นาย พรพรหม ประภากิตติกุล
ผู้บริหารความมั่นคงปลอดภัยสารสนเทศ
/ผู้เชี่ยวชาญด้าน Cybersecurity

ThaiCERT ETDA สพธอ

อีเมล :
PORNPROM@ETDA.OR.TH
PORNPROM@THAICERT.OR.TH

เบอร์โทร :
02-123-1212.
02-123-1234

ADTE by ETDA

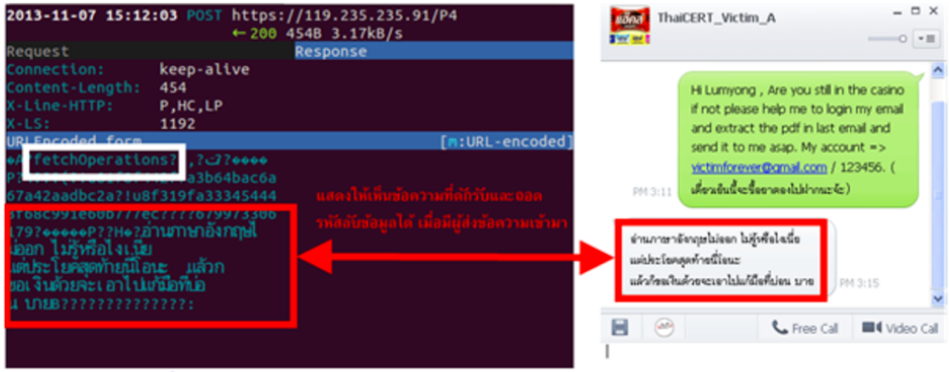
ADTE Virtual Opening Day
MAY 12, 2021

Register here

About me

Skills & Experience
(Cybersecurity)

- เจาะเข้าถึงบทสนทนาที่อยู่ในเครือข่ายเดียวกับผู้ใช้งานได้ทันที
- แจ้งเตือนกับบริษัทผู้พัฒนา เพื่อให้ปรับปรุงความปลอดภัยของซอฟต์แวร์



โปรแกรมที่ใช้ในการดักรับและถอดรหัสข้อมูล

LINE

10 ปีในหน่วยงาน **ไทยเซิร์ต (ThaiCERT)**

- **ThaiCERT Government Monitoring System**
- Incident Handling (**การรับมือภัยคุกคามไซเบอร์**) กรณีสำคัญ
- Malware Analysis (**การวิเคราะห์มัลแวร์**)
- Penetration Testing (**การตรวจประเมินช่องโหว่ระบบสารสนเทศ**)
- Digital Forensics (**การตรวจพิสูจน์พยานหลักฐานทางดิจิทัล**)
- Web Application Security (**การรักษาความมั่นคงปลอดภัยของเว็บไซต์**)
- Risk Management (**การบริหารจัดการความเสี่ยงระบบสารสนเทศ**)
- Cybersecurity Trainning and Exercise (**การอบรมหลักสูตรด้านสารสนเทศ**)
- Secure Coding (**การพัฒนาโปรแกรมอย่างปลอดภัย**)

ETDA Cybersecurity (ThaiCERT)

Scope & mission

ThaiCERT has been the first non-profit CSIRT in Thailand (established since 2000)

Incident Response

- Monitor and Coordinate Cybersecurity Incidents
- Provide Essential and Technical Support to victims
- Research and Develop Tools and Guidelines

Among more than 300 CERT(s), there are more than 50 natioal-CERTs

"ThaiCERT provides an official point of contact for dealing with computer security incidents in Thai Internet community"

*First team outside Europe to be TI Accredited

Incident Monitoring 24x7

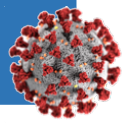
- Cooperate with Thai CIIs, Public & Private Companies and overseas (~300 CERTs around the world)

