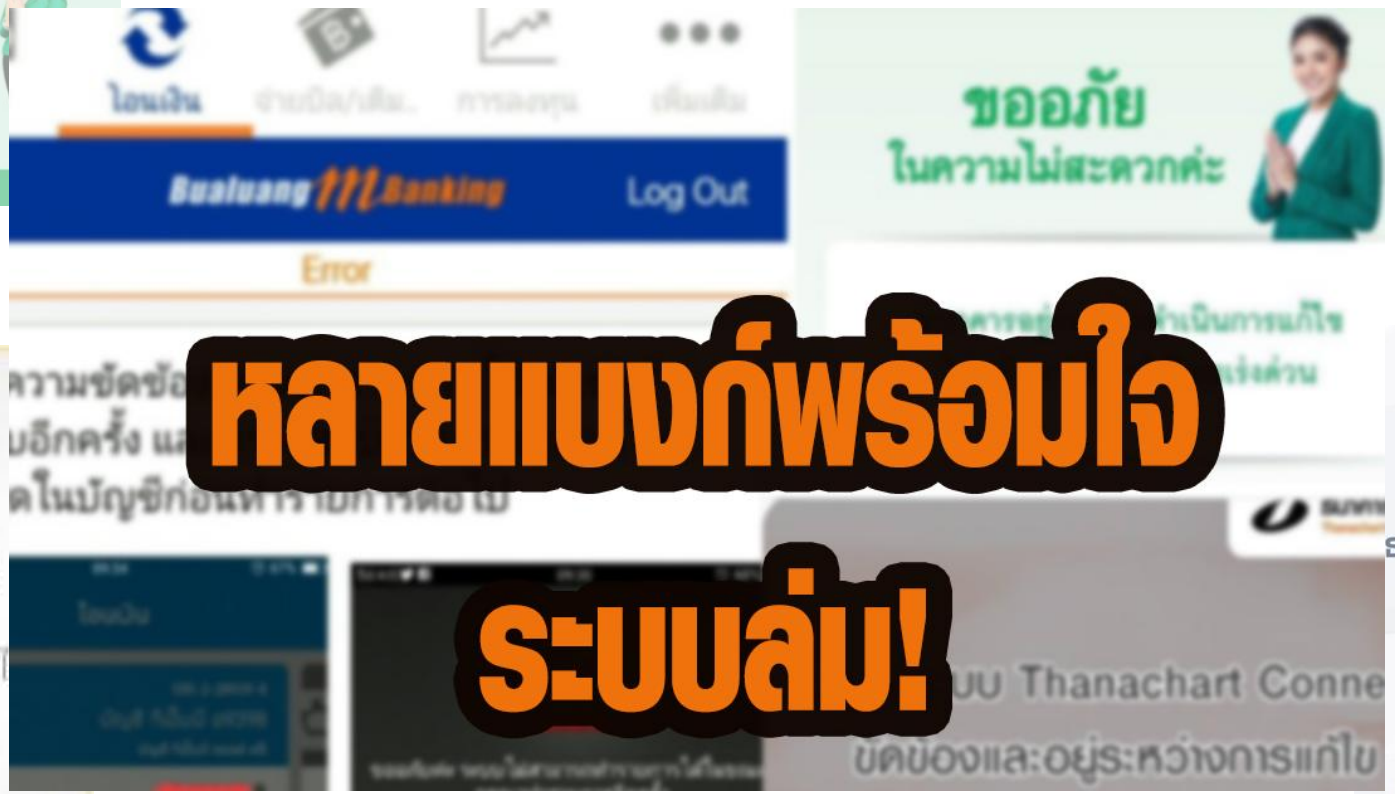
1. แล้ว Stuxnet ติดเข้ามาที่ Natanz Nuclear Facility ได้อย่างไร ทั้ง ๆ ที่มี air gap
2. ในเมื่อถูกออกแบบมาให้ทำงานกับบริบทที่**เฉพาะเจาะจง***มาก ๆ แล้วเกิดเหตุเครื่องผู้ใช้ทั่วไป booth ไม่ขึ้นได้อย่างไร

**Windows ของโรงงานนิวเคลียร์ที่อิหร่าน ซึ่งมีระบบ PLC ของ Siemens ติดตั้งอยู่เท่านั้น แถมยังต้องมีจำนวน Cascade 164 ตัว*


BAAC FAMILY
ขณะนี้ระบบการให้บริการของ ธ.ก.ส.
เกิดความขัดข้อง
อยู่ระหว่างเร่งดำเนินการแก้ไข
หากระบบสามารถกลับมาให้บริการได้
ธ.ก.ส. จะรีบแจ้งให้ท่านทราบต่อไป
ธ.ก.ส. ขออภัยในความไม่สะดวกมา ณ ที่นี้


แบงก์ระบบล่ม
ยันไม่ได้โดนแฮ็ก


ขณะนี้ บริการในช่องทางต่างๆ ของธนาคาร
ไม่สามารถใช้งานได้ชั่วคราว
ธนาคารกำลังเร่งดำเนินการแก้ไข
และคาดว่าจะสามารถใช้งานได้ตามปกติโดยเร็ว
ธนาคารขออภัยในความไม่สะดวกมา ณ โอกาสนี้


Bualuang Banking
Log Out
Error
ขออภัย
ในความไม่สะดวกค่ะ
หลายแบงก์พร้อมใจ
ระบบล่ม!


ขออภัยอย่างสูง
ในความไม่สะดวกค่ะ


ขณะนี้ระบบ
กรุงศรีโมบายแอปพลิเคชั่น (KMA)
ขัดข้องชั่วคราว
* ทั้งนี้ท่านสามารถเลือกทำรายการผ่าน
Krungsri Online และ ATM ได้ตามปกติ
ขออภัยในความไม่สะดวก
1572


ขณะนี้ระบบ KTB netbank
เกิดความขัดข้องชั่วคราว
ธนาคารกำลังดำเนินการแก้ไขอย่างเร่งด่วน
เพื่อให้กลับมาใช้บริการได้โดยเร็วที่สุด
ขออภัย
ในความไม่สะดวก
KTB Care

เปิดสถิติ ธนาคารพาณิชย์ระบบล่ม ปี 65

	ขัดข้อง	ระยะเวลา
ทหารไทยธนชาต	30 ครั้ง	96 ชม.
ไทยพาณิชย์	18 ครั้ง	16 ชม.
กรุงไทย	13 ครั้ง	19 ชม.
กรุงเทพ	5 ครั้ง	23 ชม.
กรุงศรีอยุธยา	5 ครั้ง	11 ชม.
กสิกรไทย	1 ครั้ง	1 ชม.

ที่มา : ธนาคารแห่งประเทศไทย

3Plus NEWS

today | Bizview

อัปเดตอาการล่มในปี 2566 เปิดสถิติ แอปธนาคารไหน ขยันล่ม

	ม.ค.-ก.ย. 2566	2565
กรุงเทพ	4 ครั้ง กว่า 7 ชม.	5 ครั้ง กว่า 23 ชม.
กรุงไทย	2 ครั้ง กว่า 3 ชม.	9 ครั้ง กว่า 13 ชม.
กรุงศรี	1 ครั้ง กว่า 2 ชม.	3 ครั้ง กว่า 6 ชม.
กสิกร	1 ครั้ง กว่า 2 ชม.	1 ครั้ง กว่า 1 ชม.
ทหารไทยธนชาต	2 ครั้ง กว่า 3 ชม.	22 ครั้ง กว่า 87 ชม.
ไทยพาณิชย์	4 ครั้ง กว่า 2 ชม.	18 ครั้ง กว่า 16 ชม.

รู้หรือไม่

เร็วๆ นี้ ธนาคารแห่งประเทศไทย (ธปท.) จะออกประกาศกำหนดบทลงโทษสำหรับธนาคารห้ามแอปพลิเคชันล่มเกิน 8 ชั่วโมงต่อปี หากเกินกว่านั้นจะมีโทษ ตั้งแต่ตักเตือน สั่งแก้ไข หรือปรับสูงสุด 500,000 บาท

ที่มา : รายงานข้อมูลสถิติระบบเทคโนโลยีสารสนเทศขัดข้องกระทบต่อการให้บริการสำคัญของธนาคารพาณิชย์ โดย ธนาคารแห่งประเทศไทย (ธปท.)

Business+
Management & Strategic

ที่มา : ธนาคารแห่งประเทศไทย

TIPS

ตัวเลขล่าสุดเดือน พ.ย. 2566 มีจำนวนบัญชีผู้ใช้บริการโมบายแบงก์กิ้ง รวม 106,439,691 บัญชี เพิ่มขึ้นจากช่วงเดียวกันเมื่อปีก่อน 10,794,163 บัญชี มีปริมาณรายการธุรกรรมทั้งสิ้น 2,679,189,000 รายการ เพิ่มขึ้น 642,628,000 รายการ คิดเป็นมูลค่าการทำรายการผ่านโมบายแบงก์กิ้งรวม 5.802 ล้านล้านบาท

ผลกระทบของ Cyberattack ที่มีต่อองค์กร

และ

ความรับผิดชอบของผู้บริหารต่อ Cybersecurity

Module 2: Cybersecurity Framework ของ NIST และหลักกฎหมายต่างๆ ที่เกี่ยวข้องทั้งในระดับสากล และในไทยที่องค์กรควรรู้และปฏิบัติตาม เพื่อป้องกันความเสี่ยงและหลีกเลี่ยงข้อพิพาทต่างๆ ที่อาจจะเกิดขึ้น

ความรับผิดชอบในทางกฎหมาย

พระราชบัญญัติ **คุ้มครองข้อมูลส่วนบุคคล** พ.ศ. ๒๕๖๒

พระราชบัญญัติ **ความมั่นคงปลอดภัยไซเบอร์** พ.ศ. ๒๕๖๒

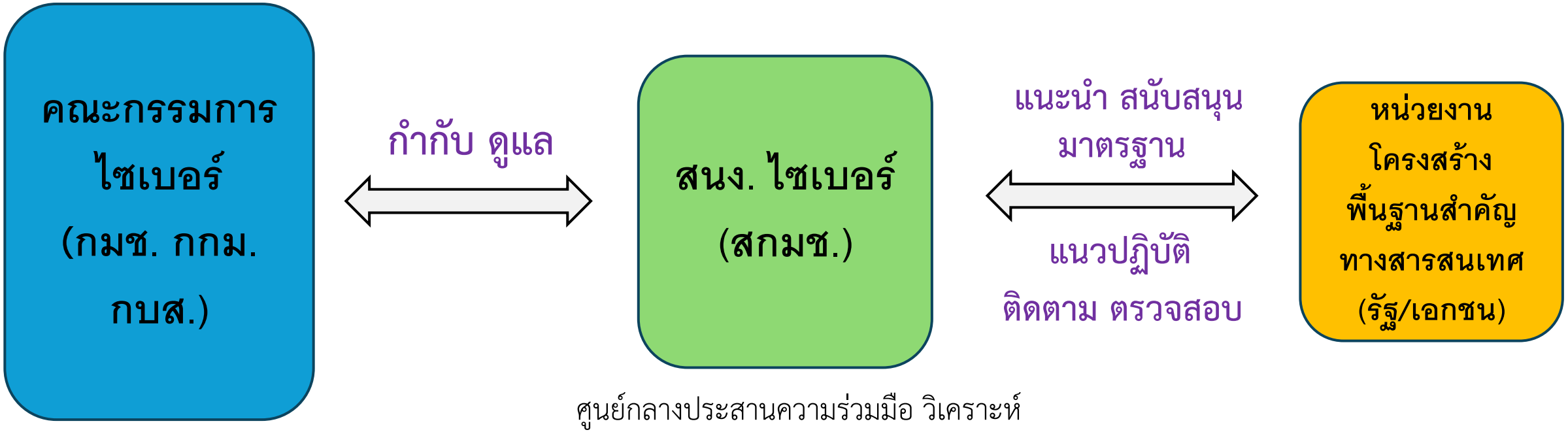
พระราชบัญญัติ **ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐**
(แก้ไข พ.ศ. ๒๕๖๐)

พระราชบัญญัติ

การรักษาความมั่นคงปลอดภัยไซเบอร์

พ.ศ. ๒๕๖๒

ภาพสรุปความสัมพันธ์ และ หน้าที่ด้านไซเบอร์



ศูนย์กลางประสานความร่วมมือ วิเคราะห์ เฝ้าระวังป้องกันภัยไซเบอร์

กมช. คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (นายกรัฐมนตรี เป็นประธาน)

กกม. คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (รมว. ดีอีเอส เป็นประธาน)

กบส. คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (รมว. ดีอีเอส เป็นประธาน)

ส่วนที่ ๓
โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

มาตรา ๔๘ โครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นกิจการที่มีความสำคัญต่อความมั่นคงของรัฐ ความมั่นคงทางทหาร ความมั่นคงทางเศรษฐกิจ และความสงบเรียบร้อยภายในประเทศ และเป็นหน้าที่ของสำนักงานในการสนับสนุนและให้ความช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

มาตรา ๔๙ ให้คณะกรรมการมีอำนาจประกาศกำหนดลักษณะหน่วยงานที่มีภารกิจหรือให้บริการในด้านดังต่อไปนี้ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๑) ด้านความมั่นคงของรัฐ

(๒) ด้านบริการภาครัฐที่สำคัญ

(๓) ด้านการเงินการธนาคาร

(๔) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม

(๕) ด้านการขนส่งและโลจิสติกส์

(๖) ด้านพลังงานและสาธารณูปโภค

(๗) ด้านสาธารณสุข

(๘) ด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม

มาตรา ๑๔ ในการดำเนินการตามมาตรา ๑๓ วรรคหนึ่ง (๒) เพื่อรับมือกับภัยคุกคามทางไซเบอร์ได้ทันท่วงที กกม. อาจมอบอำนาจให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ผู้บัญชาการทหารสูงสุด และกรรมการอื่นซึ่ง กกม. กำหนด ร่วมกันปฏิบัติการในเรื่องดังกล่าวได้ และจะกำหนดให้หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ถูกคุกคามเข้าร่วมดำเนินการ ประสานงาน และให้การสนับสนุนด้วยก็ได้

มาตรา ๑๓ กกม. มีหน้าที่และอำนาจ ดังต่อไปนี้

(๑) ติดตามการดำเนินการตามนโยบายและแผนตามมาตรา ๙ (๑) และมาตรา ๔๒

(๒) ดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ตามมาตรา ๖๑ มาตรา ๖๒ มาตรา ๖๓ มาตรา ๖๔ มาตรา ๖๕ และมาตรา ๖๖

(๓) กำกับดูแลการดำเนินงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ และการเผชิญเหตุและนิติวิทยาศาสตร์ทางคอมพิวเตอร์

(๔) กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน

(๕) กำหนดหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน้าที่ของหน่วยงานควบคุมหรือกำกับดูแล โดยอย่างน้อยต้องกำหนดหน้าที่ให้หน่วยงานควบคุมหรือกำกับดูแลต้องกำหนดมาตรฐานที่เหมาะสมเพื่อรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานของรัฐ

(๖) กำหนดระดับของภัยคุกคามทางไซเบอร์ พร้อมทั้งรายละเอียดของมาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ในแต่ละระดับเสนอต่อคณะกรรมการ

(๗) วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ เพื่อเสนอต่อคณะกรรมการพิจารณาสั่งการ เมื่อมีหรือคาดว่าจะมีภัยคุกคามทางไซเบอร์ในระดับร้ายแรงขึ้น

ในการกำหนดกรอบมาตรฐานตามวรรคหนึ่ง (๔) ให้คำนึงถึงหลักการบริหารความเสี่ยง โดยอย่างน้อยต้องประกอบด้วยวิธีการและมาตรการ ดังต่อไปนี้

(๑) การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล

(๒) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

(๓) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

(๔) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

(๕) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

“มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า การแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์โดยใช้บุคลากร กระบวนการ และเทคโนโลยี โดยผ่านคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ หรือบริการที่เกี่ยวกับคอมพิวเตอร์ใด ๆ เพื่อสร้างความมั่นใจและเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

“โครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

“หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

มาตรา ๔๒ นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ต้องมีเป้าหมายและแนวทางอย่างน้อย ดังต่อไปนี้

(๑) การบูรณาการการจัดการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ

(๒) การสร้างมาตรการและกลไกเพื่อพัฒนาศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

(๓) การสร้างมาตรการในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ

(๔) การประสานความร่วมมือระหว่างภาครัฐ เอกชน และประสานความร่วมมือระหว่างประเทศเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

(๕) การวิจัยและพัฒนาเทคโนโลยีและองค์ความรู้ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๖) การพัฒนาบุคลากรและผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งภาครัฐและเอกชน

(๗) การสร้างความตระหนักและความรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๘) การพัฒนาระเบียบและกฎหมายเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรา ๔๓ ให้คณะกรรมการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ขึ้นตามแนวทางในมาตรา ๔๒ เพื่อเสนอคณะรัฐมนตรีให้ความเห็นชอบ โดยให้ประกาศในราชกิจจานุเบกษา และเมื่อได้ประกาศแล้ว ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามที่กำหนดไว้ในแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ดำเนินการให้เป็นไปตามนโยบายและแผนดังกล่าว

ในการจัดทำนโยบายและแผนตามวรรคหนึ่ง ให้สำนักงานจัดให้มีการรับฟังความเห็นหรือประชุมร่วมกับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

มาตรา ๔๔ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว

ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่ง อย่างน้อยต้องประกอบด้วยเรื่อง ดังต่อไปนี้ **ตรวจสอบและประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง**

(๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง

(๒) แผนการรับมือภัยคุกคามทางไซเบอร์

เพื่อประโยชน์ในการจัดทำประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่ง ให้สำนักงานโดยความเห็นชอบของคณะกรรมการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานสำหรับให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนำไปใช้เป็นแนวทางในการจัดทำหรือนำไปใช้เป็นประมวลแนวทางปฏิบัติของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน และในกรณีที่หน่วยงานดังกล่าวยังไม่มีหรือมีแต่ไม่ครบถ้วนหรือไม่สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ให้นำประมวลแนวทางปฏิบัติและกรอบมาตรฐานดังกล่าวไปใช้บังคับ **ให้ สกมช. จัดทำแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์**

มาตรา ๕๔ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีผู้ตรวจประเมิน รวมทั้งต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละหนึ่งครั้ง

ประเมินความเสี่ยงและ audit ปีละครั้ง

ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการดำเนินการต่อสำนักงานภายในสามสิบวันนับแต่วันที่ดำเนินการแล้วเสร็จ

มาตรา ๕๗ เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รายงานต่อสำนักงานและหน่วยงานควบคุมหรือกำกับดูแล และปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์ตามที่กำหนดในส่วนที่ ๔ ทั้งนี้ กกม. อาจกำหนดหลักเกณฑ์และวิธีการการรายงานด้วยก็ได้

บทกำหนดโทษ

มาตรา ๗๐ ห้ามมิให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามพระราชบัญญัตินี้ให้แก่บุคคลใด ผู้ใดฝ่าฝืนต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ **จำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 6 หมื่นบาท หรือ ทั้งจำทั้งปรับ**

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้หรือผู้กระทำความผิดตามกฎหมายอื่นหรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ

มาตรา ๗๑ พนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลของผู้ใช้บริการหรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ที่ได้มาตามพระราชบัญญัตินี้ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ **จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 2 หมื่นบาท หรือ ทั้งจำทั้งปรับ**

มาตรา ๗๒ ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลของผู้ใช้บริการ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใดโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ **จำคุกไม่เกิน 2 ปี หรือปรับไม่เกิน 4 หมื่นบาท หรือ ทั้งจำทั้งปรับ**

มาตรา ๗๓ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดไม่รายงานเหตุภัยคุกคามทางไซเบอร์ตามมาตรา ๕๗ โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกินสองแสนบาท

ปรับไม่เกิน 2 แสนบาท

มาตรา ๗๔ ผู้ใดไม่ปฏิบัติตามหนังสือเรียกของพนักงานเจ้าหน้าที่หรือไม่ส่งข้อมูลให้แก่พนักงานเจ้าหน้าที่ตามมาตรา ๖๒ (๑) หรือ (๒) โดยไม่มีเหตุอันสมควรแล้วแต่กรณี ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท **ปรับไม่เกิน 1 แสนบาท**

มาตรา ๗๕ ผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามคำสั่งของ กกม. ตามมาตรา ๖๕ (๑) และ (๒) โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกินสามแสนบาท และปรับอีกไม่เกินวันละหนึ่งหมื่นบาทนับแต่วันที่ครบกำหนดระยะเวลาที่ กกม. ออกคำสั่งให้ปฏิบัติจนกว่าจะปฏิบัติให้ถูกต้อง

ผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามคำสั่งของ กกม. ตามมาตรา ๖๕ (๓) และ (๔) หรือไม่ปฏิบัติตามคำสั่งศาลตามมาตรา ๖๕ (๕) ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ **จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 2 หมื่นบาท หรือ ทั้งจำทั้งปรับ**

มาตรา ๗๖ ผู้ใดขัดขวาง หรือไม่ปฏิบัติตามคำสั่งของ กกม. หรือพนักงานเจ้าหน้าที่ซึ่งปฏิบัติการตามคำสั่งของ กกม. ตามมาตรา ๖๖ (๑) หรือไม่ปฏิบัติตามคำสั่งศาลตามมาตรา ๖๖ (๒) (๓) หรือ (๔) โดยไม่มีเหตุอันสมควร ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ **จำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 6 หมื่นบาท หรือ ทั้งจำทั้งปรับ**

มาตรา ๗๗ ในกรณีที่ผู้กระทำความผิดตามพระราชบัญญัตินี้เป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย **ผู้สั่งการเป็นผู้รับโทษ**

พระราชบัญญัติ

คุ้มครองข้อมูลส่วนบุคคล

พ.ศ. ๒๕๖๒

สรุปบทลงโทษ

สรุป บทกำหนดโทษ ตาม พรบ.

PDPA เป็นกฎหมายที่สร้างขึ้นเพื่อ

คุ้มครองบุคคล (Data Subject)

ใครถูกปรับเท่าไหร่บ้าง

TOTAL NUMBER OF GDPR FINES

465

LARGEST FINE

€50,000,000 — Google Inc.

SMALLEST FINE

€28 — Google Ireland Ltd.