What is about the topic today

Word by word

ธุรกิจจะมีความมั่นคงปลอดภัยในการให้บริการได้อย่างไร เมื่อต้องใช้ E-Platform

การให้**บริการธุรกิจ**ที่**ต้องการความอยู่รอด**ในภาวะ COVID-19 แพร่ระบาด



จึงต้อง

นำ E-Platform มาใช้ในการให้บริการธุรกิจ

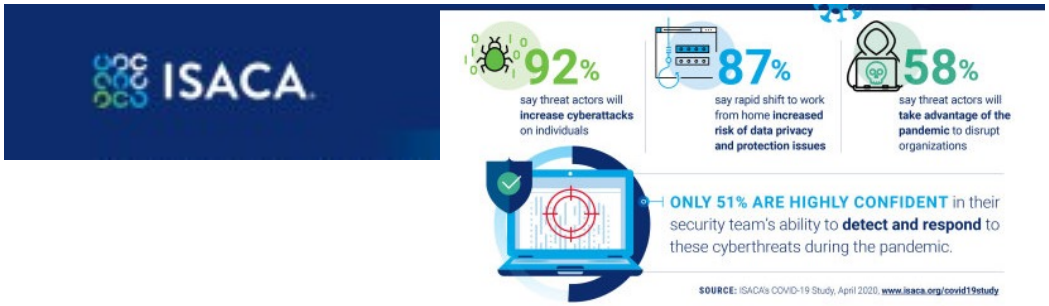
ฉะนั้น

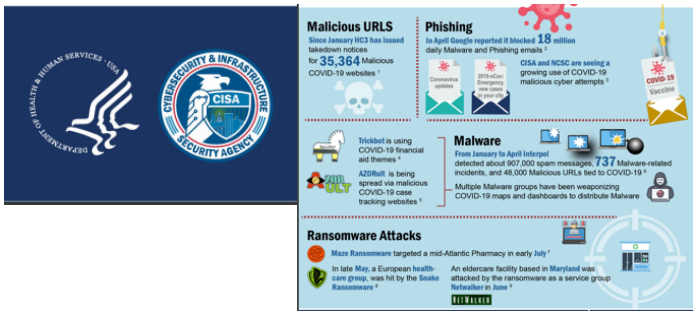
การ**ทำให้ E-Platform มีความมั่นคงปลอดภัย**คือ**กุญแจ**สำคัญไม่แพ้การวางกลยุทธ์ทางการตลาด

เพื่อ...

ทำให้ธุรกิจน่าเชื่อถือและ**รอรับทรัพย์**(อย่าลืมเข้าใจลูกค้าวางแผนธุรกิจด้วย)

Some global statistics for cybersecurity issues during COVID-19 pandemic





What are new normal E-Platform

Some technologies/services are being used or repurposed for new normal

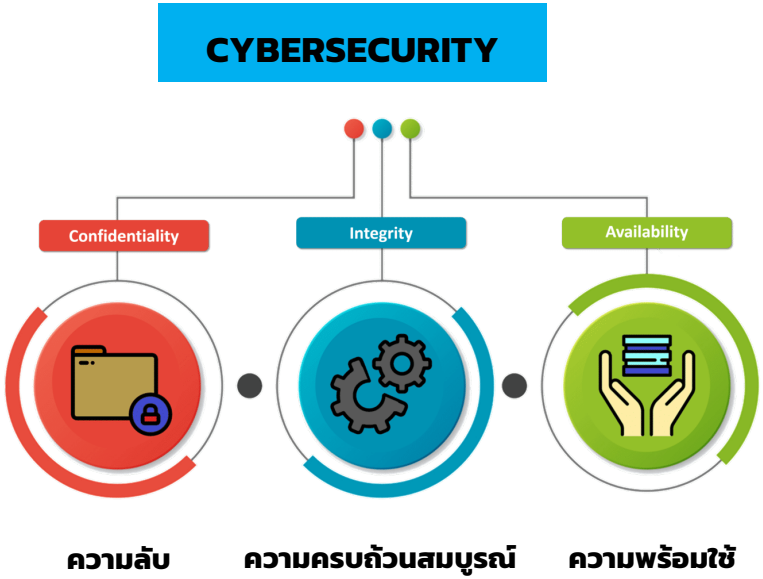
- Thermal cameras detecting elevated temperatures
- Audio sensors detecting coughs
- Video conference / Webinar / Live online concert
- Contactless technology (e.g. online payment)
- Electronic documentation (e-licensing)
- Telemedicine
- Smart home / Smart city (IoTs)
- Automation system (Artificial intelligence)

Cybersecurity

Example. for what and How

- ISO 27032 defines “Cybersecurity” as the **“preservation of confidentiality, integrity and availability of information in the Cyberspace”**

  - “Cyberspace” as “the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it.