From May 2018 – January 2020

TOP 5 BIGGEST GDPR FINES

1	Google Inc.		€50 000 000
2	H&M Hennes & Mauritz		€35 200 000
3	TIM - Telecom Provider		€27 800 000
4	British Airways		€21 900 000
5	Marriott International		€20 450 000

Source: https://dataprivacymanager.net/

การร้องเรียน

หน้าที่ของคณะกรรมการผู้เชี่ยวชาญ

มาตรา 72

1. พิจารณาเรื่องร้องเรียน
2. ตรวจสอบการกระทำใด ๆ ของผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้าง หรือ ผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล
3. ไกล่เกลี่ยข้อพิพาทเกี่ยวกับข้อมูลส่วนบุคคล
4. ออกคำสั่งให้ปฏิบัติหรือดำเนินการแก้ไขการกระทำ/
5. สั่งห้ามกระทำการเพื่อระงับความเสียหาย

บทลงโทษตาม PDPA

ความรับผิดทางแพ่ง มาตรา 77-78

ค่าสินไหมทดแทนจากความเสียหายที่ได้รับจริง และศาลสั่งลงโทษเพิ่มขึ้นได้แต่ไม่เกินสองเท่าของสินไหมทดแทนที่แท้จริง

โทษทางปกครอง มาตรา 82 - 87

โทษปรับไม่เกิน 1,000,000 บาท

ไม่ขอความยินยอมให้ถูกต้อง ไม่แจ้งรายละเอียดให้เจ้าของข้อมูลทราบ ไม่ให้เจ้าของข้อมูลเข้าถึงข้อมูลตามสิทธิ ไม่จัดทำบันทึกรายการ ไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ไม่จัดให้มีการสนับสนุนการปฏิบัติหน้าที่ของ DPO

บทลงโทษตาม PDPA

โทษทางปกครอง มาตรา 82 - 87

โทษปรับไม่เกิน 3,000,000 บาท

เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากฐานทางกฎหมาย ไม่ได้แจ้งวัตถุประสงค์การใช้งานใหม่ เก็บข้อมูลเกินความจำเป็น ขอความยินยอมที่เป็นการหลอกลวงให้เข้าใจผิด ไม่จัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสม ไม่แจ้งเหตุเมื่อมีการละเมิดข้อมูล โอนข้อมูลไปต่างประเทศโดยไม่ชอบด้วยกฎหมาย ไม่ตั้งตัวแทนในราชอาณาจักร

โทษทางปกครอง มาตรา 82 - 87

โทษปรับไม่เกิน 5,000,000 บาท

เก็บรวบรวม ใช้ เปิดเผยหรือโอนข้อมูลส่วนบุคคลอ่อนไหวโดยไม่ชอบด้วยกฎหมาย

บทลงโทษตาม PDPA

โทษอาญา มาตรา 79 - 81

ผู้ควบคุมข้อมูลส่วนบุคคล ใช้หรือเปิดเผยข้อมูลส่วนบุคคลอ่อนไหว โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือผิดจากวัตถุประสงค์ที่ได้แจ้งไว้ หรือ โอนข้อมูลส่วนบุคคลอ่อนไหวไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย

- ทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย **จำคุก <= 6 เดือน หรือ ปรับ <= 500,000 บาท**
- เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น **จำคุก <= 1 ปี หรือ ปรับ <= 500,000 บาท**

บทลงโทษตาม PDPA

โทษอาญา มาตรา 79 - 81

ผู้ใด ล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ ตามพ.ร.บ.นี้
ห้ามนำไปเปิดเผยแก่ผู้อื่น เว้นแต่เปิดเผยตามหน้าที่
หรือ เพื่อประโยชน์แก่การสอบสวนหรือพิจารณาคดี
หรือ ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล
หรือ เปิดเผยให้หน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย
หรือ ข้อมูลคดีต่างๆ ที่เปิดเผยต่อสาธารณะ

จำคุก <= 6 เดือน หรือ ปรับ <= 500,000 บาท

บทลงโทษตาม PDPA

โทษอาญา มาตรา 79 - 81

ผู้กระทำความผิดที่เป็นนิติบุคคล หาก**กรรมการหรือผู้จัดการ หรือ บุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น**

สั่งการหรือกระทำหรือละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ต้องรับโทษในส่วนที่กำหนดโทษอาญาไว้ด้วย

สิทธิขอเข้าถึงและขอรับสำเนา มาตรา 30 (Right of Access)

เจ้าของข้อมูลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลที่เกี่ยวกับตนหรือขอให้เปิดเผยถึงการได้มาของข้อมุลที่ไม่ได้ให้ความยินยอม ผู้ควบคุมจะปฏิเสธได้ก็เฉพาะเมื่อเป็นการปฏิเสธตามคำสั่งศาลหรือตามกฎหมาย หรือเป็นการขอเข้าถึงที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพผู้อื่น

สิทธิขอให้โอนข้อมูล มาตรา 31
(Right to data portability)

จะใช้สิทธินี้ได้ต้องเป็นข้อมูลที่เก็บรวบรวมจากการให้ความยินยอมหรือฐานสัญญา ตามมาตรา 24 (3) เท่านั้น

สิทธิคัดค้าน มาตรา 32 (Right to object)

จะใช้สิทธินี้ได้ต้องเป็นข้อมูลที่เก็บรวบรวมจากฐานภารกิจของรัฐตามมาตรา 24 (4) และฐานการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายตามมาตรา 24 (5) หรือเก็บรวบรวมเพื่อการตลาดแบบตรง หรือเพื่อการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติเท่านั้น

สิทธิขอให้ลบหรือทำลาย มาตรา 33 (Right to be forgotten)

ไม่สามารถใช้สิทธินี้ได้หากเก็บข้อมูลไว้เพื่อการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ หรือเป็นการศึกษาวิจัยหรือสถิติตามมาตรา 24 (1) หรือเพื่อการดำเนินภารกิจของรัฐตามมาตรา 24 (4) หรือเป็นข้อมูลอ่อนไหวเพื่อประโยชน์ทางการแพทย์หรือการสาธารณสุขตามมาตรา 26 (5) (ก) หรือ (ข)

สิทธิขอให้ระงับการใช้ มาตรา 34 (Right to restrict processing)

มีสิทธิขอให้ระงับการใช้ได้ชั่วคราว

สิทธิขอให้แก้ไขข้อมูลให้ถูกต้อง มาตรา 35 (Right to rectification)

มีสิทธิขอให้ผู้ควบคุมแก้ไขข้อมูลให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

พระราชบัญญัติ

ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ศ. ๒๕๕๐ (แก้ไข พ.ศ.๒๕๖๐)

สรุปบทลงโทษ

(เดิม) มาตรา ๕ ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุก ไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

(เดิม) มาตรา ๖ ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุก ไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

(เดิม) มาตรา ๗ ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง โดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุก ไม่เกินสองปี หรือ ปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

(เดิม) มาตรา ๘ ผู้ใดกระทำด้วยประการใดโดยมิชอบ ด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุก ไม่เกินสามปี หรือ ปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

(เดิม) มาตรา ๑๑ ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าวอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวาง**โทษปรับไม่เกินหนึ่งแสนบาท**

(ใหม่) มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ หรือมาตรา ๑๑ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือ โครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงเจ็ดปี และปรับตั้งแต่ สองหมื่นบาท ถึง หนึ่งแสนสี่หมื่นบาท

(ใหม่) ถ้าการกระทำความผิดตามวรรคหนึ่งเป็นเหตุให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ดังกล่าว ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี และปรับตั้งแต่ สองหมื่นบาท ถึง สองแสนบาท

(เดิม) มาตรา ๙ ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(เดิม) มาตรา ๑๐ ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่น ถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถ ทำงานตามปกติได้ต้องระวางโทษจำคุก ไม่เกินห้าปี หรือปรับ ไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

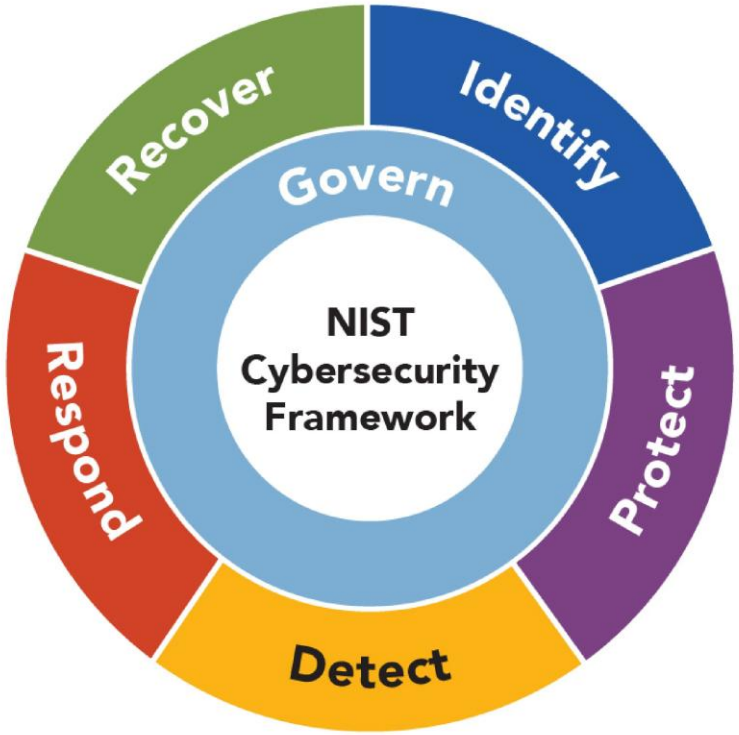
(ใหม่) ถ้าการกระทำความผิดตามมาตรา ๙ หรือ มาตรา ๑๐ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ตามวรรคหนึ่ง ต้องระวาง โทษจำคุกตั้งแต่ สามปี ถึง สิบห้าปี และ ปรับตั้งแต่หกหมื่นบาท ถึง สามแสนบาท

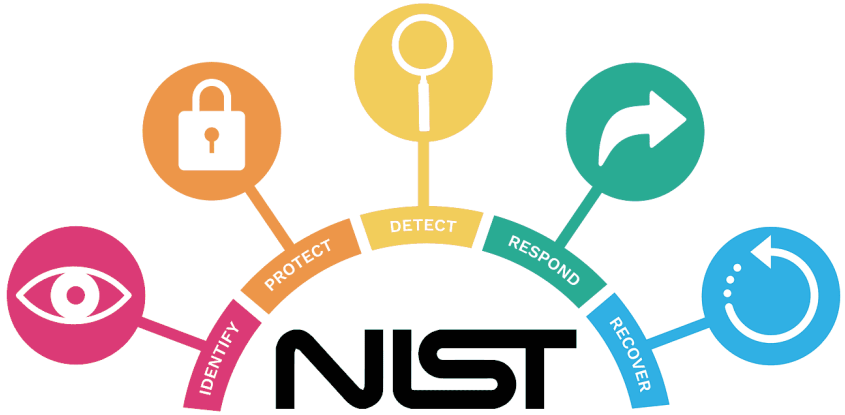
(ใหม่) ถ้าการกระทำความผิดตามวรรคหนึ่งหรือ วรรคสามโดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ ห้าปีถึงยี่สิบปี และปรับตั้งแต่ หนึ่งแสนบาท ถึงสี่แสนบาท

(ใหม่) มาตรา ๑๒/๑ ถ้าการกระทำความผิดตาม มาตรา ๙ หรือมาตรา ๑๐ เป็นเหตุให้เกิดอันตราย แก่บุคคลอื่นหรือทรัพย์สินของผู้อื่น ต้องระวาง**โทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท**

(ใหม่) ถ้าการกระทำความผิดตามมาตรา ๙ หรือ มาตรา ๑๐ โดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย ต้องระวาง**โทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท**

Cybersecurity Framework ของ NIST





NIST
National Institute of Standards and Technology
U.S. Department of Commerce

1. Cybersecurity Framework (CSF) Overview

This document is version 2.0 of the NIST Cybersecurity Framework (*Framework* or *CSF*). It includes the following components:

- ***CSF Core***, the nucleus of the CSF, which is a taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks. The CSF Core components are a hierarchy of Functions, Categories, and Subcategories that detail each outcome. These outcomes can be understood by a broad audience, including executives, managers, and practitioners, regardless of their cybersecurity expertise. Because the outcomes are sector-, country-, and technology-neutral, they provide an organization with the flexibility needed to address its unique risks, technologies, and mission considerations.
- ***CSF Organizational Profiles***, which are a mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes.
- ***CSF Tiers***, which can be applied to CSF Organizational Profiles to characterize the rigor of an organization's cybersecurity risk governance and management practices. Tiers can also provide context for how an organization views cybersecurity risks and the processes in place to manage those risks.

This document describes *what* desirable outcomes an organization can aspire to achieve. It does not *prescribe* outcomes nor *how* they may be achieved. Descriptions of *how* an organization can achieve those outcomes are provided in a suite of online resources that complement the CSF and are available through the NIST CSF website. These resources offer additional guidance on practices and controls that could be used to achieve outcomes and are intended to help an organization understand, adopt, and use the CSF. They include:

- *Informative References* that point to sources of guidance on each outcome from existing global standards, guidelines, frameworks, regulations, policies, etc.
- *Implementation Examples* that illustrate potential ways to achieve each outcome
- *Quick-Start Guides* that give actionable guidance on using the CSF and its online resources, including transitioning from previous CSF versions to version 2.0
- *Community Profiles* and *Organizational Profile Templates* that help an organization put the CSF into practice and set priorities for managing cybersecurity risks

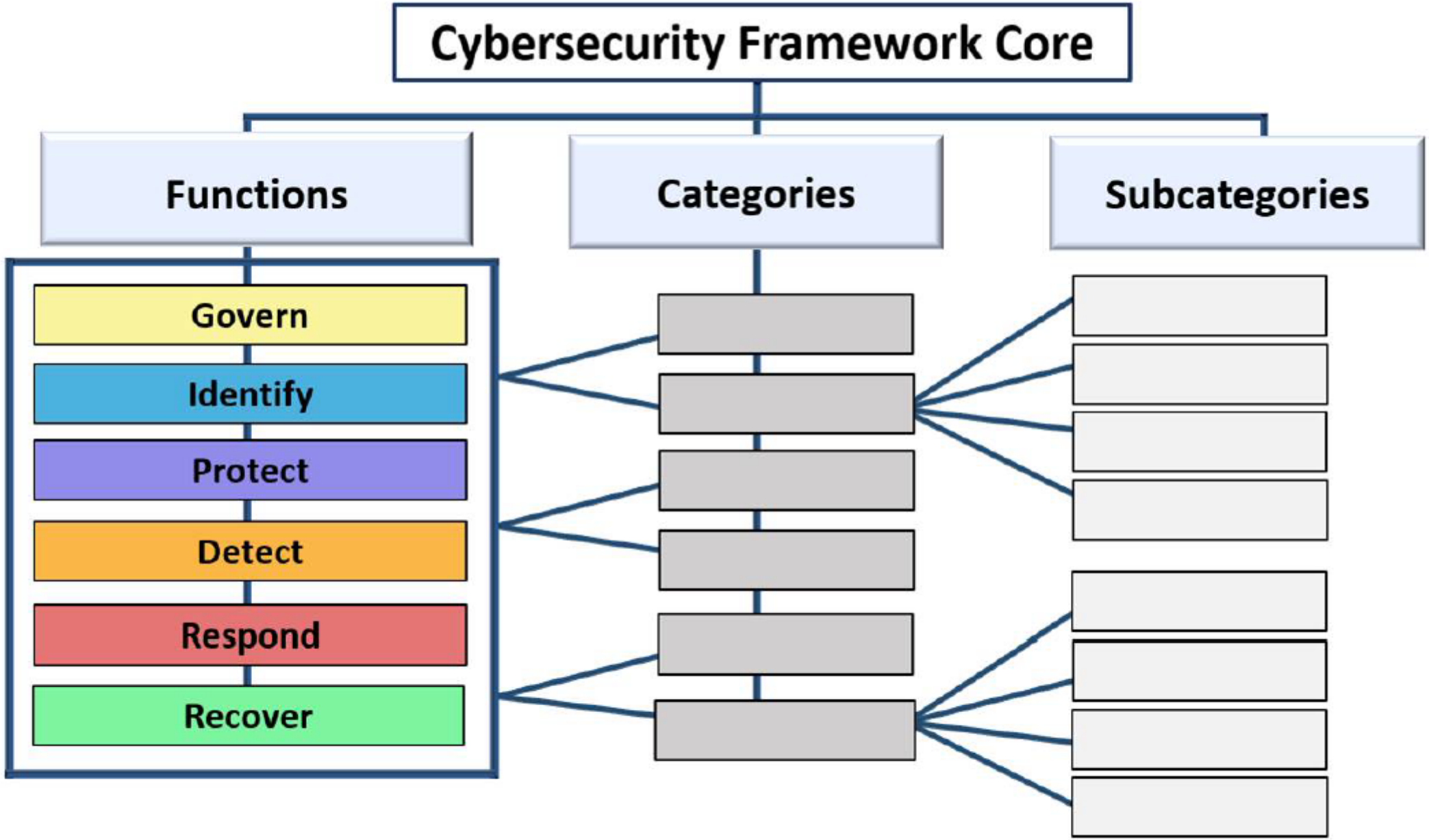


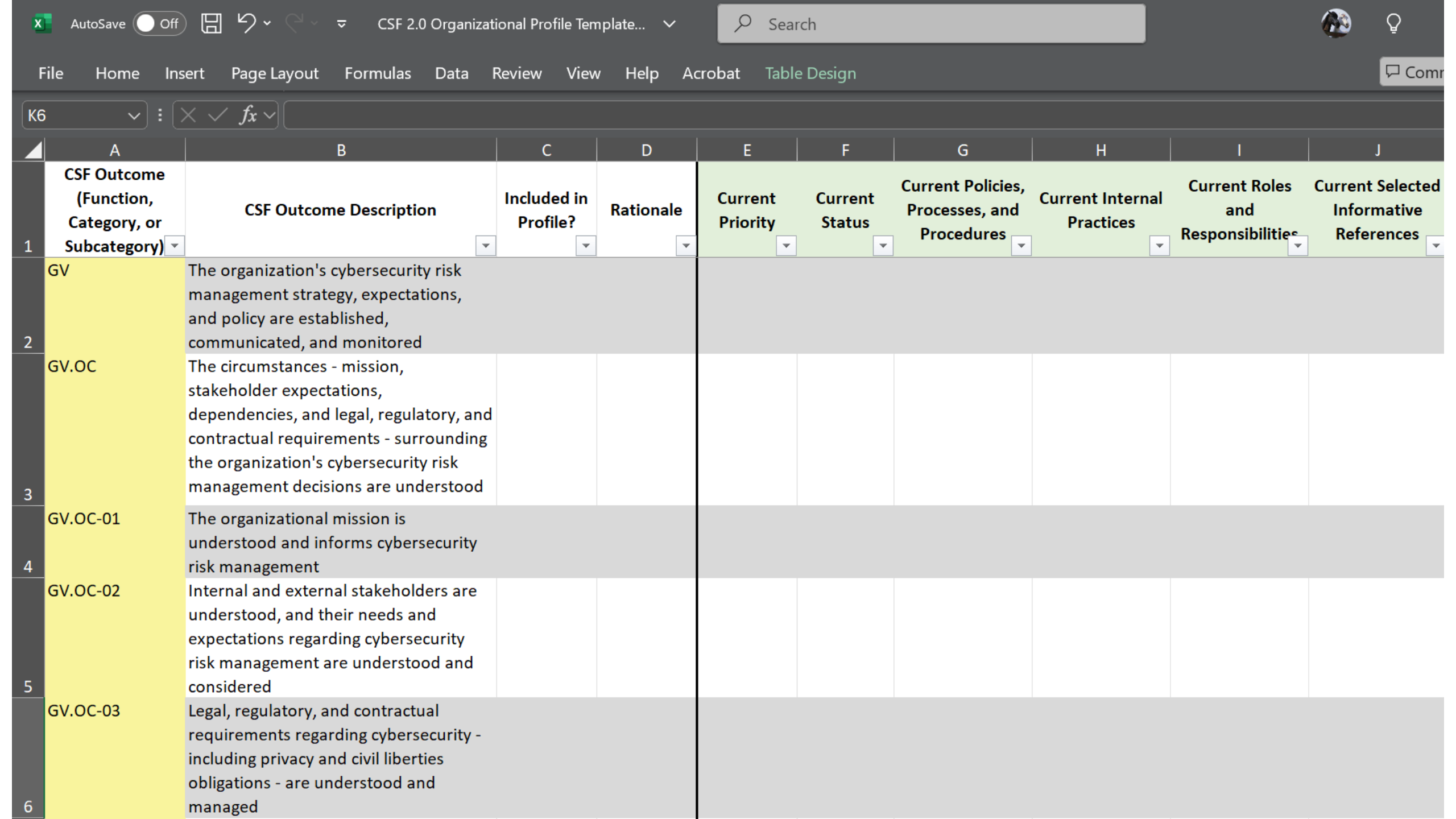
Fig. 1. CSF Core structure

Table 1. CSF 2.0 Core Function and Category names and identifiers

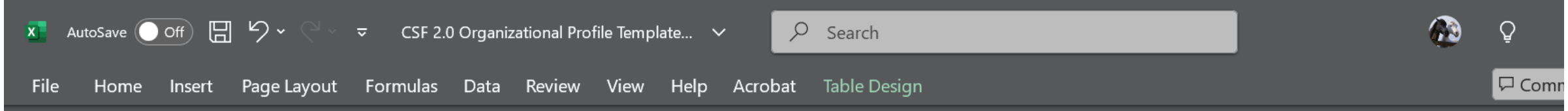
Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR

Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF Organization Profile Template



	A	B	C	D	E	F	G	H	I	J
1	CSF Outcome (Function, Category, or Subcategory)	CSF Outcome Description	Included in Profile?	Rationale	Current Priority	Current Status	Current Policies, Processes, and Procedures	Current Internal Practices	Current Roles and Responsibilities	Current Selected Informative References
2	GV	The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored								
3	GV.OC	The circumstances - mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood								
4	GV.OC-01	The organizational mission is understood and informs cybersecurity risk management								
5	GV.OC-02	Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered								
6	GV.OC-03	Legal, regulatory, and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed								