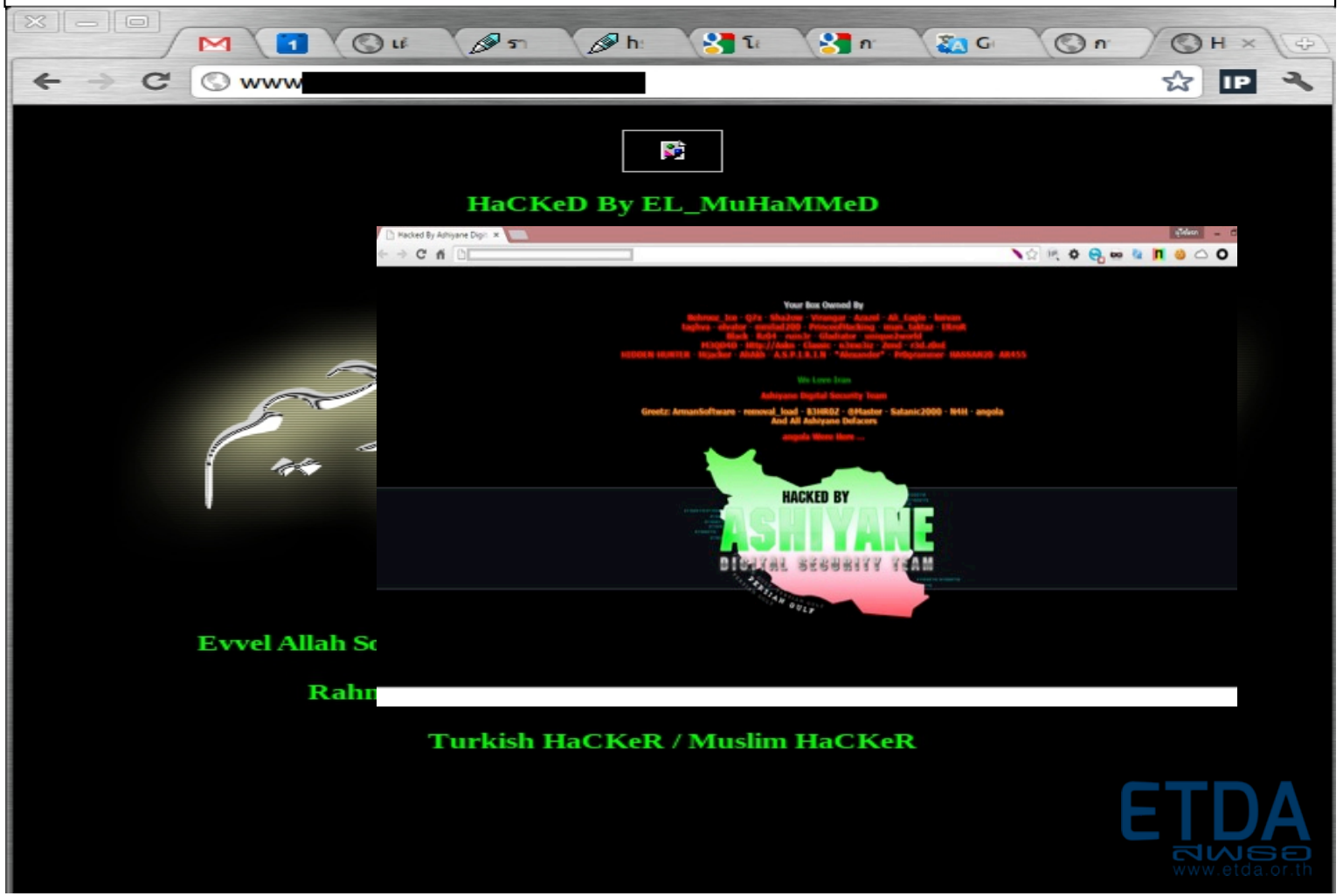
Confidentiality

Soft wrap | Raw text | Duplicate

```
[redacted]/viewnews.php?id=61


web server operating system: Linux
web application technology: Apache 2.2.15, PHP 5.2.17
back-end DBMS: MySQL 5.0.11


available databases [2]:
[*] information_schema
[*] [redacted]


Database: [redacted]
[100 tables]
+--------------------------------------+
| admin                                |
| admin_authen                         |
| answer
| authen
| badword
| busline
| busline_bustype
| busline_station
| bustype
| bustypegroup
| cart_sell
| contactus
| contactus280410
| customer
| customer_log
| expenses
| faq
| faq_category
```

```
Database: portal
Table: admin
[1 entry]
+------------+----------+----------+