	A	B	C	D	E	F	G	H	I	J
1	CSF Outcome (Function, Category, or Subcategory)	CSF Outcome Description	Included in Profile?	Rationale	Current Priority	Current Status	Current Policies, Processes, and Procedures	Current Internal Practices	Current Roles and Responsibilities	Current Selected Informative References
40	ID	The organization's current cybersecurity risks are understood								
41	ID.AM	Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy								
42	ID.AM-01	Inventories of hardware managed by the organization are maintained								
43	ID.AM-02	Inventories of software, services, and systems managed by the organization are maintained								
44	ID.AM-03	Representations of the organization's authorized network communication and internal and external network data flows are maintained								
45	ID.AM-04	Inventories of services provided by suppliers are maintained								
46	ID.AM-05	Assets are prioritized based on classification, criticality, resources, and impact on the mission								
	ID.AM-07	Inventories of data and corresponding metadata for designated data types are								

CSF Implementation Example

NIST Cybersecurity Framework (CSF) 2.0 Reference Tool

Function			
GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored			
	Category Organizational Context (GV.OC): The circumstances - mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood		
		Subcategory	**Implementation Examples**
		GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	**Ex1:** Share the organization's mission (e.g., through vision and mission statements, marketing, and service strategies) to provide a basis for identifying risks that may impede that mission
		GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	**Ex1:** Identify relevant internal stakeholders and their cybersecurity-related expectations (e.g., performance and risk expectations of officers, directors, and advisors; cultural expectations of employees) **Ex2:** Identify relevant external stakeholders and their cybersecurity-related expectations (e.g., privacy expectations of customers, business expectations of partnerships, compliance expectations of regulators, ethics expectations of society)

NIST Cybersecurity Framework (CSF) 2.0 Reference Tool

Function			
IDENTIFY (ID): The organization's current cybersecurity risks are understood			
	Category **Asset Management (ID.AM):** Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy		
		Subcategory	**Implementation Examples**
		ID.AM-01: Inventories of hardware managed by the organization are maintained	**Ex1:** Maintain inventories for all types of hardware, including IT, IoT, OT, and mobile devices **Ex2:** Constantly monitor networks to detect new hardware and automatically update inventories
		ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained	**Ex1:** Maintain inventories for all types of software and services, including commercial-off-the-shelf, open-source, custom applications, API services, and cloud-based applications and services **Ex2:** Constantly monitor all platforms, including containers and virtual machines, for software and service inventory changes **Ex3:** Maintain an inventory of the organization's systems

NIST Cybersecurity Framework (CSF) 2.0 Reference Tool

Function			
PROTECT (PR): Safeguards to manage the organization's cybersecurity risks are used			
	Category **Identity Management, Authentication, and Access Control (PR.AA):** Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access		
		Subcategory	**Implementation Examples**
		PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization	**Ex1:** Initiate requests for new access or additional access for employees, contractors, and others, and track, review, and fulfill the requests, with permission from system or data owners when needed **Ex2:** Issue, manage, and revoke cryptographic certificates and identity tokens, cryptographic keys (i.e., key management), and other credentials **Ex3:** Select a unique identifier for each device from immutable hardware characteristics or an identifier securely provisioned to the device **Ex4:** Physically label authorized hardware with an identifier for inventory and servicing purposes

NIST Cybersecurity Framework (CSF) 2.0 Reference Tool

Function			
DETECT (DE): Possible cybersecurity attacks and compromises are found and analyzed			
	Category **Continuous Monitoring (DE.CM):** Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events		
		Subcategory	**Implementation Examples**
		DE.CM-01: Networks and network services are monitored to find potentially adverse events	**Ex1:** Monitor DNS, BGP, and other network services for adverse events **Ex2:** Monitor wired and wireless networks for connections from unauthorized endpoints **Ex3:** Monitor facilities for unauthorized or rogue wireless networks **Ex4:** Compare actual network flows against baselines to detect deviations **Ex5:** Monitor network communications to identify changes in security postures for zero trust purposes

NIST Cybersecurity Framework (CSF) 2.0 Reference Tool

Function			
RESPOND (RS): Actions regarding a detected cybersecurity incident are taken			
	Category **Incident Management (RS.MA):** Responses to detected cybersecurity incidents are managed		
		Subcategory	**Implementation Examples**
		RS.MA-02: Incident reports are triaged and validated	**Ex1:** Preliminarily review incident reports to confirm that they are cybersecurity-related and necessitate incident response activities **Ex2:** Apply criteria to estimate the severity of an incident
		RS.MA-03: Incidents are categorized and prioritized	**Ex1:** Further review and categorize incidents based on the type of incident (e.g., data breach, ransomware, DDoS, account compromise) **Ex2:** Prioritize incidents based on their scope, likely impact, and time-critical nature **Ex3:** Select incident response strategies for active incidents by balancing the need to quickly recover from an incident with the need to observe the attacker or conduct a more thorough investigation

Module 3: Cyberattack Landscape ในประเทศไทย
ตัวอย่างรูปแบบการโจมตี การรั่วไหล วิเคราะห์ความเสี่ยง
ภัยคุกคามมาจากไหนได้บ้าง
มาตรการป้องกันควรมีแนวทางป้องกันกันอย่างไร

รูปแบบการโจมตีทางไซเบอร์

1. Man-in-the-Middle (MitM) Attack:

คำอธิบาย: ผู้โจมตีแทรกตัวอยู่ระหว่างการสื่อสารระหว่างสองฝ่าย (เช่น ระหว่างผู้ใช้กับเว็บไซต์) เพื่อดักจับ, ดัดแปลง หรือสอดแนมข้อมูลที่ส่งผ่านไปมา

ตัวอย่าง: การดักจับข้อมูลการเข้าสู่ระบบ Wi-Fi สาธารณะ หรือการปลอมแปลงเว็บไซต์เพื่อดักจับข้อมูลส่วนตัว

2. SQL Injection:

คำอธิบาย: ผู้โจมตีใช้ช่องโหว่ในโค้ดของแอปพลิเคชันที่เชื่อมต่อกับฐานข้อมูล เพื่อแทรกคำสั่ง SQL ที่เป็นอันตรายเข้าไป ซึ่งอาจทำให้สามารถเข้าถึง, แก้ไข หรือลบข้อมูลในฐานข้อมูลได้

ตัวอย่าง: การกรอกข้อมูลที่เป็นโค้ด SQL ในช่องกรอกข้อมูลของเว็บไซต์เพื่อเข้าถึงข้อมูลผู้ใช้

3. Zero-Day Exploit:

คำอธิบาย: การโจมตีโดยใช้ช่องโหว่ในซอฟต์แวร์หรือระบบที่ยังไม่เป็นที่รู้จัก หรือยังไม่มีการแก้ไขจากผู้ผลิต

ตัวอย่าง: การใช้ช่องโหว่ที่เพิ่งถูกค้นพบเพื่อแพร่กระจายมัลแวร์หรือควบคุมระบบ

4. Cross-Site Scripting (XSS):

คำอธิบาย: ผู้โจมตีแทรกสคริปต์ที่เป็นอันตรายเข้าไปในเว็บไซต์ที่น่าเชื่อถือ เพื่อให้สคริปต์นั้นทำงานในเบราว์เซอร์ของผู้ใช้งานคนอื่น ๆ และขโมยข้อมูลหรือควบคุมบัญชี

ตัวอย่าง: การฝังโค้ด JavaScript ในความคิดเห็นของเว็บบอร์ดเพื่อขโมยคุกกี้ของผู้ใช้งาน

5. Password Attack:

คำอธิบาย: การพยายามถอดรหัสหรือเข้าถึงรหัสผ่านของผู้ใช้ด้วยวิธีต่างๆ เช่น การสุ่มรหัส (Brute-Force Attack), การใช้พจนานุกรม (Dictionary Attack), หรือการใช้รหัสผ่านที่ถูกขโมยมาก่อน

ตัวอย่าง: การใช้โปรแกรมสุ่มรหัสผ่านเพื่อพยายามเข้าสู่บัญชีอีเมลหรือบัญชีโซเชียลมีเดีย

6. Eavesdropping/Sniffing:

คำอธิบาย: การดักจับข้อมูลที่ส่งผ่านเครือข่ายโดยไม่ได้รับอนุญาต โดยใช้โปรแกรมหรืออุปกรณ์พิเศษ

ตัวอย่าง: การใช้โปรแกรมดักจับข้อมูลบนเครือข่าย Wi-Fi เพื่อดูข้อมูลที่ผู้ใช้กำลังส่งผ่าน

7. Drive-by Download:

คำอธิบาย: การดาวน์โหลดมัลแวร์ลงในคอมพิวเตอร์ของผู้ใช้โดยอัตโนมัติ โดยที่ผู้ใช้ไม่รู้ตัว เพียงแค่เข้าชมเว็บไซต์ที่ถูกบุกรุก

ตัวอย่าง: การเข้าเว็บไซต์ที่มีโค้ดฝังเพื่อดาวน์โหลดมัลแวร์โดยอัตโนมัติ

8. DNS Spoofing/Cache Poisoning:

คำอธิบาย: ผู้โจมตีแก้ไขการจับคู่ระหว่างชื่อโดเมนกับ IP Address เพื่อให้ผู้ใช้ถูกเปลี่ยนเส้นทางไปยังเว็บไซต์ปลอม
ตัวอย่าง: เมื่อผู้ใช้พิมพ์ชื่อเว็บไซต์ที่ถูกต้อง แต่ถูกเปลี่ยนเส้นทางไปยังเว็บไซต์ที่ผู้โจมตีควบคุม
คำอธิบายเพิ่มเติม:

- DNS Server (Domain Name System Server): เป็นเหมือนสมุดโทรศัพท์ของอินเทอร์เน็ต ทำหน้าที่แปลงชื่อโดเมน (เช่น google.com) ให้เป็น IP Address (เช่น 172.217.160.142) ที่คอมพิวเตอร์ใช้สื่อสารกันได้
- Recursive Resolver: เป็น DNS Server ที่รับคำขอจากผู้ใช้ และทำการสืบค้นหา IP Address ของโดเมนที่ถูกร้องขอให้จนได้คำตอบ ถ้าไม่มีข้อมูลใน Cache (หน่วยความจำชั่วคราว) ก็จะส่งคำขอต่อไปยัง DNS Server ระดับสูงกว่า
- Cache: Recursive Resolver จะเก็บข้อมูลการจับคู่ชื่อโดเมนกับ IP Address ที่เคยค้นหาไว้ใน Cache เพื่อให้การตอบคำขอครั้งต่อไปทำได้เร็วขึ้น

วิธีการโจมตี DNS Spoofing/Cache Poisoning:

- การแทรกข้อมูลปลอม: ผู้โจมตีจะส่งข้อมูล DNS Response (คำตอบ) ที่ปลอมแปลงมาไปยัง Recursive Resolver โดยที่ข้อมูลนั้นมี IP Address ที่ผิดพลาด ซึ่งชี้ไปยังเว็บไซต์ปลอมที่ผู้โจมตีควบคุม
- การใช้ช่องโหว่: ผู้โจมตีอาจใช้ช่องโหว่ในซอฟต์แวร์ของ DNS Server เพื่อแทรกข้อมูลปลอมเข้าไปใน Cache
- การเดา Transaction ID: เมื่อ Recursive Resolver ส่งคำขอ DNS ไปยัง Authoritative Name Server (DNS Server ที่เก็บข้อมูลจริงของโดเมน) จะมีการใช้ Transaction ID เพื่อระบุคำขอแต่ละครั้ง ผู้โจมตีอาจพยายามเดา Transaction ID เพื่อส่งคำตอบปลอมที่ตรงกับคำขอที่กำลังดำเนินการอยู่

DNS Table

HOSTNAME	IP ADDRESSES	OPERATOR
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	Verisign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California, Information Sciences Institute
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	Verisign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

9. Advanced Persistent Threat (APT):

คำอธิบาย: การโจมตีที่ซับซ้อนและใช้เวลานาน โดยมีเป้าหมายเฉพาะเจาะจง เพื่อแทรกซึมเข้าไปในระบบและขโมยข้อมูล หรือก่อให้เกิดความเสียหายอย่างต่อเนื่อง

ตัวอย่าง: การโจมตีหน่วยงานรัฐหรือบริษัทขนาดใหญ่เพื่อขโมยข้อมูลลับ

10. Supply Chain Attack:

คำอธิบาย: การโจมตีโดยการแทรกซึมเข้าไปในซอฟต์แวร์หรือฮาร์ดแวร์ของบริษัทผู้ผลิต เพื่อทำให้ผู้ใช้งานปลายทางได้รับผลกระทบ

ตัวอย่าง: การแทรกมัลแวร์เข้าไปในโปรแกรมอัปเดตของซอฟต์แวร์

11. Malware (มัลแวร์)

คำอธิบาย: มัลแวร์เป็นคำกว้าง ๆ ที่ใช้เรียกซอฟต์แวร์ที่เป็นอันตราย ซึ่งถูกออกแบบมาเพื่อทำลาย, ขัดขวาง, หรือเข้าถึงระบบคอมพิวเตอร์หรือเครือข่ายโดยไม่ได้รับอนุญาต มัลแวร์มีหลายประเภท แต่ละประเภทก็มีวิธีการทำงานและเป้าหมายที่แตกต่างกันไป

ประเภทของมัลแวร์ที่พบบ่อย:

- ไวรัส (Virus): มัลแวร์ที่แนบตัวเองไปกับไฟล์อื่น ๆ และจะทำงานเมื่อไฟล์นั้นถูกเปิดหรือใช้งาน ไวรัสสามารถแพร่กระจายไปยังไฟล์อื่น ๆ และทำลายข้อมูลหรือทำให้ระบบทำงานผิดปกติได้
- แรนซัมแวร์ (Ransomware): มัลแวร์ที่เข้ารหัสไฟล์ของผู้ใช้ ทำให้ไม่สามารถเข้าถึงข้อมูลได้ จากนั้นผู้โจมตีจะเรียกร้องค่าไถ่เพื่อแลกกับการถอดรหัสไฟล์
- สปายแวร์ (Spyware): มัลแวร์ที่แอบติดตามกิจกรรมของผู้ใช้บนคอมพิวเตอร์ เช่น บันทึกการกดแป้นพิมพ์ ข้อมูลการท่องเว็บ หรือข้อมูลส่วนตัวอื่น ๆ เพื่อส่งข้อมูลเหล่านี้ไปยังผู้โจมตี
- หนอน (Worm): มัลแวร์ที่สามารถแพร่กระจายตัวเองไปยังคอมพิวเตอร์อื่น ๆ ในเครือข่ายโดยไม่ต้องอาศัยการกระทำของผู้ใช้ ซึ่งต่างจากไวรัสที่ต้องอาศัยการเปิดไฟล์
- โทรจัน (Trojan): มัลแวร์ที่แฝงตัวมาในรูปแบบของโปรแกรมหรือไฟล์ที่ดูเหมือนปกติ แต่เมื่อถูกเปิดใช้งานแล้วจะทำการโจมตีระบบ

12. Phishing (ฟิชชิง)

คำอธิบาย: ฟิชชิงเป็นการโจมตีที่ใช้วิธีการหลอกลวงเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลหรือข้อมูลทางการเงินของผู้ใช้ โดยมักจะมาในรูปแบบของข้อความหรืออีเมลที่ดูเหมือนมาจากองค์กรที่น่าเชื่อถือ

ประเภทของฟิชชิง:

- อีเมลหลอกลวง (Email Phishing): การส่งอีเมลที่หลอกลวงให้ผู้รับเปิดเผยข้อมูลส่วนตัว เช่น รหัสผ่าน, หมายเลขบัตรเครดิต หรือข้อมูลบัญชีธนาคาร โดยอ้างเหตุผลต่าง ๆ เช่น การยืนยันบัญชี หรือการได้รับรางวัล
- เอสเอ็มเอสหลอกลวง (Smishing): การส่งข้อความ SMS ที่หลอกลวงในลักษณะเดียวกับอีเมลฟิชชิง
- การหลอกลวงทางโทรศัพท์ (Vishing): การโทรศัพท์หลอกลวง โดยอ้างว่าเป็นเจ้าหน้าที่จากธนาคาร บริษัท หรือหน่วยงานต่าง ๆ เพื่อหลอกให้เหยื่อเปิดเผยข้อมูล

13. Social Engineering (การหลอกลวงทางสังคม)

คำอธิบาย: การหลอกลวงทางสังคมเป็นการโจมตีที่ใช้เทคนิคทางจิตวิทยาเพื่อหลอกล่อให้ผู้ใช้เปิดเผยข้อมูลส่วนตัว, ทำการบางอย่างที่เป็นประโยชน์ต่อผู้โจมตี หรือเข้าถึงระบบหรือข้อมูลที่ต้องการ ผู้โจมตีอาจแกล้งทำเป็นคนรู้จัก, เจ้าหน้าที่หรือผู้ให้บริการเพื่อสร้างความน่าเชื่อถือ

เทคนิคที่ใช้:

- การแอบอ้างเป็นบุคคลอื่น: การแกล้งเป็นเพื่อนร่วมงาน, เจ้าหน้าที่ IT หรือบุคคลที่มีอำนาจ เพื่อขอข้อมูลหรือเข้าถึงระบบ
- การสร้างสถานการณ์ฉุกเฉิน: การสร้างสถานการณ์เร่งด่วนหรือฉุกเฉินเพื่อให้เหยื่อตัดสินใจโดยไม่ได้คิดให้รอบคอบ
- การใช้ความอยากรู้อยากเห็น: การส่งข้อความที่น่าสนใจหรือมีเนื้อหาที่กระตุ้นความอยากรู้ เพื่อหลอกให้คลิกลิงก์หรือดาวน์โหลดไฟล์
- การใช้ความไว้ใจ: การสร้างความสัมพันธ์หรือความไว้วางใจกับเหยื่อเพื่อหลอกให้เปิดเผยข้อมูล

14. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS)

คำอธิบาย: การโจมตีแบบ DoS และ DDoS มีเป้าหมายเพื่อทำให้ระบบ, เว็บไซต์ หรือเครือข่ายไม่สามารถใช้งานได้ โดยการส่งคำขอจำนวนมากเกินกว่าที่ระบบจะรับไหว ทำให้ระบบทำงานช้าลง, หยุดทำงาน หรือเข้าถึงไม่ได้

ความแตกต่างระหว่าง DoS และ DDoS:

- DoS (Denial-of-Service): การโจมตีจากคอมพิวเตอร์เครื่องเดียวไปยังเป้าหมาย
- DDoS (Distributed Denial-of-Service): การโจมตีจากคอมพิวเตอร์หลายเครื่อง (ส่วนใหญ่มักเป็นคอมพิวเตอร์ที่ถูกควบคุมโดยผู้โจมตี) ไปยังเป้าหมาย ซึ่งมีพลังในการโจมตีมากกว่า

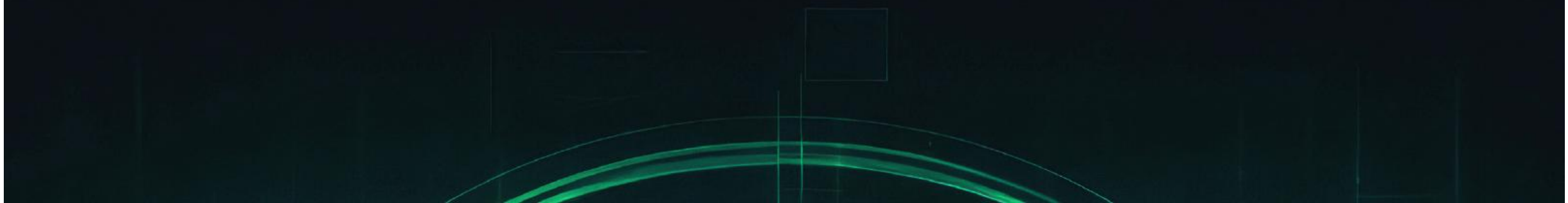
วิธีการโจมตี: ผู้โจมตีจะส่งคำขอ (request) จำนวนมากไปยังเป้าหมาย ทำให้ทรัพยากรของเป้าหมาย (เช่น แบนด์วิดท์, หน่วยประมวลผล, หน่วยความจำ) หมดลง จนไม่สามารถให้บริการได้

ITUPublications

International Telecommunication Union
Development Sector

Global Cybersecurity Index 2024

5th Edition

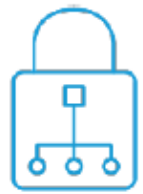


Report summary

The fifth edition of the Global Cybersecurity Index (GCI) measures the commitment of countries to cybersecurity in the context of measures across the following five pillars:

Legal

Technical



Organizational

Capacity development

Cooperation

The GCI, launched in 2015 by the International Telecommunication Union, seeks to help countries to identify areas of improvement and encourage countries to act in building capacity and capabilities under each pillar. The GCI has been continuously adapted across editions to respond to changing risks, priorities and resources, in order to provide a more relevant snapshot of cybersecurity measures taken by countries.