| password   | username | validity |
+------------+----------+----------+
| qwert12345 | admin    | 0        |
+------------+----------+----------+
```

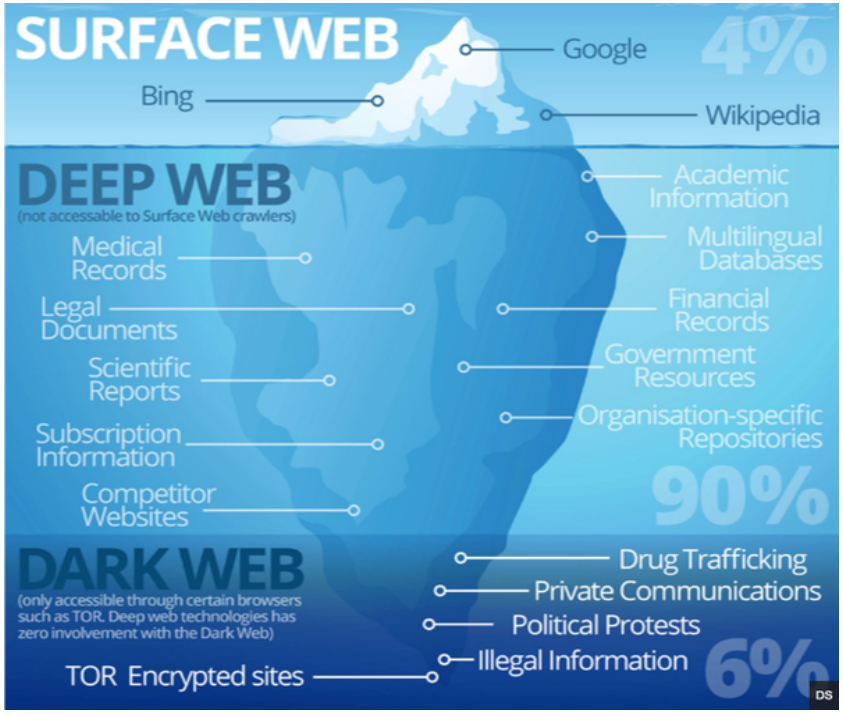
Integrity


HaCKeD By EL_MuHaMMeD
HACKED BY
ASHIYANE
DIGITAL SECURITY TEAM
Turkish HaCKeR / Muslim HaCKeR

Availability

Real internet

Different levels of internet access with various purposes and risks



Sites which can be found with the traditional search engine

Sites which can not be searched by search engines - Including intranet websites

Sites which require special browsers to view - Often associate with criminal activity

http://www.skyindya.com/wp-content/uploads/2017/01/surface-web-vs-deep-web-vs-dark-web-2.png