Countries measured	Collection years	Focal points from countries	Average overall score growth since 2020
194	2023-2024	172	27%

83 questions → **20 indicators** → **5 pillars** → **Overall Score**

Figure 1: Tier performance, by region

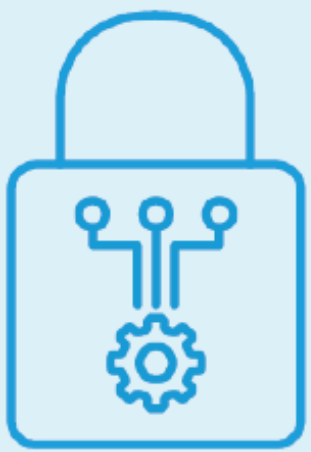
Source: ITU

Key statistics by pillar

Legal

Measuring the laws and regulations on cyber-crime and cybersecurity

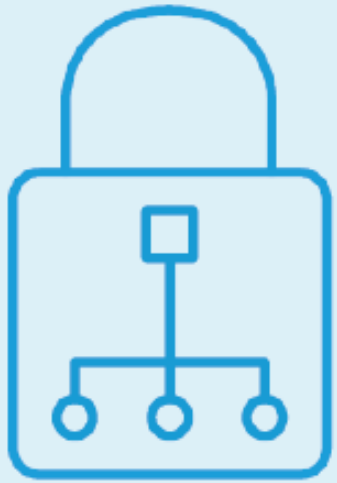
177	Countries had at least one regulation on either personal data protection, privacy protection, or breach notification in force or in progress.
151	Countries with data protection regulations in force
104	Countries with critical infrastructure regulations



Technical

Measuring the implementation of technical capabilities through national and sector-specific agencies

139	Countries with active CIRTs
83	Countries engaged with a regional CIRT association
110	Countries with frameworks to adopt cybersecurity standards



Organizational

Measuring national strategies and organizations implementing cybersecurity

132	Countries with national cybersecurity strategies
161	Countries with cybersecurity agencies
94	Countries with child online protection strategies and initiatives reported

Capacity development

Measuring awareness campaigns, training, education and incentives for cybersecurity capacity development

152	Countries conducting cyber-awareness initiatives
153	Countries with cybersecurity at some level of national curricula
99	Countries with cybersecurity capacity-development incentives

Cooperation

Measuring partnerships between agencies, firms and countries

108	Countries engaged or will be engaged in domestic or international cybersecurity public-private partnerships
166	Countries with international cybersecurity agreements
122	Countries reporting inter-agency collaboration

Cybersecurity issues have become more prominent, owing *inter alia* to:

1) **Increased ransomware**: growing reports of ransomware attacks targeting government services and other critical sectors in many countries.[3]
2) **Breaches affecting core industries**: the scale, frequency and intensity of cybersecurity incidents or breaches affecting individuals and various sectors including education, manufacturing, energy and IT services, to name but a few.
3) **Privacy concerns**: data breaches resulted in European data protection authorities issuing General Data Protection Regulation (GDPR) fines worth over EUR 1.9 billion in 2023,[4] with total GDPR fines issued since 2018 estimated to be currently worth more than EUR 4.5 billion.[5]
4) **Cost to businesses**: the global average cost of a data breach was estimated at USD 4.45 million in 2023.
5) **Outages**: information technology disruptions affecting the integrity and availability of systems, services and supply chains.[6]

THREATS AND RISKS

Explain the concepts threat, risk and risk analysis

- **Threat**: a potential cause of an unwanted Incident, which may result in harm to a System or Organization
- **Risk analysis**: a process to comprehend the nature of risk and to determine the level of risk. It provides the basis for risk evaluation and decisions about risk treatment

Explain the concepts threat, risk and risk analysis

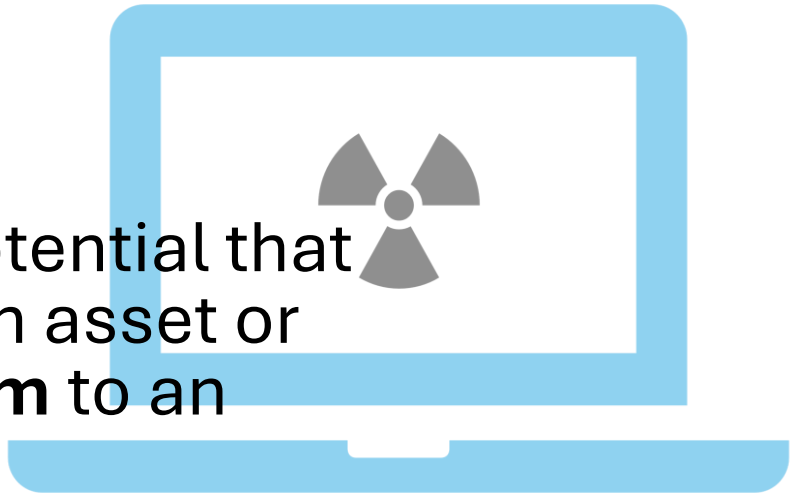
Threats and information security measures

- In the process of information security, undesired effects (threats) are mapped as well as possible
- In information security, it is determined whether something must be done to avoid these effects
- Information security determines which security measures must be taken to avoid these effects

Explain the concepts threat, risk and risk analysis

- **Risk**: A combination of the probability of an event and its consequence
- ISO/IEC 27000:2018 definition:

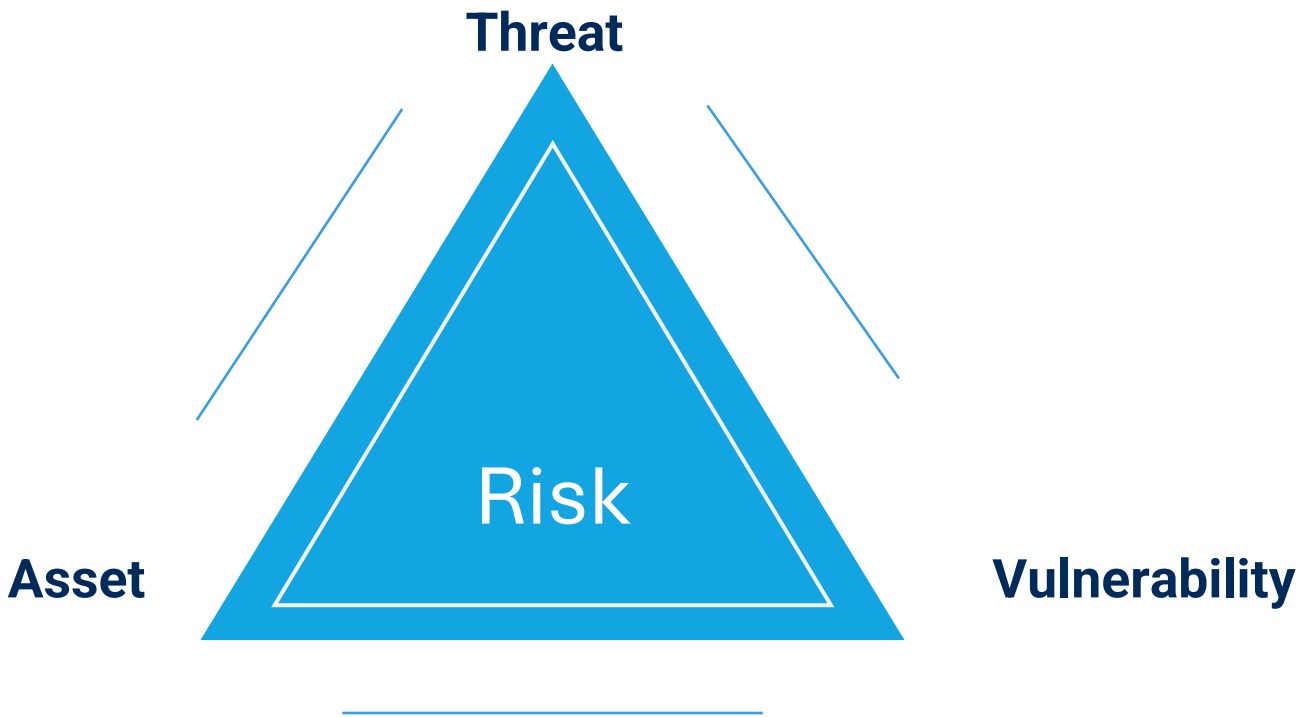
Risk is the **effect of uncertainty on objectives** and is often characterized by reference to potential **events** and **consequences**, or a combination of these.



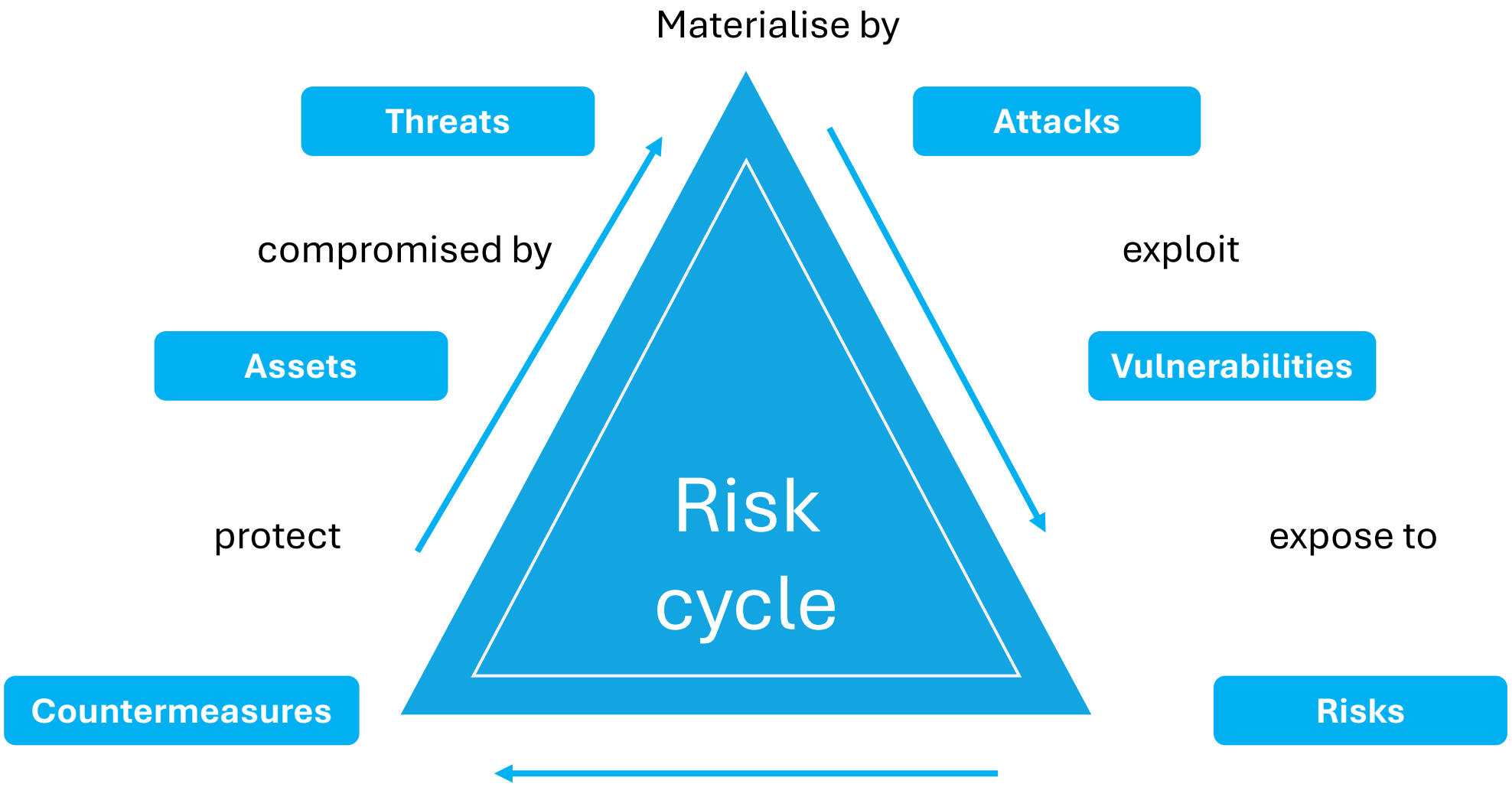
Information security risk is associated with the potential that **threats** will exploit **vulnerabilities** of an information asset or group of information assets and thereby **cause harm** to an organization

Explain the relationship between a threat and a risk

- A **risk** is the likelihood of a **threat** agent taking advantage of a **vulnerability** in an **asset** and the corresponding business **impact**



Explain the relationship between a threat and a risk



Explain various types of threats

A threat could be:

- an intruder accessing the network through a port on the firewall
- a process accessing data in a way that violates the security policy, a tornado wiping out a facility
- an employee making a mistake that could expose confidential information or destroy a file's integrity

- Two kinds of threats
  - **Human threats**
    - Intentional (Hacking, damaging property, Destroying e-mails after being fired)
    - Unintentional (Deleting data and carelessly confirming this with OK)
    - Social Engineering (Tricking people into voluntarily providing sensitive information: phishing)
  - **Non-human Threats**
    - Lightning strikes, fire, floods, hurricanes, tornadoes, etc.

Describe various types of damage

Damage types:

- Direct Damage
  - Theft
  - Water
- Indirect Damage
  - Inability to provide a service because the IT infrastructure is down
  - Financial damage due to loss of customer contract

Describe various risk strategies

- Risk bearing (acceptance)
  - Risk are accepted, no action is taken (e.g. due to a low expected impact or likelihood)
    - Security measures are too costly
    - Security measures exceed the possible damage
    - Security measures that are taken are repressive by nature
- Risk neutral (treat)
  - Measures are taken to prevent risks happening or minimize damage (e.g. physical security, fire protection systems)
    - The threat no longer occurs
    - The resulting damage is minimized
    - Security measures taken are a combination of preventative, detective and Repressive measures
- Risk avoiding
  - Measures are taken to make sure the risk does not happen
  - Security measures that are taken are preventative by nature
    - E.g. software patching

Module 4: องค์ประกอบสำคัญสำหรับการจัดการ Cybersecurity ด้าน Device/Communication/Systems/Information

องค์ประกอบสำคัญของ Cybersecurity

- Device Security (คอมพิวเตอร์, สมาร์ทโฟน, อุปกรณ์ IoT)
- Communication Security (เครือข่าย, อีเมล, แอปพลิเคชัน)
- System Security (ระบบปฏิบัติการ, ฐานข้อมูล, เซิร์ฟเวอร์)
- Information Security (ข้อมูล, เอกสาร, ทรัพย์สินทางปัญญา)
- Application Security (ความปลอดภัยของแอปพลิเคชัน)

1. Device Security (ความปลอดภัยของอุปกรณ์)

คำอธิบาย: การรักษาความปลอดภัยของอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับเครือข่าย ทั้งคอมพิวเตอร์ส่วนบุคคล, สมาร์ทโฟน, แท็บเล็ต, และอุปกรณ์ IoT (Internet of Things) เป็นสิ่งสำคัญ เนื่องจากอุปกรณ์เหล่านี้เป็นจุดเริ่มต้นของการเข้าถึงข้อมูลและระบบ

องค์ประกอบย่อย:

- การป้องกันมัลแวร์: ติดตั้งโปรแกรมป้องกันไวรัส, สแกนอุปกรณ์อย่างสม่ำเสมอ, และหลีกเลี่ยงการดาวน์โหลดซอฟต์แวร์จากแหล่งที่ไม่น่าเชื่อถือ
- การอัปเดตซอฟต์แวร์: อัปเดตระบบปฏิบัติการและแอปพลิเคชันให้เป็นเวอร์ชันล่าสุด เพื่อปิดช่องโหว่ด้านความปลอดภัย
- การตั้งรหัสผ่านที่แข็งแกร่ง: ใช้รหัสผ่านที่ซับซ้อนและไม่ซ้ำกันสำหรับแต่ละบัญชี และเปลี่ยนรหัสผ่านเป็นประจำ
- การเข้ารหัสข้อมูล: เข้ารหัสข้อมูลที่จัดเก็บในอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- การตั้งค่าความปลอดภัยของอุปกรณ์: เปิดใช้งานคุณสมบัติความปลอดภัยของอุปกรณ์ เช่น การล็อกหน้าจอ, การยืนยันตัวตนด้วยไบโอเมตริกซ์, และการลบข้อมูลระยะไกล

2. Communication Security (ความปลอดภัยในการสื่อสาร)

คำอธิบาย: การรักษาความปลอดภัยของการสื่อสารข้อมูลผ่านเครือข่าย, อีเมล, และแอปพลิเคชันต่าง ๆ เพื่อป้องกันการดักฟัง, การปลอมแปลง, หรือการเปลี่ยนแปลงข้อมูลระหว่างการส่ง

องค์ประกอบย่อย:

- การเข้ารหัสข้อมูล: เข้ารหัสข้อมูลที่ส่งผ่านเครือข่าย เพื่อป้องกันการดักฟังข้อมูลระหว่างทาง (เช่น การใช้ HTTPS บนเว็บไซต์)
- การตรวจสอบความถูกต้อง: ตรวจสอบความถูกต้องของผู้ส่งและผู้รับข้อมูล เพื่อป้องกันการปลอมแปลง
- ความปลอดภัยของอีเมล: ใช้โปรแกรมป้องกันสแปมและฟิชชิง, ระมัดระวังในการเปิดอีเมลและไฟล์แนบจากแหล่งที่ไม่รู้จัก, และใช้การเข้ารหัสอีเมล (เช่น PGP)
- ความปลอดภัยของเครือข่าย: ใช้ไฟร์วอลล์เพื่อป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต, ใช้ VPN (Virtual Private Network) ในการเชื่อมต่อเครือข่ายที่ไม่น่าเชื่อถือ, และใช้โปรโตคอลเครือข่ายที่ปลอดภัย
- ความปลอดภัยของแอปพลิเคชัน: ตรวจสอบและอัปเดตแอปพลิเคชันอย่างสม่ำเสมอ, ใช้แอปพลิเคชันจากแหล่งที่น่าเชื่อถือ, และจำกัดสิทธิ์การเข้าถึงข้อมูลของแอปพลิเคชัน

3. System Security (ความปลอดภัยของระบบ)

คำอธิบาย: การรักษาความปลอดภัยของระบบปฏิบัติการ, ฐานข้อมูล, และเซิร์ฟเวอร์ ซึ่งเป็นโครงสร้างพื้นฐานที่สำคัญในการทำงานของระบบไอที

องค์ประกอบย่อย:

- การบริหารจัดการแพทช์: อัปเดตระบบปฏิบัติการและซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุด เพื่อแก้ไขช่องโหว่ด้านความปลอดภัย
- การกำหนดค่าความปลอดภัย: กำหนดค่าระบบปฏิบัติการและซอฟต์แวร์ให้มีความปลอดภัยสูงสุด
- การควบคุมการเข้าถึง: จำกัดสิทธิ์การเข้าถึงระบบและข้อมูล ให้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
- การตรวจสอบและบันทึก: ตรวจสอบและบันทึกกิจกรรมต่าง ๆ ในระบบ เพื่อตรวจสอบการทำงานผิดปกติและติดตามการโจมตี
- การสำรองข้อมูล: สำรองข้อมูลอย่างสม่ำเสมอ เพื่อให้สามารถกู้คืนข้อมูลได้ในกรณีที่เกิดความเสียหาย
- ความปลอดภัยของเซิร์ฟเวอร์: ใช้ระบบป้องกันการโจมตี DDoS, ติดตั้งไฟร์วอลล์, และจำกัดการเข้าถึงเซิร์ฟเวอร์

4. Information Security (ความปลอดภัยของข้อมูล)

คำอธิบาย: การรักษาความปลอดภัยของข้อมูลที่จัดเก็บ, ส่งผ่าน, หรือประมวลผล เพื่อป้องกันการเข้าถึง, ใช้งาน, เปิดเผย, ทำลาย หรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต

องค์ประกอบย่อย:

- การจำแนกประเภทข้อมูล: จำแนกประเภทข้อมูลตามความสำคัญและความอ่อนไหว เพื่อกำหนดระดับการป้องกันที่เหมาะสม
- การควบคุมการเข้าถึง: กำหนดสิทธิ์การเข้าถึงข้อมูลให้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
- การเข้ารหัสข้อมูล: เข้ารหัสข้อมูลที่จัดเก็บและส่งผ่านเครือข่าย เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- การป้องกันการรั่วไหลของข้อมูล: ใช้ระบบ DLP (Data Loss Prevention) เพื่อป้องกันการรั่วไหลของข้อมูล
- การจัดการสิทธิ์การเข้าถึง: กำหนดและตรวจสอบสิทธิ์การเข้าถึงข้อมูลอย่างสม่ำเสมอ
- การจัดการเอกสารและความลับทางการค้า: กำหนดนโยบายและมาตรการในการจัดการเอกสารและความลับทางการค้าอย่างเหมาะสม

5. Application Security (ความปลอดภัยของแอปพลิเคชัน)

คำอธิบาย: Application Security คือ การรักษาความปลอดภัยของซอฟต์แวร์และแอปพลิเคชันต่าง ๆ ตั้งแต่ขั้นตอนการออกแบบ, พัฒนา, ทดสอบ, ไปจนถึงการใช้งานจริง เพื่อป้องกันช่องโหว่ที่อาจถูกโจมตีจากผู้ไม่ประสงค์ดี และรักษาความปลอดภัยของข้อมูลและฟังก์ชันการทำงานของแอปพลิเคชัน

องค์ประกอบย่อย:

- Secure Coding Practices (หลักการเขียนโค้ดที่ปลอดภัย): นักพัฒนาต้องเขียนโค้ดโดยคำนึงถึงความปลอดภัย เช่น การตรวจสอบอินพุตของผู้ใช้, การป้องกัน SQL Injection, และการจัดการกับข้อผิดพลาดอย่างเหมาะสม
- Input Validation (การตรวจสอบอินพุต): การตรวจสอบข้อมูลที่ผู้ใช้ป้อนเข้ามา เพื่อป้องกันการโจมตี เช่น Cross-Site Scripting (XSS) และ SQL Injection
- Authentication and Authorization (การพิสูจน์ตัวตนและการอนุญาต): การตรวจสอบว่าผู้ใช้เป็นใครและมีสิทธิ์เข้าถึงอะไรในแอปพลิเคชัน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- Session Management (การจัดการเซสชัน): การจัดการเซสชันของผู้ใช้อย่างปลอดภัย เพื่อป้องกันการขโมยเซสชันหรือการปลอมแปลงตัวตน
- Error Handling (การจัดการข้อผิดพลาด): การจัดการข้อผิดพลาดที่เกิดขึ้นในแอปพลิเคชันอย่างเหมาะสม เพื่อป้องกันการเปิดเผยข้อมูลที่สำคัญ หรือทำให้แอปพลิเคชันไม่เสถียร
- Security Testing (การทดสอบความปลอดภัย): การทดสอบแอปพลิเคชันเพื่อหาช่องโหว่ด้านความปลอดภัย เช่น Penetration Testing และ Vulnerability Scanning
- Third-Party Components (ส่วนประกอบจากบุคคลที่สาม): การตรวจสอบความปลอดภัยของไลบรารีและส่วนประกอบจากบุคคลที่สามที่ใช้ในแอปพลิเคชัน
- Web Application Firewalls (WAF): การใช้ไฟร์วอลล์สำหรับเว็บแอปพลิเคชันเพื่อป้องกันการโจมตีที่มุ่งเป้าไปยังแอปพลิเคชันโดยเฉพาะ
- Continuous Integration/Continuous Deployment (CI/CD): การรวมความปลอดภัยเข้ากับกระบวนการพัฒนาและติดตั้งแอปพลิเคชันอย่างต่อเนื่อง

6. Cloud Security (ความปลอดภัยของระบบคลาวด์)

คำอธิบาย: Cloud Security คือ การรักษาความปลอดภัยของข้อมูล, แอปพลิเคชัน, และโครงสร้างพื้นฐานที่จัดเก็บและให้บริการบนระบบคลาวด์ เพื่อป้องกันการเข้าถึง, ใช้งาน, เปิดเผย, ทำลาย หรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต

องค์ประกอบย่อย:

- Data Security (ความปลอดภัยของข้อมูล):
  - Data Encryption (การเข้ารหัสข้อมูล): เข้ารหัสข้อมูลที่จัดเก็บและส่งผ่านระบบคลาวด์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
  - Data Loss Prevention (DLP): ใช้ระบบ DLP เพื่อป้องกันการรั่วไหลของข้อมูลออกจากระบบคลาวด์
  - Data Backup and Recovery (การสำรองและกู้คืนข้อมูล): สำรองข้อมูลอย่างสม่ำเสมอและมีแผนการกู้คืนข้อมูลในกรณีที่เกิดความเสียหาย
- Access Control (การควบคุมการเข้าถึง):
  - Identity and Access Management (IAM): จัดการข้อมูลระบุตัวตนของผู้ใช้และสิทธิ์การเข้าถึงทรัพยากรในระบบคลาวด์
  - Multi-Factor Authentication (MFA): ใช้การยืนยันตัวตนหลายขั้นตอนเพื่อเพิ่มความปลอดภัยในการเข้าสู่ระบบ
  - Principle of Least Privilege: ให้สิทธิ์การเข้าถึงเฉพาะที่จำเป็นเท่านั้น
- Network Security (ความปลอดภัยของเครือข่าย):
  - Virtual Private Networks (VPNs): ใช้ VPN เพื่อสร้างการเชื่อมต่อที่ปลอดภัยในการเข้าถึงระบบคลาวด์
  - Firewalls: ใช้ไฟร์วอลล์เพื่อป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต
  - Intrusion Detection and Prevention Systems (IDPS): ใช้ระบบ IDPS เพื่อตรวจจับและป้องกันการโจมตีในเครือข่าย
- Compliance (การปฏิบัติตามกฎระเบียบ):
  - Cloud Security Compliance: ปฏิบัติตามกฎหมายและข้อบังคับที่เกี่ยวข้องกับความปลอดภัยของระบบคลาวด์ เช่น GDPR หรือ HIPAA
- Visibility and Monitoring (การมองเห็นและการตรวจสอบ):
  - Cloud Logging and Monitoring: ติดตามและบันทึกกิจกรรมต่าง ๆ ในระบบคลาวด์ เพื่อตรวจสอบการทำงานผิดปกติและติดตามการโจมตี
  - Security Information and Event Management (SIEM): ใช้ระบบ SIEM เพื่อรวบรวมและวิเคราะห์ข้อมูลความปลอดภัยจากระบบคลาวด์
- Shared Responsibility Model: ทำความเข้าใจและแบ่งความรับผิดชอบด้านความปลอดภัยระหว่างผู้ให้บริการคลาวด์และผู้ใช้งาน
- Third-Party Security: ตรวจสอบความปลอดภัยของผู้ให้บริการคลาวด์และบริการเสริมต่าง ๆ ที่ใช้งาน

Module 5: การวัด ตรวจจับความเสี่ยง แผนรับมือ การคืนสภาพหลังเผชิญเหตุ รวมถึงการประเมินความเสี่ยงเพื่อการทำประกันภัยไซเบอร์ในประเทศไทย

“หกคำถาม” ที่ผู้บริหารทุกคนควรถามเกี่ยวกับประกันไซเบอร์

1. **Do we have a cyber insurance policy?**
    - และมีแล้วครอบคลุมค่าเสียหายหรือไม่ แค่ไหน
    - In 2020, the top 10 biggest ransomware attacks cost victims nearly $213 million to investigate, rebuild networks and restore backups, pay the ransom and put preventative measures in place to avoid future incidents.
2. **Who owns the task of mitigating cyber risk with insurance?**
    - ใครรับผิดชอบซื้อประกัน และ ใครรับผิดชอบติดต่อเคลมประกัน
3. **Do we have the right amount of cyber insurance?**
    - สถาบันการเงินเป็นกลุ่มที่ค่อนข้างทำได้ชัดเจน
    - อุตสาหกรรมอื่น ยังไม่ชัดเจน และมักประเมินความเสียหาย (และวงเงินประกัน) ต่ำไป

“หกคำถาม” ที่ผู้บริหารทุกคนควรถามเกี่ยวกับประกันไซเบอร์

4. **What does our policy cover?** ประกันของเราครอบคลุมอะไรบ้างกันแน่ และอะไรที่ไม่ครอบคลุม
   - ประกันส่วนใหญ่จ่ายชดเชยค่า network security ค่าจ้างที่ปรึกษา และจ่ายค่าสืบสวนสาเหตุ
   - บางกรมธรรม์ จ่าย restoring data และการนำระบบกลับคืนบริการให้ด้วย
   - ค่าใช้จ่ายในการสืบลงไปถึงสาเหตุหลักพื้นฐาน ครอบคลุมไหม หรือ แค่สาเหตุเบื้องต้น
   - ค่าใช้จ่ายในการแรก
   - ค่าใช้จ่ายด้านประชาสัมพันธ์ เพื่อแก้ไขภาพลักษณ์แจ้งเตือนผู้เสียหาย ครอบคลุมหรือไม่ เช่น 1 แสนราย
   - ครอบคลุมการติดตามการนำข้อมูลส่วนบุคคลไปใช้ในทางที่ผิด และ การทำบัตรใหม่หรือไม่ กรณีข้อมูลส่วนบุคคลถูกขโมย

“หกคำถาม” ที่ผู้บริหารทุกคนควรถามเกี่ยวกับประกันไซเบอร์

5. What does our policy cover?

- ถ้าถูกโจมตีโดย ransomware ประกันรับผิดชอบค่าเจรจา และจ่ายค่าไถ่ด้วยหรือไม่
- ครอบคลุมความเสียหายต่อเนื่องในแง่กระบวนการธุรกิจหรือไม่ เช่น ความเสียหายจากการยกเลิกเที่ยวบิน หรือ การส่งสินค้า หรือการผลิตไม่ทันกำหนด
- ถ้าการโจมที่เกิดกับเราเป็นส่วนหนึ่งของโจมตีระดับรัฐ หรือ ประเทศ ประกันจะรับผิดชอบด้วย หรือ จะยกเลิกการคุ้มครอง เพราะถือว่าอยู่ในภาวะสงคราม
- ถ้าบริษัทมีค่าปรับจากการละเมิดกฎหมาย (เช่น PDPA) ประกันจะจ่ายด้วยหรือไม่อย่างไร
- ถ้าการถูกโจมตีนั้น เกิดจากองค์กรหละหลวมเอง ประกัน**<u>มักจะไม่จ่าย</u>**ค่าปรับปรุงความปลอดภัยต่าง ๆ ให้ได้มาตรฐาน

“หกคำถาม” ที่ผู้บริหารทุกคนควรถามเกี่ยวกับประกันไซเบอร์

6. Does our insurance provider understand our industry and its risks?

- บริษัทประกันส่วนใหญ่ เข้าใจภัยพิบัติทางกายภาพเป็นอย่างดี เช่น ภัยธรรมชาติ การจราจร การผิดชำระหนี้ แต่มักไม่เข้าใจภัย และความเสียหายจากอีเมลปลอม (phishing mail), social engineering และ มัลแวร์ต่าง ๆ
- บรัษทประกันเข้าใจข้อกำหนดความเป็นส่วนบุคคลและการรักษาความปลอดภัยที่ระบุในกฎหมายหรือไม่ เช่น HIPAA และ PDPA
- รวมถึงปัจจัยทางด้านความปลอดภัยที่ต้องตระหนักเมื่อผู้กำกับดูแลอุตสาหกรรมสุขภาพกำหนดให้ต้องมีการแบ่งปันข้อมูลคนไข้
- บริษัทประกันเข้าใจความสำคัญและข้อกำหนดต่าง ๆ ที่ออกโดย regulator ต่าง ๆ หรือไม่ เช่น กฎระเบียบและข้อกำหนดทางการเงินที่ออกโดยธนาคารแห่งประเทศไทย

หกคำถามที่ผู้บริหารทุกคนควรถามเกี่ยวกับประกันไซเบอร์

7. Is our policy flexible enough to adapt as our business grows?

- การปรับเปลี่ยนซอฟต์แวร์ และเทคโนโลยีใหม่ ส่งผลให้ต้องแก้กรมธรรม์หรือไม่ กรมธรรม์ยืดหยุ่นแค่ไหน
- องค์กรควรกำหนดผู้รับผิดชอบมาทำหน้าที่ทบทวนกรมธรรม์เป็นระยะ ๆ ด้วย เพราะด้วยสถานการณ์ต่าง ๆ ที่เปลี่ยนแปลงไป อาจจะต้องแก้ไขกรมธรรม์ หรือ เปลี่ยนเงื่อนไขต่าง ๆ

https://www.pwc.com/us/en/tech-effect/cybersecurity/buying-cybersecurity-insurance.html

Module 6: การพัฒนาแผนปฏิบัติงาน Personalized Cybersecurity Playbook

องค์ประกอบสำคัญของ Personalized Cybersecurity Playbook:

1. **การประเมินความเสี่ยง (Risk Assessment):** วิเคราะห์ภัยคุกคาม สินทรัพย์ที่สำคัญ และผลกระทบที่อาจเกิดขึ้นกับองค์กร
2. **วัตถุประสงค์และเป้าหมาย (Objectives & Goals):** กำหนดเป้าหมายด้านความปลอดภัยไซเบอร์ที่ชัดเจน สอดคล้องกับวิสัยทัศน์ และ กลยุทธ์ขององค์กร
3. **กลยุทธ์และมาตรการ (Strategies & Controls):** กำหนดแนวทาง และ มาตรการในการป้องกัน ตรวจจับ ตอบสนอง และกู้คืนจากภัยคุกคาม
4. **บทบาทและความรับผิดชอบ (Roles & Responsibilities):** กำหนดหน้าที่ และ ความรับผิดชอบของบุคลากร และหน่วยงานต่างๆ
5. **แผนการสื่อสาร (Communication Plan):** กำหนดช่องทาง และ วิธีการสื่อสารข้อมูลด้าน Cybersecurity ทั้งภายในและ ภายนอกองค์กร
6. **แผนการฝึกอบรม (Training Plan):** เพื่อฝึกอบรม พัฒนาความรู้ และความตระหนักด้าน Cybersecurity ให้กับพนักงาน
7. **แผนการทดสอบและปรับปรุง (Testing & Improvement Plan):** เพื่อปรับปรุง Cybersecurity Playbook อย่างต่อเนื่อง

ตัวอย่างโจทย์ Workshop จัดทำ Personal Cybersecurity Playbook

- # การตอบสนองเหตุการณ์ทางไซเบอร์ เช่น
  - การขโมยข้อมูล, การโจมตีโดย Ransomware หรือ Virus
  - ปริมาณการใช้ IT System สูงมากกว่าปกติ (Network/Application/Database)
  - ระบบล่มแบบ Crowd Strike
- # การย้ายระบบจาก Local Sever เข้าสู่คลาวด์
- # การนำ AI มาใช้ในองค์กร สำหรับงานด้าน.....
- # งานหลักขององค์กร (เช่น การพัฒนาซอฟต์แวร์ งานบริการรับเรื่องร้องเรียน งานพิจารณาสินเชื่อ)

องค์ประกอบสำคัญของ Personalized Cybersecurity Playbook

การประเมินความเสี่ยง
(Risk Assessment)

วัตถุประสงค์และเป้าหมาย
(Objectives & Goals)

กลยุทธ์และมาตรการ
(Strategies & Controls)

แผนการสื่อสาร
(Communication Plan)

บทบาทและความรับผิดชอบ
(Roles & Responsibilities)

แผนการฝึกอบรม
(Training Plan)

แผนการทดสอบและปรับปรุง
(Testing & Improvement Plan)

องค์ประกอบสำคัญของ Personalized Cybersecurity Playbook

การประเมินความเสี่ยง

(Risk Assessment)

กระบวนการประเมินความเสี่ยงโดยทั่วไปประกอบด้วย 3 ส่วนหลัก ดังนี้

1. การระบุภัยคุกคาม (Threat Identification): ขั้นตอนนี้คือการระบุภัยคุกคามที่อาจเกิดขึ้นกับองค์กร ซึ่งอาจมาจากทั้งภายในและภายนอก โดยสามารถจำแนกได้ดังนี้:

A. **ภัยคุกคามจากภายนอก:**

- **Malware (มัลแวร์):** ไวรัส, หนอน, โทรจัน, แรนซัมแวร์ ฯลฯ
- **Hacking (การแฮก):** การบุกรุกระบบเพื่อขโมยข้อมูลหรือก่อความเสียหาย
- **Phishing (ฟิชชิง):** การหลอกลวงเพื่อให้ได้ข้อมูลส่วนตัวหรือข้อมูลสำคัญ
- **DDoS Attack (การโจมตีแบบ DDoS):** การทำให้ระบบไม่สามารถใช้งานได้
- **Social Engineering (วิศวกรรมสังคม):** การหลอกลวงโดยใช้จิตวิทยา
- **ภัยธรรมชาติ:** แผ่นดินไหว, น้ำท่วม, ไฟไหม้ ฯลฯ

B. **ภัยคุกคามจากภายใน:**

- **ความผิดพลาดของบุคลากร:** การตั้งค่าระบบผิดพลาด, การละเมิดนโยบาย
- **การกระทำโดยเจตนา:** การขโมยข้อมูล, การทำลายข้อมูล
- **ผู้ไม่หวังดีภายใน:** อดีตพนักงาน, พนักงานที่ต้องการแก้แค้น
- **อุปกรณ์หรือซอฟต์แวร์ที่ไม่ได้รับอนุญาต:** การนำอุปกรณ์ส่วนตัวมาใช้ (BYOD)

C. **ภัยคุกคามที่เกิดขึ้นใหม่:**

- **ช่องโหว่ของระบบ:** ช่องโหว่ที่เกิดขึ้นจากซอฟต์แวร์ หรือฮาร์ดแวร์
- **เทคโนโลยีใหม่:** การใช้เทคโนโลยีใหม่ที่ยังไม่มีการป้องกันที่เหมาะสม

2. การระบุสินทรัพย์ที่สำคัญ (Asset Identification): ขั้นตอนนี้คือการระบุสินทรัพย์ที่มีคุณค่าต่อองค์กรและต้องการการปกป้อง ซึ่งอาจแบ่งได้ดังนี้:

- **ข้อมูล:** ข้อมูลลูกค้า, ข้อมูลทางการเงิน, ข้อมูลทรัพย์สินทางปัญญา, ข้อมูลส่วนบุคคล ฯลฯ
- **ระบบ:** ระบบฐานข้อมูล, ระบบเครือข่าย, เซิร์ฟเวอร์, แอปพลิเคชัน ฯลฯ
- **อุปกรณ์:** คอมพิวเตอร์, โทรศัพท์มือถือ, อุปกรณ์ IoT, อุปกรณ์จัดเก็บข้อมูล ฯลฯ
- **บุคลากร:** บุคลากรที่มีความเชี่ยวชาญเฉพาะทาง, บุคลากรที่มีสิทธิเข้าถึงข้อมูลสำคัญ
- **ทรัพย์สินทางกายภาพ:** อาคาร, อุปกรณ์สำนักงาน, อุปกรณ์การผลิต ฯลฯ
- **ชื่อเสียงขององค์กร:** ความน่าเชื่อถือ, ภาพลักษณ์ขององค์กร

ในขั้นตอนนี้ ควรมีการจัดลำดับความสำคัญของสินทรัพย์ (Asset Prioritization) เพื่อให้ทราบว่าสินทรัพย์ใดสำคัญที่สุด และควรได้รับการปกป้องเป็นอันดับแรก

องค์กรที่ยังไม่มีการสำรวจควรเริ่มต้นสำรวจ ส่วนที่สำรวจแล้ว ควรทบทวนการจัดลำดับความสำคัญ เช่น กรณีสถาบันการเงิน ก่อนและหลังเกิด mobile banking ย่อมส่งผลต่อลำดับความสำคัญของ Assets

3. การวิเคราะห์ผลกระทบ (Impact Analysis): ขั้นตอนนี้คือการประเมินผลกระทบที่อาจเกิดขึ้นกับองค์กรหากเกิดเหตุการณ์ด้านความปลอดภัย โดยพิจารณาจาก:

- **ความเสียหายทางการเงิน:** ค่าใช้จ่ายในการกู้คืนระบบ, ค่าปรับ, การสูญเสียรายได้
- **ความเสียหายต่อชื่อเสียง:** การสูญเสียความน่าเชื่อถือ, การสูญเสียลูกค้า
- **ความเสียหายต่อการดำเนินงาน:** การหยุดชะงักของธุรกิจ, การสูญเสียประสิทธิภาพ
- **ความเสียหายด้านกฎหมายและข้อบังคับ:** การละเมิดกฎหมาย, การถูกฟ้องร้อง
- **ความเสียหายต่อข้อมูล:** การสูญเสียข้อมูล, การรั่วไหลของข้อมูล

ในการวิเคราะห์ผลกระทบ อาจใช้เทคนิคการวิเคราะห์เชิงคุณภาพ (Qualitative Analysis) หรือเชิงปริมาณ (Quantitative Analysis) หรือทั้งสองอย่างควบคู่กัน

องค์กรที่ยังไม่มีการวิเคราะห์ควรเริ่มวิเคราะห์ ส่วนที่ทำไปแล้ว ควรทบทวนว่าบริบทที่เปลี่ยนไปส่งผลต่อสมมติฐานเดิมหรือไม่อย่างไร และ ส่งผลต่อเนื่องต่อผลการวิเคราะห์ (ที่ทำไว้เดิม) หรือไม่อย่างไร

องค์ประกอบสำคัญของ Personalized Cybersecurity Playbook

วัตถุประสงค์และเป้าหมาย

(Objectives & Goals)

ความแตกต่างระหว่างวัตถุประสงค์และเป้าหมาย

วัตถุประสงค์ (Objectives): คือ**สิ่งที่องค์กรต้องการบรรลุในภาพรวม** ซึ่งมักจะเป็นสิ่งที่กว้างและครอบคลุมมากกว่า โดยอาจเป็นสิ่งที่ต้องการบรรลุในระยะยาว เช่น การสร้างความเชื่อมั่นด้านความปลอดภัยให้กับลูกค้า หรือการลดความเสี่ยงด้านความปลอดภัยทางไซเบอร์โดยรวม

เป้าหมาย (Goals): คือสิ่งที่**เฉพาะเจาะจงและสามารถวัดผลได้** ซึ่งเป็นขั้นตอนย่อยๆ ที่จะนำไปสู่วัตถุประสงค์ที่ตั้งไว้ โดยมีกรอบเวลาที่ชัดเจน เช่น การลดจำนวนเหตุการณ์ด้านความปลอดภัยลง 20% ภายในหนึ่งปี หรือการอบรมพนักงานทั้งหมดให้มีความรู้ด้านความปลอดภัยทางไซเบอร์ภายใน 6 เดือน

การกำหนดวัตถุประสงค์และเป้าหมายที่ดี

1. สอดคล้องกับวิสัยทัศน์และกลยุทธ์ขององค์กร: เช่น หากองค์กรมีเป้าหมายในการขยายตลาดออนไลน์ ก็ควรมีวัตถุประสงค์และเป้าหมายด้านความปลอดภัยที่สนับสนุนการเติบโตของช่องทางดังกล่าว

2. เฉพาะเจาะจง (Specific): เช่น แทนที่จะบอกว่า "ปรับปรุงความปลอดภัย" ควรระบุว่า "ลดช่องโหว่ในระบบเครือข่ายลง 50% (จากที่สำรวจไว้)"

3. วัดผลได้ (Measurable): ควรมีตัวชี้วัดที่ชัดเจน เพื่อให้สามารถติดตามความคืบหน้าและประเมินผลสำเร็จได้ เช่น "ลดระยะเวลาในการตอบสนองต่อเหตุการณ์ด้านความปลอดภัยลง 10%" หรือ "เพิ่มอัตราการตรวจจับมัลแวร์ได้ 95%"

4. ทำได้จริง (Achievable): ควรมีความท้าทาย แต่ก็ต้องสามารถบรรลุได้จริง โดยคำนึงถึงทรัพยากรและขีดความสามารถขององค์กร รวมถึงทราบ (หรือสร้าง) กลไก และ ขั้นตอนที่จะไปถึงเป้าหมาย

5. เกี่ยวข้อง (Relevant): ควรมีความเกี่ยวข้องกับความเสี่ยงและความต้องการขององค์กร เช่น หากองค์กรมีข้อมูลลูกค้าจำนวนมาก ก็ควรมีเป้าหมายในการปกป้องข้อมูลลูกค้า

6. มีกรอบเวลา (Time-bound): ควรมีกรอบเวลาที่ชัดเจน เพื่อให้สามารถติดตามความคืบหน้าและประเมินผลสำเร็จได้ เช่น "ติดตั้งระบบป้องกันการบุกรุกภายใน **3 เดือน**" หรือ "อบรมพนักงานทั้งหมดให้มีความรู้ด้านความปลอดภัยทางไซเบอร์ภายใน **สิ้นปีนี้**"

(ตัวอย่าง) วัตถุประสงค์และเป้าหมายด้านความปลอดภัยทางไซเบอร์

วัตถุประสงค์:

- สร้างความมั่นใจในความปลอดภัยของข้อมูลและระบบสารสนเทศ
- ลดความเสี่ยงด้านความปลอดภัยทางไซเบอร์ให้อยู่ในระดับที่ยอมรับได้
- สร้างความตระหนักด้านความปลอดภัยทางไซเบอร์ให้กับบุคลากร
- ปรับปรุงความสามารถในการตอบสนองต่อเหตุการณ์ด้านความปลอดภัย
- ปฏิบัติตามกฎหมายและข้อบังคับด้านความปลอดภัยข้อมูล

เป้าหมาย:

- ลดจำนวนเหตุการณ์ด้านความปลอดภัยลง 25% ภายในปีหน้า
- ลดระยะเวลาในการตรวจจับและตอบสนองต่อเหตุการณ์ลง 15% ภายใน 6 เดือน
- อบรมพนักงานทั้งหมดให้มีความรู้ด้านความปลอดภัยทางไซเบอร์ภายในสิ้นปีนี้
- ติดตั้งระบบป้องกันการบุกรุกและระบบตรวจจับความผิดปกติภายใน 3 เดือน
- ได้รับการรับรองตามมาตรฐาน ISO 27001 ภายใน 2 ปี
- ประเมินความเสี่ยงด้านความปลอดภัยทางไซเบอร์อย่างน้อยปีละครั้ง
- ปรับปรุงนโยบายด้านความปลอดภัยทางไซเบอร์ให้ทันสมัยทุก 6 เดือน

องค์ประกอบสำคัญของ Personalized Cybersecurity Playbook

กลยุทธ์และมาตรการ

(Strategies & Controls)

กลยุทธ์และมาตรการ (Strategies & Controls) เป็นส่วนสำคัญในการนำ Personalized Cybersecurity Playbook ไปปฏิบัติจริง โดยหัวข้อนี้จะครอบคลุมแนวทางและมาตรการต่างๆ ที่องค์กรใช้ในการป้องกัน ตรวจจับ ตอบสนอง และกู้คืนจากภัยคุกคามทางไซเบอร์