[WEF] Most worrisome risks

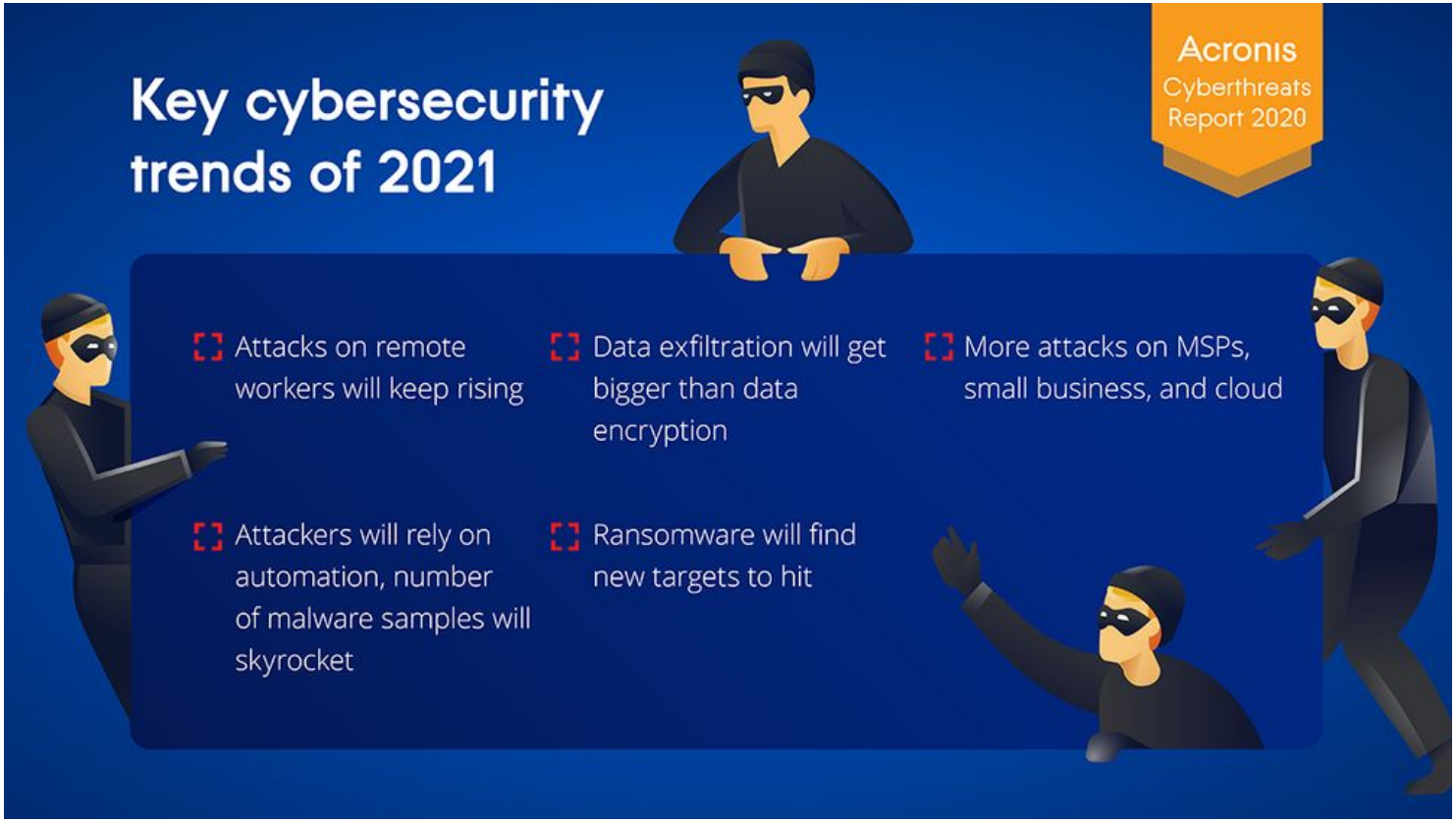
For your company

*** Cyberattacks and data fraud rank third among the greatest COVID-related business concerns.***

COVID-19 Risks Outlook A Preliminary Mapping and Its Implications

[Acronis] Key issues

Cybersecurity trends 2021



The Importance of Cybersecurity in Business

Why and How

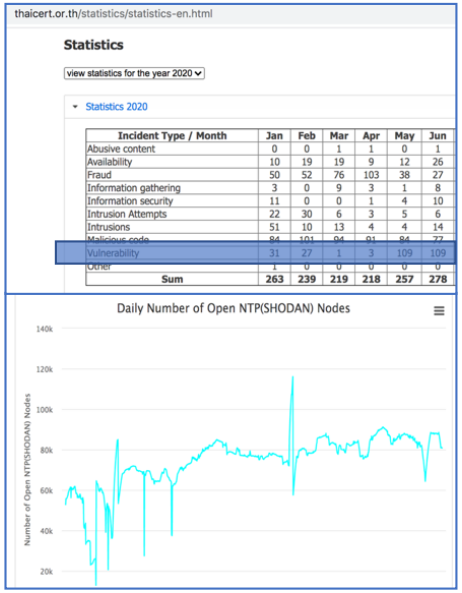
- Cybersecurity is an important measure to **ensure smooth business operations and to maintain reputation**. It also involves increasing opportunities for creating more customers.
- In the case of failing in cybersecurity, **businesses may collapse**.
  - **Phishing** can cause a lot of damage to your business like BEC.
  - **Social engineering** can launch together with advance hacking to find the critical vulnerabilities in an organization.
  - **Malware** is used as a common technique in data breach or hacking situations
- The **COVID-19 pandemic** has raised the stakes, **increasing cyber risk in every Sector** in proportion to the increased pace of activity amid widespread transition to **remote work environments**