กลยุทธ์ (Strategies) คือ แนวทางหรือแผนการปฏิบัติงานในภาพรวม เพื่อให้บรรลุวัตถุประสงค์และเป้าหมายด้านความปลอดภัยทางไซเบอร์ขององค์กร ซึ่งกลยุทธ์ที่ดีควรมีความชัดเจน ครอบคลุม และ สอดคล้องกับความเสี่ยงและความต้องการขององค์กร

มาตรการ (Controls) คือ วิธีการหรือกลไกที่นำมาใช้เพื่อควบคุมหรือลดความเสี่ยงที่ระบุไว้ซึ่งมาตรการต่างๆ ควรมีความเฉพาะเจาะจง สามารถวัดผลได้ และสอดคล้องกับกลยุทธ์ที่กำหนดไว้

กรอบแนวคิดในการกำหนดกลยุทธ์และมาตรการ

ควรพิจารณาถึง 4 ด้านหลัก ได้แก่

1. **การป้องกัน (Prevention):**
2. **การตรวจจับ (Detection):**
3. **การตอบสนอง (Response):**
4. **การกู้คืน (Recovery):**

องค์ประกอบสำคัญของ Personalized Cybersecurity Playbook

ตัวอย่างกลยุทธ์และมาตรการในแต่ละด้าน

1. การป้องกัน (Prevention):

กลยุทธ์:

1.ลดช่องโหว่ของระบบ

2.ควบคุมการเข้าถึงข้อมูลและระบบ

3.ป้องกันมัลแวร์

4.ป้องกันการโจมตีทางเครือข่าย

5.สร้างความตระหนักด้านความปลอดภัย

มาตรการ:

1. ติดตั้งและปรับปรุงแพตช์ความปลอดภัย
2. ใช้ระบบการพิสูจน์ตัวตนที่แข็งแกร่ง (Multi-Factor Authentication)
3. จำกัดสิทธิ์การเข้าถึงข้อมูลและระบบตามหลักการ Least Privilege
4. ติดตั้งและปรับปรุงโปรแกรมป้องกันไวรัส
5. ติดตั้งไฟร์วอลล์และระบบป้องกันการบุกรุก (Intrusion Prevention System)
6. ฝึกอบรมพนักงานด้านความปลอดภัยทางไซเบอร์
7. กำหนดนโยบายด้านความปลอดภัยที่ชัดเจนและบังคับใช้
8. เข้ารหัสข้อมูลที่สำคัญ
9. ทำการสำรองข้อมูล (Backup) เป็นประจำ

2. การตรวจจับ (Detection):

กลยุทธ์:

1. ตรวจสอบกิจกรรมที่ไม่ปกติ
2. ตรวจจับมัลแวร์
3. ตรวจจับการบุกรุก
4. ติดตามความเคลื่อนไหวของภัยคุกคาม

มาตรการ:

1. ติดตั้งระบบตรวจจับการบุกรุก (Intrusion Detection System)
2. ติดตั้งระบบ Security Information and Event Management (SIEM)
3. ตรวจสอบบันทึกการเข้าถึง (Log) อย่างสม่ำเสมอ
4. ใช้ระบบ Honey Pot เพื่อล่อให้ผู้โจมตีเข้ามา
5. ติดตามข่าวสารและภัยคุกคามล่าสุด
6. ทำการทดสอบเจาะระบบ (Penetration Testing)
7. ใช้ระบบ Endpoint Detection and Response (EDR)

3. การตอบสนอง (Response):

กลยุทธ์:

1. ระบุและประเมินผลกระทบของเหตุการณ์
2. ควบคุมและจำกัดความเสียหาย
3. แก้ไขปัญหาและกำจัดภัยคุกคาม
4. สื่อสารกับผู้ที่เกี่ยวข้อง

มาตรการ:

1. จัดตั้งทีมตอบสนองต่อเหตุการณ์ด้านความปลอดภัย (Incident Response Team)
2. กำหนดแผนการตอบสนองต่อเหตุการณ์ (Incident Response Plan)
3. ใช้เครื่องมือและเทคโนโลยีในการวิเคราะห์เหตุการณ์
4. สื่อสารกับผู้บริหาร, พนักงาน, และลูกค้าที่ได้รับผลกระทบ
5. เก็บรวบรวมหลักฐานและข้อมูลที่เกี่ยวข้องกับเหตุการณ์
6. ประเมินผลและปรับปรุงแผนการตอบสนอง

4. การกู้คืน (Recovery):

กลยุทธ์:

1.กู้คืนระบบและข้อมูลที่ได้รับผลกระทบ

2.กลับมาดำเนินธุรกิจได้ตามปกติ

3.ป้องกันการเกิดเหตุการณ์ซ้ำ

มาตรการ:

1.กู้คืนระบบจากข้อมูลสำรอง (Backup and Restore)

2.ทดสอบแผนการกู้คืนอย่างสม่ำเสมอ

3.ปรับปรุงระบบและมาตรการรักษาความปลอดภัย

4.วิเคราะห์สาเหตุของเหตุการณ์

5.เรียนรู้จากบทเรียนที่ได้รับ

การเลือกกลยุทธ์และมาตรการที่เหมาะสม

ในการเลือกกลยุทธ์และมาตรการที่เหมาะสม ควรพิจารณาปัจจัยต่างๆ ดังนี้:

- **ความเสี่ยงขององค์กร:** มาตรการควรสอดคล้องกับความเสี่ยงที่องค์กรกำลังเผชิญอยู่
- **ทรัพยากรที่มี:** มาตรการควรเหมาะสมกับงบประมาณและทรัพยากรที่มีอยู่
- **ข้อกำหนดทางกฎหมาย:** มาตรการควรสอดคล้องกับกฎหมายและข้อบังคับที่เกี่ยวข้อง
- **ความซับซ้อนของระบบ:** มาตรการควรเหมาะสมกับความซับซ้อนของระบบและโครงสร้างพื้นฐานขององค์กร
- **ความต้องการของธุรกิจ:** มาตรการควรสนับสนุนเป้าหมายทางธุรกิจขององค์กร

องค์ประกอบสำคัญของ Personalized Cybersecurity Playbook

บทบาทและความรับผิดชอบ

(Roles & Responsibilities)

ความสำคัญของการกำหนดบทบาทและความรับผิดชอบ

- **ความชัดเจน:** ทำให้ทุกคนในองค์กรรู้ว่าตนเองมีหน้าที่และความรับผิดชอบอะไรบ้าง
- **การทำงานร่วมกัน:** ช่วยให้บุคลากรและหน่วยงานต่างๆ สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ
- **การหลีกเลี่ยงความซ้ำซ้อน:** ลดความซ้ำซ้อนในการทำงานและช่วยให้การดำเนินงานเป็นไปอย่างราบรื่น
- **ความรับผิดชอบ:** สร้างความรู้สึกรับผิดชอบต่อความปลอดภัยทางไซเบอร์ในทุกระดับขององค์กร
- **การตรวจสอบ:** ช่วยให้สามารถตรวจสอบและติดตามการดำเนินงานด้านความปลอดภัยได้อย่างมีประสิทธิภาพ

การกำหนดบทบาทและความรับผิดชอบ

ในการกำหนดบทบาทและความรับผิดชอบ ควรพิจารณาถึง:

1. **โครงสร้างองค์กร:** โครงสร้างองค์กรและสายงานบังคับบัญชาที่มีอยู่
2. **ความเชี่ยวชาญของบุคลากร:** ความรู้และทักษะของบุคลากรแต่ละคน
3. **ความเสี่ยงของแต่ละหน่วยงาน:** ความเสี่ยงที่แต่ละหน่วยงานต้องเผชิญ
4. **ขนาดขององค์กร:** ขนาดและลักษณะขององค์กร
5. **ทรัพยากรที่มี:** ทรัพยากรที่องค์กรมีอยู่

ตัวอย่างบทบาทและความรับผิดชอบด้านความปลอดภัยทางไซเบอร์

1. คณะกรรมการบริหาร (Board of Directors) หรือผู้บริหารระดับสูง :

1. กำหนดวิสัยทัศน์และกลยุทธ์ด้านความปลอดภัยทางไซเบอร์
2. อนุมัติงบประมาณสำหรับมาตรการด้านความปลอดภัย
3. ติดตามความคืบหน้าในการดำเนินงานด้านความปลอดภัย
4. ให้การสนับสนุนและส่งเสริมวัฒนธรรมความปลอดภัยทางไซเบอร์

2. ประธานเจ้าหน้าที่บริหารด้านความปลอดภัยสารสนเทศ (Chief Information Security Officer - CISO):

1. กำหนดและดำเนินการตามกลยุทธ์ด้านความปลอดภัย
2. บริหารจัดการความเสี่ยงด้านความปลอดภัย
3. กำกับดูแลการดำเนินงานด้านความปลอดภัย
4. รายงานสถานะด้านความปลอดภัยต่อผู้บริหารระดับสูง
5. เป็นผู้นำในการตอบสนองต่อเหตุการณ์ด้านความปลอดภัย

3. หัวหน้าฝ่ายไอที (Head of IT):

1. ดูแลโครงสร้างพื้นฐานด้านไอทีให้มีความปลอดภัย
2. ติดตั้งและบำรุงรักษาอุปกรณ์และระบบรักษาความปลอดภัย
3. บริหารจัดการการเข้าถึงระบบและข้อมูล
4. สนับสนุนการดำเนินงานด้านความปลอดภัยของ CISO

4. ทีมรักษาความปลอดภัยทางไซเบอร์ (Cybersecurity Team):

1. ตรวจสอบและประเมินความเสี่ยงด้านความปลอดภัย
2. ตรวจจับและตอบสนองต่อเหตุการณ์ด้านความปลอดภัย
3. ดำเนินการทดสอบเจาะระบบ (Penetration Testing)
4. ติดตามข่าวสารและภัยคุกคามล่าสุด
5. ให้คำแนะนำและสนับสนุนด้านความปลอดภัยแก่หน่วยงานอื่นๆ

5. ทีมเครือข่าย (Network Team):

1.ดูแลความปลอดภัยของเครือข่าย

2.ติดตั้งและบำรุงรักษาอุปกรณ์เครือข่าย

3.ตรวจสอบและแก้ไขปัญหาด้านเครือข่าย

4.สนับสนุนการดำเนินงานด้านความปลอดภัยของทีม Cybersecurity

6. ทีมพัฒนาแอปพลิเคชัน (Application Development Team):

1.พัฒนาแอปพลิเคชันที่ปลอดภัย

2.แก้ไขช่องโหว่ด้านความปลอดภัย

3.ปฏิบัติตามแนวทางการพัฒนาซอฟต์แวร์ที่ปลอดภัย

4.ทดสอบความปลอดภัยของแอปพลิเคชัน

7. พนักงานทั่วไป:

1.ปฏิบัติตามนโยบายด้านความปลอดภัยขององค์กร

2.ระมัดระวังในการใช้งานอุปกรณ์และระบบต่างๆ

3.รายงานเหตุการณ์ด้านความปลอดภัยที่พบ

4.เข้ารับการฝึกอบรมด้านความปลอดภัย

5.รักษาความลับของข้อมูลและรหัสผ่าน

8. ผู้จัดการฝ่ายต่างๆ:

1.สนับสนุนการดำเนินงานด้านความปลอดภัยของทีมงานในฝ่าย

2.สร้างความตระหนักด้านความปลอดภัยให้กับทีมงาน

3.สื่อสารและให้ข้อมูลด้านความปลอดภัยกับทีมงาน

4.ประเมินความเสี่ยงด้านความปลอดภัยในขอบเขตงานของตน

องค์ประกอบสำคัญของ Personalized Cybersecurity Playbook

แผนการสื่อสาร

(Communication Plan)

การสื่อสารบทบาทและความรับผิดชอบ

หลังจากกำหนดบทบาทและความรับผิดชอบแล้ว สิ่งสำคัญคือการสื่อสารให้ทุกคนในองค์กรเข้าใจบทบาทและความรับผิดชอบของตนเอง โดยอาจใช้วิธีการต่างๆ เช่น:

- **จัดทำเอกสาร:** จัดทำเอกสารที่อธิบายบทบาทและความรับผิดชอบของแต่ละตำแหน่งและหน่วยงาน
- **จัดประชุม:** จัดประชุมเพื่ออธิบายและทำความเข้าใจบทบาทและความรับผิดชอบ
- **จัดฝึกอบรม:** จัดฝึกอบรมเพื่อเสริมสร้างความรู้ความเข้าใจเกี่ยวกับบทบาทและความรับผิดชอบ
- **สื่อสารอย่างสม่ำเสมอ:** สื่อสารและทบทวนบทบาทและความรับผิดชอบอย่างสม่ำเสมอ

การทบทวนและปรับปรุง

ควรมีการทบทวนและปรับปรุงบทบาทและความรับผิดชอบอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับการเปลี่ยนแปลงขององค์กรและภัยคุกคามทางไซเบอร์

โดยสรุปแล้ว การกำหนดบทบาทและความรับผิดชอบที่ชัดเจน เป็นขั้นตอนสำคัญในการสร้าง Personalized Cybersecurity Playbook ที่มีประสิทธิภาพ ช่วยให้องค์กรสามารถดำเนินงานด้านความปลอดภัยได้อย่างราบรื่นและมีประสิทธิภาพ

องค์ประกอบสำคัญของ Personalized Cybersecurity Playbook

แผนการฝึกอบรม

(Training Plan)

ตัวอย่างเนื้อหาการฝึกอบรม

สำหรับพนักงานทั่วไป:

- พื้นฐานด้านความปลอดภัยทางไซเบอร์
- การระบุและป้องกันฟิชชิง
- การใช้รหัสผ่านที่ปลอดภัย
- การจัดการกับอุปกรณ์ส่วนตัวในการทำงาน (BYOD)
- การรายงานเหตุการณ์ด้านความปลอดภัย

สำหรับผู้บริหาร:

- ความสำคัญของความปลอดภัยทางไซเบอร์ต่อธุรกิจ
- การบริหารจัดการความเสี่ยงด้านความปลอดภัย
- การสนับสนุนการดำเนินงานด้านความปลอดภัย
- การทำความเข้าใจกับกฎหมายและข้อบังคับที่เกี่ยวข้อง

สำหรับทีมไอที:

- การตั้งค่าระบบและอุปกรณ์ให้ปลอดภัย
- การบริหารจัดการความปลอดภัยของเครือข่าย
- การตรวจจับและตอบสนองต่อเหตุการณ์ด้านความปลอดภัย
- การพัฒนาซอฟต์แวร์ที่ปลอดภัย
- การใช้เครื่องมือและเทคโนโลยีรักษาความปลอดภัย

องค์ประกอบสำคัญของ Personalized Cybersecurity Playbook

แผนการทดสอบและปรับปรุง

(Testing & Improvement Plan)

ความสำคัญของแผนการทดสอบและปรับปรุง

การมีแผนการทดสอบและปรับปรุงที่ชัดเจน มีความสำคัญต่อการรักษาความปลอดภัยทางไซเบอร์ขององค์กร ดังนี้:

- **ระบุจุดอ่อน:** ช่วยระบุจุดอ่อนและช่องโหว่ในระบบและกระบวนการรักษาความปลอดภัย
- **ประเมินประสิทธิภาพ:** ช่วยประเมินประสิทธิภาพของมาตรการรักษาความปลอดภัยที่ใช้
- **ปรับปรุงมาตรการ:** ช่วยปรับปรุงมาตรการรักษาความปลอดภัยให้มีประสิทธิภาพมากขึ้น
- **เตรียมพร้อมรับภัยคุกคาม:** ช่วยให้องค์กรเตรียมพร้อมรับมือกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น
- **ลดความเสี่ยง:** ช่วยลดความเสี่ยงที่อาจเกิดขึ้นจากภัยคุกคามทางไซเบอร์
- **สร้างความเชื่อมั่น:** สร้างความเชื่อมั่นให้กับลูกค้าและผู้มีส่วนได้ส่วนเสีย

องค์ประกอบของแผนการทดสอบและปรับปรุง

1. **การกำหนดวัตถุประสงค์ของการทดสอบ (Testing Objectives):**
    1. ระบุสิ่งที่ต้องการทดสอบ เช่น ประสิทธิภาพของระบบป้องกันการบุกรุก, การตอบสนองต่อเหตุการณ์ด้านความปลอดภัย, การกู้คืนระบบหลังเหตุการณ์
    2. กำหนดเป้าหมายที่สามารถวัดผลได้ เช่น ตรวจจับการโจมตี 95%, ลดเวลาในการตอบสนองต่อเหตุการณ์ลง 10%
2. **การเลือกวิธีการทดสอบ (Testing Methods):**
    1. **การทดสอบเจาะระบบ (Penetration Testing):** ทดสอบความแข็งแกร่งของระบบโดยจำลองการโจมตีจากผู้ไม่หวังดี
    2. **การทดสอบช่องโหว่ (Vulnerability Assessment):** สแกนระบบเพื่อหาช่องโหว่ที่อาจถูกโจมตี
    3. **การทดสอบการจำลองสถานการณ์ (Simulation Testing):** ทดสอบแผนการตอบสนองต่อเหตุการณ์โดยจำลองสถานการณ์จริง
    4. **การตรวจสอบความปลอดภัย (Security Audit):** ตรวจสอบการปฏิบัติตามนโยบายและมาตรฐานด้านความปลอดภัย
    5. **การตรวจสอบโค้ด (Code Review):** ตรวจสอบโค้ดโปรแกรมเพื่อหาช่องโหว่ที่อาจถูกโจมตี
    6. **การทดสอบความรู้และทักษะของพนักงาน (Awareness Testing):** ทดสอบความรู้และความตระหนักด้านความปลอดภัยของพนักงาน เช่น การจำลองการทำฟิชชิง

3. การกำหนดความถี่ของการทดสอบ (Testing Frequency):

1. กำหนดความถี่ในการทดสอบแต่ละประเภท เช่น ทดสอบเจาะระบบปีละครั้ง, ทดสอบช่องโหว่ไตรมาสละครั้ง, ทดสอบการจำลองสถานการณ์ปีละสองครั้ง
2. พิจารณาความเสี่ยงและทรัพยากรที่มีในการกำหนดความถี่

4. การกำหนดผู้รับผิดชอบในการทดสอบ (Testing Responsibilities):

1. กำหนดผู้รับผิดชอบในการวางแผน, ดำเนินการ, และวิเคราะห์ผลการทดสอบ
2. อาจใช้ผู้เชี่ยวชาญภายในองค์กรหรือผู้เชี่ยวชาญภายนอก

5. การวิเคราะห์ผลการทดสอบ (Test Result Analysis):

1. วิเคราะห์ผลการทดสอบเพื่อระบุจุดอ่อนและช่องโหว่ที่พบ
2. ประเมินประสิทธิภาพของมาตรการรักษาความปลอดภัยที่ใช้

6. การกำหนดแผนการปรับปรุง (Improvement Plan):

1. กำหนดแผนการปรับปรุงมาตรการรักษาความปลอดภัยโดยพิจารณาจากผลการทดสอบ
2. กำหนดผู้รับผิดชอบในการดำเนินการปรับปรุง
3. กำหนดกรอบเวลาในการปรับปรุง

7. การติดตามและประเมินผลการปรับปรุง (Follow-up & Evaluation):

1. ติดตามความคืบหน้าในการดำเนินการปรับปรุง
2. ประเมินประสิทธิภาพของการปรับปรุงที่ดำเนินการ
3. ทำการทดสอบซ้ำเพื่อประเมินผลการปรับปรุง

8. การปรับปรุง Cybersecurity Playbook (Playbook Update):

1. ปรับปรุง Cybersecurity Playbook ให้สอดคล้องกับการเปลี่ยนแปลงของภัยคุกคามและผลการทดสอบ
2. สื่อสารการเปลี่ยนแปลงใน Playbook ให้ทุกคนในองค์กรทราบ

ตัวอย่างแผนการทดสอบและปรับปรุง

การทดสอบเจาะระบบ:

- **วัตถุประสงค์:** ทดสอบความแข็งแกร่งของระบบเครือข่ายและแอปพลิเคชัน
- **วิธีการ:** ให้ผู้เชี่ยวชาญด้านความปลอดภัยภายนอกทำการจำลองการโจมตี
- **ความถี่:** ปีละครั้ง
- **การวิเคราะห์ผล:** ระบุช่องโหว่ที่พบและประเมินความเสี่ยง
- **การปรับปรุง:** ปรับปรุงระบบและมาตรการรักษาความปลอดภัยเพื่อแก้ไขช่องโหว่ที่พบ

การทดสอบการจำลองสถานการณ์ (ตั้งเป้าหมายจำลองเพื่อทบทวนกระบวนการ หรือ เพื่อมองหาช่องโหว่):

- **วัตถุประสงค์:** ทดสอบแผนการตอบสนองต่อเหตุการณ์ด้านความปลอดภัย
- **วิธีการ:** จำลองสถานการณ์การโจมตีทางไซเบอร์และประเมินการตอบสนองของทีมงาน
- **ความถี่:** ปีละสองครั้ง
- **การวิเคราะห์ผล:** ประเมินประสิทธิภาพของแผนการตอบสนองและระบุจุดที่ต้องปรับปรุง
- **การปรับปรุง:** ปรับปรุงแผนการตอบสนองให้มีประสิทธิภาพมากขึ้น

ตัวอย่างที่ 1: กรณีศึกษาบริษัทค้าปลีกออนไลน์

บริบท: บริษัทค้าปลีกออนไลน์ขนาดกลาง มีข้อมูลลูกค้าจำนวนมาก และทำธุรกรรมทางการเงินออนไลน์เป็นประจำ

วัตถุประสงค์หลัก: เพื่อตรวจสอบและปรับปรุงความปลอดภัยของระบบและข้อมูลลูกค้า

แผนการทดสอบและปรับปรุง:

1.การทดสอบเจาะระบบ (Penetration Testing):

1. **วัตถุประสงค์:** ทดสอบความแข็งแกร่งของระบบเว็บแอปพลิเคชันและเซิร์ฟเวอร์
2. **วิธีการ:** จ้างบริษัทภายนอกที่มีความเชี่ยวชาญด้านการเจาะระบบ ทำการจำลองการโจมตีหลากหลายรูปแบบ (เช่น SQL Injection, Cross-Site Scripting)
3. **ความถี่:** ปีละครั้ง
4. **ผู้รับผิดชอบ:** หัวหน้าทีม IT และผู้เชี่ยวชาญจากภายนอก
5. **การวิเคราะห์ผล:** รายงานผลการทดสอบจากบริษัทภายนอก จะระบุช่องโหว่ที่พบ ระดับความเสี่ยง และข้อเสนอแนะในการแก้ไข
6. **การปรับปรุง:** ทีม IT จะดำเนินการแก้ไขช่องโหว่ตามรายงาน และตรวจสอบซ้ำหลังการแก้ไข

1. **การทดสอบช่องโหว่ (Vulnerability Assessment):**
    1. **วัตถุประสงค์:** สแกนระบบเครือข่ายและอุปกรณ์ต่างๆ เพื่อหาช่องโหว่ที่อาจเกิดขึ้น
    2. **วิธีการ:** ใช้เครื่องมือสแกนช่องโหว่อัตโนมัติ (Automated Vulnerability Scanner)
    3. **ความถี่:** ไตรมาสละครั้ง
    4. **ผู้รับผิดชอบ:** ทีม IT
    5. **การวิเคราะห์ผล:** ทีม IT จะวิเคราะห์ผลการสแกน และจัดลำดับความสำคัญในการแก้ไขช่องโหว่
    6. **การปรับปรุง:** ทีม IT จะดำเนินการแก้ไขช่องโหว่ที่พบ โดยเริ่มจากช่องโหว่ที่มีความเสี่ยงสูง
2. **การทดสอบการจำลองสถานการณ์ (Simulation Testing):**
    1. **วัตถุประสงค์:** ทดสอบแผนการตอบสนองต่อเหตุการณ์ด้านความปลอดภัย (Incident Response Plan)
    2. **วิธีการ:** ทีมรักษาความปลอดภัยทางไซเบอร์จะจำลองสถานการณ์การโจมตี DDoS หรือการรั่วไหลของข้อมูล และประเมินการตอบสนองของทีม IT และทีมที่เกี่ยวข้อง
    3. **ความถี่:** ปีละสองครั้ง
    4. **ผู้รับผิดชอบ:** หัวหน้าทีมรักษาความปลอดภัยทางไซเบอร์
    5. **การวิเคราะห์ผล:** ทีมรักษาความปลอดภัยทางไซเบอร์วิเคราะห์ประสิทธิภาพของแผน และระบุจุดที่ต้องปรับปรุง
    6. **การปรับปรุง:** ปรับปรุงแผนการตอบสนองและฝึกอบรมทีมงานให้พร้อมรับมือกับสถานการณ์ต่างๆ

3. การทดสอบความรู้และทักษะของพนักงาน (Awareness Testing):

1. **วัตถุประสงค์:** ทดสอบความตระหนักและความรู้ด้านความปลอดภัยของพนักงาน
2. **วิธีการ:** จัดแคมเปญฟิชชิงจำลอง (Simulated Phishing Campaign) และประเมินจำนวนพนักงานที่หลงกล
3. **ความถี่:** รายไตรมาส
4. **ผู้รับผิดชอบ:** ทีมทรัพยากรบุคคล (HR) และทีมรักษาความปลอดภัยทางไซเบอร์
5. **การวิเคราะห์ผล:** วิเคราะห์จำนวนพนักงานที่หลงกล และระบุประเด็นที่ต้องเน้นในการฝึกอบรม
6. **การปรับปรุง:** จัดฝึกอบรมเพิ่มเติมให้พนักงานที่มีความเสี่ยง และปรับปรุงสื่อการฝึกอบรมให้มีประสิทธิภาพมากขึ้น

แผนการปรับปรุง (Improvement Plan):

- **การแก้ไขช่องโหว่:** ทีม IT จะแก้ไขช่องโหว่ที่พบจากการทดสอบเจาะระบบและช่องโหว่ โดยเริ่มจากช่องโหว่ที่มีความเสี่ยงสูง และติดตามผลการแก้ไข
- **การปรับปรุงแผนการตอบสนอง:** ทีมรักษาความปลอดภัยทางไซเบอร์จะปรับปรุงแผนการตอบสนองต่อเหตุการณ์ด้านความปลอดภัย โดยพิจารณาจากผลการทดสอบการจำลองสถานการณ์
- **การปรับปรุงการฝึกอบรม:** ทีม HR และทีมรักษาความปลอดภัยทางไซเบอร์จะปรับปรุงเนื้อหาและวิธีการฝึกอบรม โดยพิจารณาจากผลการทดสอบความรู้และทักษะของพนักงาน
- **การปรับปรุงนโยบายและมาตรฐาน:** ทบทวนและปรับปรุงนโยบายและมาตรฐานด้านความปลอดภัยให้ทันสมัยอยู่เสมอ
- **การลงทุนในเทคโนโลยี:** พิจารณาลงทุนในเทคโนโลยีใหม่ๆ ที่สามารถช่วยเพิ่มความปลอดภัยให้กับระบบ

การติดตามและประเมินผล:

- ทีม IT และทีมรักษาความปลอดภัยทางไซเบอร์จะติดตามผลการแก้ไขช่องโหว่ และประเมินประสิทธิภาพของการปรับปรุงที่ดำเนินการ
- ทำการทดสอบซ้ำเพื่อประเมินผลการปรับปรุง
- รายงานผลการทดสอบและการปรับปรุงให้ผู้บริหารระดับสูงทราบ

ตัวอย่างที่ 2: กรณีศึกษาโรงงานผลิต

บริบท: โรงงานผลิตขนาดใหญ่ มีระบบควบคุมการผลิตอัตโนมัติ (Industrial Control System - ICS) ที่เชื่อมต่อกับเครือข่าย

วัตถุประสงค์หลัก: เพื่อป้องกันการโจมตีที่อาจส่งผลกระทบต่อการผลิต

แผนการทดสอบและปรับปรุง:

1. การทดสอบเจาะระบบเฉพาะ ICS (ICS Penetration Testing):

1. **วัตถุประสงค์:** ทดสอบความปลอดภัยของระบบควบคุมการผลิต
2. **วิธีการ:** จ้างผู้เชี่ยวชาญด้าน ICS Security ทำการจำลองการโจมตี
3. **ความถี่:** ปีละครั้ง
4. **การวิเคราะห์ผล:** รายงานจากผู้เชี่ยวชาญจะระบุช่องโหว่ในระบบ ICS และข้อเสนอแนะ
5. **การปรับปรุง:** ทีมวิศวกรและทีม IT จะดำเนินการแก้ไขช่องโหว่และปรับปรุงระบบ ICS

2. การประเมินความเสี่ยงของระบบ ICS (ICS Risk Assessment):

1. **วัตถุประสงค์:** ประเมินความเสี่ยงที่อาจเกิดขึ้นกับระบบ ICS
2. **วิธีการ:** ใช้แนวทางการประเมินความเสี่ยงด้าน ICS ที่ได้มาตรฐาน
3. **ความถี่:** ปีละครั้ง
4. **การวิเคราะห์ผล:** ระบุความเสี่ยงที่อาจเกิดขึ้น และจัดลำดับความสำคัญในการแก้ไข
5. **การปรับปรุง:** ปรับปรุงมาตรการป้องกันและควบคุมความเสี่ยง

3. การทดสอบการกู้คืนระบบ ICS (ICS Disaster Recovery Testing):

1. **วัตถุประสงค์:** ทดสอบแผนการกู้คืนระบบ ICS หลังเกิดเหตุการณ์
2. **วิธีการ:** จำลองเหตุการณ์ระบบขัดข้องและประเมินความสามารถในการกู้คืนระบบ
3. **ความถี่:** ปีละครั้ง
4. **การวิเคราะห์ผล:** ประเมินประสิทธิภาพของแผนการกู้คืนและระบุจุดที่ต้องปรับปรุง
5. **การปรับปรุง:** ปรับปรุงแผนการกู้คืนและฝึกอบรมทีมงานให้พร้อมรับมือ

4. การตรวจสอบการปฏิบัติตามมาตรฐาน ICS (ICS Compliance Audit):

1. **วัตถุประสงค์:** ตรวจสอบการปฏิบัติตามมาตรฐานด้านความปลอดภัยของ ICS (เช่น NIST SP 800-82)
2. **วิธีการ:** จ้างผู้ตรวจสอบภายนอกทำการตรวจสอบ
3. **ความถี่:** ปีละครั้ง
4. **การวิเคราะห์ผล:** ระบุความไม่สอดคล้องกับการปฏิบัติตามมาตรฐาน
5. **การปรับปรุง:** ปรับปรุงกระบวนการและมาตรการเพื่อให้สอดคล้องกับมาตรฐาน

แผนการปรับปรุง (Improvement Plan):

- **การปรับปรุงระบบ ICS:** ปรับปรุงระบบและอุปกรณ์ ICS เพื่อแก้ไขช่องโหว่ที่พบ
- **การปรับปรุงมาตรการป้องกัน:** ปรับปรุงมาตรการป้องกันการโจมตีและควบคุมความเสี่ยง
- **การปรับปรุงแผนกู้คืนระบบ:** ปรับปรุงแผนการกู้คืนระบบให้มีประสิทธิภาพมากขึ้น
- **การฝึกอบรมพนักงาน:** จัดฝึกอบรมให้พนักงานที่เกี่ยวข้องกับระบบ ICS เพื่อเพิ่มความรู้และทักษะ
- **การลงทุนในเทคโนโลยี:** พิจารณาลงทุนในเทคโนโลยีใหม่ๆ เพื่อเพิ่มความปลอดภัยให้กับระบบ ICS

การติดตามและประเมินผล:

- ทีมวิศวกรและทีม IT จะติดตามผลการแก้ไขช่องโหว่ และประเมินประสิทธิภาพของการปรับปรุงที่ดำเนินการ
- ทำการทดสอบซ้ำเพื่อประเมินผลการปรับปรุง
- รายงานผลการทดสอบและการปรับปรุงให้ผู้บริหารทราบ

Module 7: Cybersecurity Mindset and Culture/ Communication Plan to Outside and Inside

1 Cybersecurity Mindset สำหรับผู้บริหาร

- ความเข้าใจในความสำคัญของ Cybersecurity
- การเป็นแบบอย่างที่ดีในการปฏิบัติตามนโยบาย
- การสร้างวัฒนธรรม Cybersecurity ในองค์กร

2 การสร้าง Cybersecurity Culture

- การฝึกอบรมและสร้างความตระหนักรู้ให้กับพนักงาน
- การสื่อสารและการมีส่วนร่วมจากพนักงาน
- การสร้างแรงจูงใจในการปฏิบัติตามนโยบาย

3 การสื่อสาร Cybersecurity

- การสื่อสารภายในองค์กร (พนักงาน, ผู้บริหาร)
- การสื่อสารภายนอกองค์กร (ลูกค้า, คู่ค้า, สาธารณะ)
- ช่องทางและเทคนิคการสื่อสารที่เหมาะสม

1. Cybersecurity Mindset สำหรับผู้บริหาร

- **ความเข้าใจในความสำคัญของ Cybersecurity:**
  - **ความเสี่ยงทางธุรกิจ:** ผู้บริหารต้องเข้าใจว่าภัยคุกคามทางไซเบอร์ไม่ใช่แค่ปัญหาทางเทคนิค แต่เป็นความเสี่ยงทางธุรกิจที่ส่งผลกระทบต่อความน่าเชื่อถือ ชื่อเสียง ผลกำไร และความต่อเนื่องทางธุรกิจ
  - **ผลกระทบต่อองค์กร:** ต้องตระหนักถึงผลกระทบที่อาจเกิดขึ้นจากการละเมิดความปลอดภัยทางไซเบอร์ เช่น การสูญเสียข้อมูลสำคัญ การถูกขัดขวางการดำเนินงาน การถูกฟ้องร้อง หรือการสูญเสียความไว้วางใจจากลูกค้า
  - **การลงทุนเชิงกลยุทธ์:** มองว่าการลงทุนด้าน Cybersecurity เป็นการลงทุนเชิงกลยุทธ์ที่สำคัญ ไม่ใช่แค่ค่าใช้จ่าย เพื่อป้องกันความเสียหายและสร้างความได้เปรียบในการแข่งขัน
  - **การเปลี่ยนแปลงของภัยคุกคาม:** ต้องเข้าใจว่าภัยคุกคามทางไซเบอร์มีการเปลี่ยนแปลงและพัฒนาอยู่ตลอดเวลา ต้องติดตามและปรับปรุงมาตรการรักษาความปลอดภัยอย่างต่อเนื่อง
- **การเป็นแบบอย่างที่ดีในการปฏิบัติตามนโยบาย:**
  - **การปฏิบัติตามกฎระเบียบ:** ผู้บริหารต้องปฏิบัติตามนโยบายและขั้นตอนด้าน Cybersecurity ขององค์กรอย่างเคร่งครัด ไม่ว่าจะเป็นการใช้รหัสผ่านที่ปลอดภัย การระมัดระวังในการคลิกลิงก์ การใช้งานอุปกรณ์ขององค์กรอย่างเหมาะสม
  - **การให้ความสำคัญ:** แสดงให้เห็นถึงความสำคัญของ Cybersecurity ด้วยการเข้าร่วมการอบรมหรือการประชุมที่เกี่ยวข้อง และสนับสนุนการดำเนินงานด้านนี้อย่างเต็มที่
  - **การเป็นผู้นำ:** เป็นผู้นำในการสร้างวัฒนธรรม Cybersecurity ในองค์กร ด้วยการสื่อสารและแสดงออกถึงความมุ่งมั่นในการรักษาความปลอดภัย
- **การสร้างวัฒนธรรม Cybersecurity ในองค์กร:**
  - **การสื่อสารและส่งเสริม:** สื่อสารให้พนักงานทุกคนเข้าใจถึงความสำคัญของ Cybersecurity และบทบาทของแต่ละคนในการรักษาความปลอดภัยขององค์กร
  - **การสนับสนุนและการให้กำลังใจ:** สนับสนุนการดำเนินงานด้าน Cybersecurity และให้กำลังใจพนักงานที่ปฏิบัติตามนโยบายอย่างเคร่งครัด
  - **การสร้างความตระหนักรู้:** สร้างความตระหนักรู้และกระตุ้นให้พนักงานมีส่วนร่วมในการรักษาความปลอดภัยขององค์กรอย่างสม่ำเสมอ
  - **การเปิดโอกาสให้แสดงความคิดเห็น:** เปิดโอกาสให้พนักงานแสดงความคิดเห็นและข้อเสนอแนะเกี่ยวกับมาตรการด้าน Cybersecurity เพื่อให้เกิดการมีส่วนร่วมและปรับปรุงให้ดียิ่งขึ้น

2. การสร้าง Cybersecurity Culture

- **การฝึกอบรมและสร้างความตระหนักรู้ให้กับพนักงาน:**
  - **การฝึกอบรมที่สม่ำเสมอ:** จัดอบรมด้าน Cybersecurity ให้กับพนักงานทุกคนอย่างสม่ำเสมอ โดยครอบคลุมหัวข้อต่างๆ เช่น การระบุอีเมลฟิชชิง การจัดการรหัสผ่านที่ปลอดภัย การใช้งานอุปกรณ์อย่างปลอดภัย
  - **การฝึกอบรมที่เหมาะสมกับบทบาท:** ปรับเนื้อหาการฝึกอบรมให้เหมาะสมกับบทบาทหน้าที่ของแต่ละคน เพื่อให้เข้าใจถึงความเสี่ยงที่เกี่ยวข้องและวิธีปฏิบัติที่ถูกต้อง
  - **การใช้สื่อที่หลากหลาย:** ใช้สื่อการฝึกอบรมที่หลากหลาย เช่น วิดีโอ อินโฟกราฟิก หรือเกม เพื่อดึงดูดความสนใจและทำให้เข้าใจง่าย
  - **การประเมินผล:** ประเมินผลการฝึกอบรมเพื่อวัดความเข้าใจและประสิทธิภาพของโปรแกรมการฝึกอบรม
- **การสื่อสารและการมีส่วนร่วมจากพนักงาน:**
  - **การสื่อสารที่เปิดเผยและโปร่งใส:** สื่อสารข้อมูลด้าน Cybersecurity อย่างเปิดเผยและโปร่งใส เพื่อให้พนักงานเข้าใจสถานการณ์และรับทราบถึงความเสี่ยงที่อาจเกิดขึ้น
  - **การรับฟังความคิดเห็น:** เปิดโอกาสให้พนักงานแสดงความคิดเห็นและข้อเสนอแนะเกี่ยวกับมาตรการด้าน Cybersecurity เพื่อให้เกิดการมีส่วนร่วมและปรับปรุงให้ดียิ่งขึ้น
  - **การสร้างกิจกรรม:** จัดกิจกรรมที่ส่งเสริมการมีส่วนร่วม เช่น การแข่งขัน การตอบคำถาม หรือการทำแบบทดสอบ เพื่อสร้างความสนุกสนานและส่งเสริมการเรียนรู้
  - **การยกย่องชมเชย:** ยกย่องชมเชยพนักงานที่ปฏิบัติตามนโยบายด้าน Cybersecurity อย่างเคร่งครัด เพื่อเป็นแบบอย่างที่ดีและสร้างแรงจูงใจ
- **การสร้างแรงจูงใจในการปฏิบัติตามนโยบาย:**
  - **การให้รางวัล:** มอบรางวัลหรือสิ่งจูงใจให้กับพนักงานที่ปฏิบัติตามนโยบายด้าน Cybersecurity อย่างเคร่งครัด หรือมีส่วนร่วมในการรายงานเหตุการณ์ด้านความปลอดภัย
  - **การสร้างความเข้าใจในผลประโยชน์:** สื่อสารให้พนักงานเข้าใจถึงผลประโยชน์ของการปฏิบัติตามนโยบายด้าน Cybersecurity ทั้งต่อองค์กรและต่อตัวพนักงานเอง
  - **การสร้างสภาพแวดล้อมที่เอื้อต่อการปฏิบัติ:** สร้างสภาพแวดล้อมที่เอื้อต่อการปฏิบัติตามนโยบายด้าน Cybersecurity เช่น การจัดหาเครื่องมือและทรัพยากรที่จำเป็น
  - **การแก้ไขข้อบกพร่อง:** แก้ไขข้อบกพร่องหรือข้อจำกัดที่อาจทำให้พนักงานไม่สามารถปฏิบัติตามนโยบายได้อย่างเต็มที่

3. การสื่อสาร Cybersecurity

•การสื่อสารภายในองค์กร (พนักงาน, ผู้บริหาร):

- **•การสื่อสารที่ชัดเจนและเข้าใจง่าย:** ใช้ภาษาที่เข้าใจง่าย ไม่ใช้ศัพท์เทคนิคที่ยากเกินไป เพื่อให้ทุกคนสามารถเข้าใจข้อมูลด้าน Cybersecurity ได้
- **•การสื่อสารที่สม่ำเสมอ:** สื่อสารข้อมูลด้าน Cybersecurity อย่างสม่ำเสมอ ไม่ว่าจะเป็นการแจ้งเตือนภัยคุกคาม การปรับปรุงนโยบาย หรือการให้ความรู้
- **•การสื่อสารสองทาง:** เปิดโอกาสให้พนักงานและผู้บริหารสามารถสื่อสารกันได้ทั้งสองทาง ไม่ว่าจะเป็นการสอบถามข้อสงสัย หรือการเสนอแนะความคิดเห็น
- **•การใช้ช่องทางที่เหมาะสม:** ใช้ช่องทางการสื่อสารที่เหมาะสม เช่น อีเมล อินทราเน็ต หรือการประชุม เพื่อให้มั่นใจว่าข้อมูลจะเข้าถึงทุกคน

•การสื่อสารภายนอกองค์กร (ลูกค้า, คู่ค้า, สาธารณะ):

- **•การสื่อสารที่โปร่งใส:** สื่อสารข้อมูลด้าน Cybersecurity อย่างโปร่งใสและซื่อสัตย์ ไม่ปิดบังข้อมูล หรือหลีกเลี่ยงความรับผิดชอบ
- **•การสื่อสารที่เหมาะสมกับกลุ่มเป้าหมาย:** ปรับภาษาและรูปแบบการสื่อสารให้เหมาะสมกับกลุ่มเป้าหมาย เพื่อให้เข้าใจข้อมูลได้อย่างถูกต้อง
- **•การให้ข้อมูลที่จำเป็น:** ให้ข้อมูลที่จำเป็นและเป็นประโยชน์ต่อลูกค้า คู่ค้า หรือสาธารณะ เพื่อให้เข้าใจถึงความเสี่ยงที่เกี่ยวข้องและมาตรการที่องค์กรใช้
- **•การสื่อสารในสถานการณ์วิกฤต:** เตรียมแผนการสื่อสารในสถานการณ์วิกฤต เช่น การเกิดการละเมิดข้อมูล เพื่อให้สามารถสื่อสารกับผู้ที่เกี่ยวข้องได้อย่างทันท่วงทีและมีประสิทธิภาพ

•ช่องทางและเทคนิคการสื่อสารที่เหมาะสม:

- **•อีเมล:** ใช้สำหรับการแจ้งข่าวสาร การประกาศ หรือการส่งข้อมูลที่เป็นทางการ
- **•อินทราเน็ต:** ใช้สำหรับการเผยแพร่ข้อมูล นโยบาย หรือคู่มือด้าน Cybersecurity ให้กับพนักงาน
- **•การประชุม:** ใช้สำหรับการสื่อสารสองทาง การอภิปราย หรือการฝึกอบรม
- **•วิดีโอ:** ใช้สำหรับการนำเสนอข้อมูล การฝึกอบรม หรือการสัมภาษณ์
- **•อินโฟกราฟิก:** ใช้สำหรับการนำเสนอข้อมูลที่ซับซ้อนให้เข้าใจง่าย
- **•โปสเตอร์หรือป้าย:** ใช้สำหรับการสื่อสารในที่สาธารณะ หรือในสำนักงาน
- **•สื่อสังคมออนไลน์:** ใช้สำหรับการสื่อสารกับลูกค้า คู่ค้า หรือสาธารณะ

ตัวอย่างโจทย์ Workshop จัดทำ Personal Cybersecurity Playbook

- # การตอบสนองเหตุการณ์ทางไซเบอร์ เช่น
  - การขโมยข้อมูล, การโจมตีโดย Ransomware หรือ Virus
  - ปริมาณการใช้ IT System สูงมากกว่าปกติ (Network/Application/Database)
  - ระบบล่มแบบ Crowd Strike
- # การย้ายระบบจาก Local Sever เข้าสู่คลาวด์
- # การนำ AI มาใช้ในองค์กร สำหรับงานด้าน.....
- # งานหลักขององค์กร (เช่น การพัฒนาซอฟต์แวร์ งานบริการรับเรื่องร้องเรียน งานพิจารณาสินเชื่อ)

Module 8: การจำลองสถานการณ์ เหตุการณ์ Cybersecurity แบบ Interactive เพื่อวิเคราะห์ Outcome ที่ได้จากบทเรียน

1 วัตถุประสงค์และประโยชน์ของ Cybersecurity Simulation

- การทดสอบประสิทธิภาพของแผน Incident Response
- การฝึกฝนการตัดสินใจและการประสานงาน
- การระบุจุดอ่อนและปรับปรุงแผนปฏิบัติการ

2 การจำลองสถานการณ์ Cyberattack แบบ Interactive

- การกำหนดสถานการณ์จำลองที่สอดคล้องกับภัยคุกคาม
- การแบ่งบทบาทและความรับผิดชอบของผู้เข้าร่วม
- การใช้เครื่องมือและเทคโนโลยีในการจำลองสถานการณ์

3 การวิเคราะห์ Outcome และบทเรียนที่ได้รับ

- การประเมินประสิทธิภาพของแผน Incident Response
- การระบุจุดแข็งและจุดอ่อนของทีมงาน
- การปรับปรุงแผนปฏิบัติการ

Cyber Security Attack Simulation

1. Phishing Attack Simulation
2. Ransomware Attack Simulation
3. Brute Force Attack Simulation
4. DDoS Attack Simulation
5. Insider Threat Simulation

Phishing Attack Simulation

สถานการณ์: ในการจำลองนี้ พนักงานจะได้รับอีเมลที่ดูเหมือนเป็นการสื่อสารทางธุรกิจที่ถูกต้องตามกฎหมาย ซึ่งเป็นอีเมลที่เกี่ยวข้องกับการทำงานในอุตสาหกรรม อย่างไรก็ตาม อีเมลดังกล่าวจะมีไฟล์แนบที่เป็นอันตรายแฝงอยู่ ซึ่งไฟล์แนบเหล่านี้อาจเป็นไวรัส มัลแวร์ หรือโปรแกรมที่ไม่พึงประสงค์อื่นๆ ที่สามารถสร้างความเสียหายต่อระบบคอมพิวเตอร์และข้อมูลขององค์กรได้

วัตถุประสงค์: ทดสอบความใส่ใจและการตอบสนองของพนักงานต่อเหตุการณ์ฟิชชิง หรือการหลอกลวงทางอีเมล โดยต้องการดูว่าพนักงานสามารถแยกแยะอีเมลที่น่าสงสัยออกจากอีเมลปกติได้หรือไม่ และจะมีการตอบสนองอย่างไรเมื่อได้รับอีเมลดังกล่าว

ผลลัพธ์: ผลลัพธ์ของการจำลองจะแสดงออกมาในรูปแบบของสถิติและเปอร์เซ็นต์ที่บ่งบอกถึงพฤติกรรมของพนักงานดังนี้:

- จำนวน (หรือ %) พนักงานที่ไม่สนใจอีเมลหรือไม่ได้คลิกลิงก์ที่อยู่ในอีเมล
- จำนวน (หรือ %) พนักงานที่ตระหนักถึงความผิดปกติของอีเมลและรายงานไปยังแผนกไอทีหรือผู้ที่เกี่ยวข้อง
- จำนวน (หรือ %) พนักงานที่หลงเชื่อและเปิดไฟล์แนบที่มาพร้อมกับอีเมล

Ransomware Attack Simulation

สถานการณ์: จำลองสถานการณ์โดยใช้สคริปต์แรนซัมแวร์ ซึ่งสคริปต์นี้จะพยายามเข้ารหัสเอกสารหรือไฟล์ต่างๆ ที่อยู่ในระบบนั้น ควรเป็นการจำลองการโจมตีด้วยแรนซัมแวร์ในสภาพแวดล้อมที่จำกัด เพื่อไม่ให้เกิดความเสียหายต่อระบบหลัก

วัตถุประสงค์: วัตถุประสงค์หลักของการจำลองนี้คือการประเมินประสิทธิภาพของระบบการตรวจจับภัยคุกคามที่ปลายทาง (Endpoint Identification), โปรแกรมป้องกันไวรัส (Antivirus Software), และกรอบการตอบสนองต่อเหตุการณ์ (Response Frameworks) ที่องค์กรมีอยู่ โดยต้องการตรวจสอบว่าระบบเหล่านี้สามารถตรวจจับและตอบสนองต่อภัยคุกคามแรนซัมแวร์ได้ดีเพียงใด

ผลลัพธ์: ผลลัพธ์ของการจำลองสถานการณ์นี้จะแสดงให้เห็นถึงสถานะต่างๆ ที่เกี่ยวข้องกับการตรวจจับแรนซัมแวร์ ซึ่งอาจรวมถึง:

- ระบบสามารถตรวจจับแรนซัมแวร์ได้หรือไม่ และหากตรวจจับได้ จะตรวจจับได้เมื่อใด (ในขั้นตอนไหน ระยะใด)
- หากระบบตรวจจับแรนซัมแวร์ได้ ระบบสามารถลบหรือกักกันแรนซัมแวร์ได้หรือไม่
- ใช้เวลานานเท่าใดในการตรวจจับและตอบสนองต่อแรนซัมแวร์

Brute Force Attack Simulation

สถานการณ์: ในการจำลองนี้ จะมีการจำลองการโจมตีแบบ Brute Force ซึ่งเป็นการพยายามเดารหัสผ่านของบัญชีผู้ใช้หรือระบบใดระบบหนึ่ง โดยการลองใส่รหัสผ่านที่เป็นไปได้ต่างๆ โดยอัตโนมัติอย่างต่อเนื่อง เพื่อพยายามเข้าถึงบัญชีหรือระบบนั้นๆ

วัตถุประสงค์: ตรวจสอบความแข็งแกร่งของกลยุทธ์การจัดการรหัสผ่าน (Password Strategies) และเทคโนโลยีการล็อกบัญชี (Account Lockout Technologies) ที่องค์กรใช้อยู่ โดยต้องการดูว่าระบบสามารถป้องกันการโจมตีแบบ Brute Force ได้ดีเพียงใด

ผลลัพธ์: ผลลัพธ์ของการจำลองสถานการณ์นี้จะแสดงให้เห็นถึงข้อมูลต่างๆ ที่เกี่ยวข้องกับการโจมตีแบบ Brute Force ซึ่งอาจรวมถึง:

- จำนวนครั้งที่ระบบพยายามเดารหัสผ่านก่อนที่จะมีการตรวจจับการโจมตี
- ระยะเวลาที่ใช้ในการบล็อกผู้โจมตีหลังจากตรวจพบความพยายามในการโจมตีแบบ Brute Force
- บัญชีผู้ใช้ได้รับความเสียหายหรือไม่ เช่น ถูกเข้าถึงโดยไม่ได้รับอนุญาต หรือถูกล็อก

DDoS Attack Simulation

สถานการณ์: เป็นการจำลองสถานการณ์การโจมตีแบบ Distributed Denial of Service (DDoS) ที่มุ่งเป้าไปที่โครงสร้างเครือข่ายขององค์กร โดยเป็นการจำลองการโจมตีที่มาจากหลายแหล่งพร้อมกัน เพื่อทำให้ระบบเครือข่ายหรือบริการต่างๆ ไม่สามารถใช้งานได้

วัตถุประสงค์: ประเมินประสิทธิภาพของโซลูชันด้านความปลอดภัย DDoS (DDoS Security Solutions) และความแข็งแกร่งของบริการเว็บ (Web Services) ที่องค์กรใช้อยู่ โดยต้องการตรวจสอบว่าระบบสามารถรับมือกับการโจมตีแบบ DDoS ได้ดีเพียงใด

ผลลัพธ์: ผลลัพธ์ของการจำลองสถานการณ์นี้จะแสดงให้เห็นถึงความสามารถในการรับมือและข้อมูลต่างๆ ที่เกี่ยวข้องกับการโจมตีแบบ DDoS ซึ่งอาจรวมถึง:

- ความรุนแรงของปริมาณการจราจรที่เข้ามาโจมตี และระยะเวลาที่การโจมตีดำเนินอยู่ก่อนที่จะมีการใช้มาตรการบรรเทา
- ระยะเวลาที่ระบบหรือบริการไม่สามารถใช้งานได้เนื่องจากการโจมตีแบบ DDoS

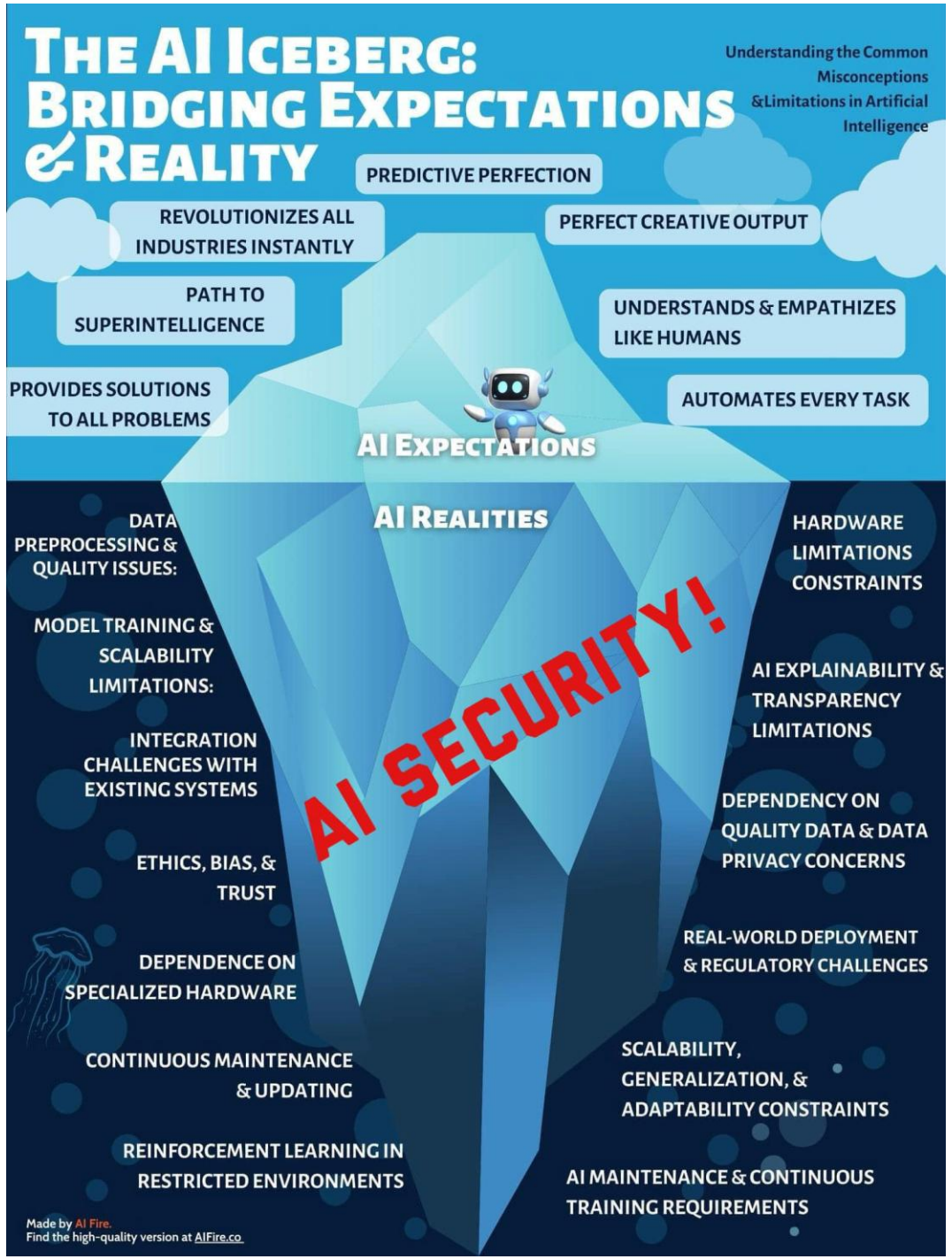
Insider Threat Simulation

สถานการณ์: จะเป็นการจำลองกิจกรรมที่เป็นภัยคุกคามจากภายในองค์กร ซึ่งรวมถึงการกระทำที่เป็นอันตราย เช่น การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือการนำข้อมูลออกไปโดยมิชอบ (excretion)

วัตถุประสงค์: ประเมินประสิทธิภาพของระบบการตรวจจับความผิดปกติ (Anomaly Identification Systems) และขั้นตอนด้านความปลอดภัยภายในองค์กร (Internal Safety Procedures) โดยต้องการตรวจสอบว่าระบบเหล่านี้สามารถตรวจจับและตอบสนองต่อภัยคุกคามจากภายในได้ดีเพียงใด

ผลลัพธ์: ผลลัพธ์ของการจำลองสถานการณ์นี้จะแสดงให้เห็นถึงตัวชี้วัดต่างๆ ที่เกี่ยวข้องกับภัยคุกคามจากภายใน ซึ่งอาจรวมถึง:

- ระบบตรวจจับกิจกรรมที่เป็นภัยคุกคามได้อย่างไร และตรวจจับได้เมื่อใด
- ข้อมูลประเภทใดที่ถูกเข้าถึงหรือนำออกไปโดยไม่ได้รับอนุญาต
- ระยะเวลาที่ใช้ในการตอบสนองต่อกิจกรรมที่เป็นภัยคุกคามหลังจากตรวจพบ


THE AI ICEBERG: BRIDGING EXPECTATIONS & REALITY
Understanding the Common Misconceptions &Limitations in Artificial Intelligence
PREDICTIVE PERFECTION
REVOLUTIONIZES ALL INDUSTRIES INSTANTLY
PERFECT CREATIVE OUTPUT
PATH TO SUPERINTELLIGENCE
UNDERSTANDS & EMPATHIZES LIKE HUMANS
PROVIDES SOLUTIONS TO ALL PROBLEMS
AUTOMATES EVERY TASK
AI EXPECTATIONS
AI REALITIES
AI SECURITY!
DATA PREPROCESSING & QUALITY ISSUES:
HARDWARE LIMITATIONS CONSTRAINTS
MODEL TRAINING & SCALABILITY LIMITATIONS:
AI EXPLAINABILITY & TRANSPARENCY LIMITATIONS
INTEGRATION CHALLENGES WITH EXISTING SYSTEMS
DEPENDENCY ON QUALITY DATA & DATA PRIVACY CONCERNS
ETHICS, BIAS, & TRUST
REAL-WORLD DEPLOYMENT & REGULATORY CHALLENGES
DEPENDENCE ON SPECIALIZED HARDWARE
SCALABILITY, GENERALIZATION, & ADAPTABILITY CONSTRAINTS
CONTINUOUS MAINTENANCE & UPDATING
REINFORCEMENT LEARNING IN RESTRICTED ENVIRONMENTS
AI MAINTENANCE & CONTINUOUS TRAINING REQUIREMENTS
Made by AI Fire.
Find the high-quality version at AIFire.co

References

- Cyber insurance: six questions every CEO should ask: PwC
  https://www.pwc.com/us/en/tech-effect/cybersecurity/buying-cybersecurity-insurance.html
- What Is Cyber Insurance and Should You Get It? | PCMag
  https://www.pcmag.com/news/what-is-cyber-insurance-and-should-you-get-it

เพื่อความปลอดภัยของระบบปัญญาประดิษฐ์ (AI) การมีแนวทางและมาตรฐานที่ชัดเจนเป็นสิ่งสำคัญ เพื่อให้สามารถนำ AI มาใช้งานได้อย่างปลอดภัยและเชื่อถือได้ ต่อไปนี้คือแนวทางและมาตรฐานที่ครอบคลุมด้านความปลอดภัยของ AI:

1. NIST AI Risk Management Framework (AI RMF):

พัฒนาโดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติของสหรัฐอเมริกา (NIST) เป็นกรอบแนวทางสำหรับการจัดการความเสี่ยงของ AI โดยเน้นหลักการโปร่งใส ความเป็นธรรม และความรับผิดชอบ ดูกรอบแนวทางนี้ได้ที่: nist.gov https://www.nist.gov/itl/ai-risk-management-framework

2. ISO/IEC 27090 - มาตรฐานด้านความปลอดภัยทางไซเบอร์สำหรับ AI:

มาตรฐานระดับสากลนี้ให้คำแนะนำสำหรับองค์กรในการจัดการภัยคุกคามด้านความปลอดภัยในระบบ AI ตลอดอายุการใช้งานของระบบ ช่วยให้องค์กรเข้าใจและจัดการกับผลกระทบของภัยคุกคามด้านความปลอดภัยในระบบ AI อ่านเพิ่มเติมได้ที่: iso.org https://www.iso.org/standard/56581.html

NIST Trustworthy and Responsible AI
NIST AI 600-1

Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile

This publication is available free of charge from:
https://doi.org/10.6028/NIST.AI.600-1

1. CBRN Information or Capabilities: Eased access to or synthesis of materially nefarious information or design capabilities related to **chemical, biological, radiological, or nuclear (CBRN)** weapons or other dangerous materials or agents.
2. **Confabulation:** The production of confidently stated but erroneous or false content (known colloquially as “hallucinations” or “fabrications”) by which users may be misled or deceived.
3. **Dangerous, Violent, or Hateful Content:** Eased production of and access to violent, inciting, radicalizing, or threatening content as well as recommendations to carry out self-harm or conduct illegal activities. Includes difficulty controlling public exposure to hateful and disparaging or stereotyping content.
4. **Data Privacy:** Impacts due to leakage and unauthorized use, disclosure, or de-anonymization of biometric, health, location, or other personally identifiable information or sensitive data.
5. **Environmental Impacts:** Impacts due to high compute resource utilization in training or operating GAI models, and related outcomes that may adversely impact ecosystems.

6. **Harmful Bias or Homogenization:** Amplification and exacerbation of historical, societal, and systemic biases; performance disparities between sub-groups or languages, possibly due to non-representative training data, that result in discrimination, amplification of biases, or incorrect presumptions about performance; undesired homogeneity that skews system or model outputs, which may be erroneous, lead to ill-founded decision-making, or amplify harmful biases.
7. **Human-AI Configuration:** Arrangements of or interactions between a human and an AI system which can result in the **human inappropriately anthropomorphizing** GAI systems or experiencing algorithmic aversion, automation bias, over-reliance, or emotional entanglement with GAI systems.
8. **Information Integrity:** Lowered barrier to entry to generate and support the exchange and consumption of content which may not distinguish fact from opinion or fiction or acknowledge uncertainties, or could be leveraged for large-scale dis- and mis-information campaigns.

9. **Information Security:** Lowered barriers for offensive cyber capabilities, including via automated discovery and exploitation of vulnerabilities to ease hacking, malware, phishing, offensive cyber operations, or other cyberattacks; increased attack surface for targeted cyberattacks, which may compromise a system's availability or the confidentiality or integrity of training data, code, or model weights.
10. **Intellectual Property:** Eased production or replication of alleged copyrighted, trademarked, or licensed content without authorization (possibly in situations which do not fall under fair use); eased exposure of trade secrets; or plagiarism or illegal replication.
11. **Obscene, Degrading, and/or Abusive Content:** Eased production of and access to obscene, degrading, and/or abusive imagery which can cause harm, including synthetic child sexual abuse material (CSAM), and nonconsensual intimate images (NCII) of adults.
12. **Value Chain and Component Integration:** Non-transparent or untraceable integration of upstream third-party components, including data that has been improperly obtained or not processed and cleaned due to increased automation from GAI; improper supplier vetting across the AI lifecycle; or other issues that diminish transparency or accountability for downstream users.

3. OWASP AI Security and Privacy Guide:

แนวทางจากโครงการ Open Web Application Security Project (OWASP) ซึ่งมุ่งเน้นการออกแบบ สร้าง ทดสอบ และจัดหา AI ที่มีความปลอดภัยและคำนึงถึงความเป็นส่วนตัว รวมถึงการป้องกันภัยคุกคามและการละเมิดความเป็นส่วนตัวในการพัฒนา AI https://owasp.org/www-project-ai-security-and-privacy-guide/

4. คำสั่งประธานาธิบดีเกี่ยวกับการพัฒนาและการใช้งาน AI อย่างปลอดภัยและเชื่อถือได้:

ประกาศโดยทำเนียบขาวของสหรัฐฯ ซึ่งเป็นนโยบายและหลักการเพื่อการพัฒนา AI อย่างปลอดภัย โดยเน้นการทดสอบ ประเมินผล และการตรวจสอบการทำงานหลังการนำไปใช้ เพื่อให้มั่นใจว่าระบบ AI จะทำงานตามที่คาดหวัง อ่านประกาศเต็มได้ที่: whitehouse.gov

5. แผนการพัฒนามาตรฐาน AI ระดับสากล (A Plan for Global Engagement on AI Standards):

พัฒนาโดย NIST เพื่อส่งเสริมการพัฒนามาตรฐาน AI ระดับโลกและการประสานงานเพื่อการแบ่งปันข้อมูลและความร่วมมือในการพัฒนามาตรฐานด้าน AI อ่านแผนฉบับเต็มได้ที่: nvlpubs.nist.gov https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-5.pdf

6. แนวทางการรักษาความปลอดภัยระบบ AI ของสิงคโปร์:

สำนักงานความมั่นคงทางไซเบอร์ของสิงคโปร์ (Cyber Security Agency: CSA) ได้ประกาศแนวทางในการรักษาความปลอดภัยระบบ AI เพื่อช่วยให้องค์กรลดความเสี่ยงที่อาจเกิดขึ้นในการพัฒนาและใช้งานระบบ AI โดยเน้นการออกแบบที่ปลอดภัยและการรักษาความปลอดภัยตามค่าเริ่มต้น รายละเอียดเพิ่มเติมได้ที่:

https://thaipublica.org/2024/10/asean-weekly-roundup-272/

7. มูลนิธิตรวจสอบปัญญาประดิษฐ์ (AI Verify Foundation) ของสิงคโปร์:

สิงคโปร์ได้ก่อตั้งมูลนิธิตรวจสอบปัญญาประดิษฐ์เพื่อสนับสนุนชุมชนโอเพนซอร์ซทั่วโลกในการพัฒนาเครื่องมือทดลอง AI และส่งเสริมการใช้ AI อย่างมีความรับผิดชอบ

https://www.prd.go.th/.../category/detail/id/2124/iid/188700

แนวทางและมาตรฐานเหล่านี้ให้ข้อมูลพื้นฐานสำหรับองค์กรที่ต้องการนำ AI มาใช้อย่างปลอดภัย พร้อมการจัดการความเสี่ยงและการป้องกันภัยคุกคามที่อาจเกิดขึ้น