Observed cybersecurity issues in 2020

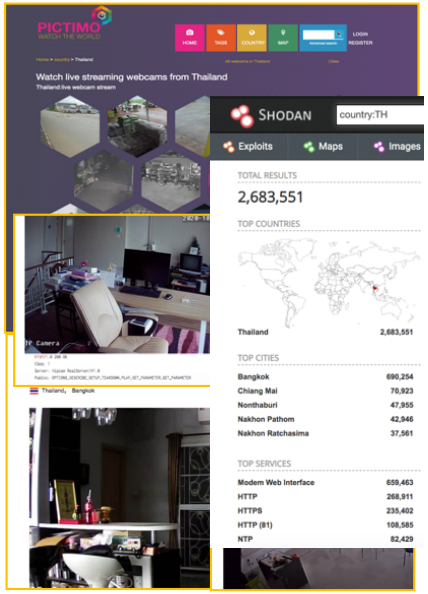
New technologies with new threats

Thailand (by ETDA/ThaiCERT)

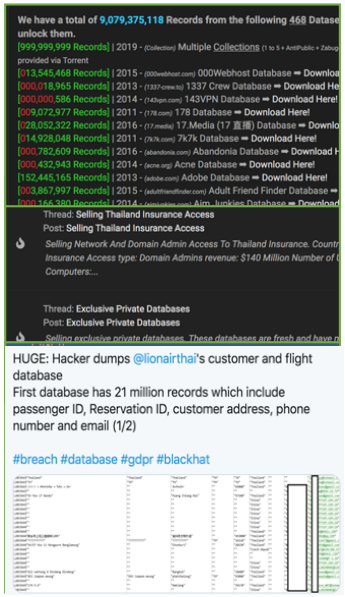
Increasing of vulnerability report



A lot of [vulnerable] IOT devices



Data breach is a new normal

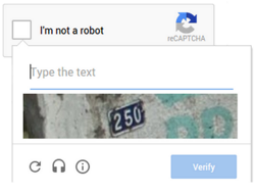


HUGE: Hacker dumps @lionairthai's customer and flight database
First database has 21 million records which include passenger ID, Reservation ID, customer address, phone number and email (1/2)

#breach #database #gdpr #blackhat

Global

AI as weaponizations



Google's reCaptcha service has been cracked by a group of University of Maryland researchers who devised an automated attack that can break the service with 85 percent accuracy.

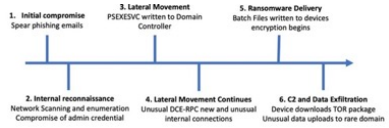
The researchers created a tool called unCaptcha that is able to abuse the audio challenge option of Google's reCaptcha V2 service.

Ref : threatpost.com

AI as security solutions

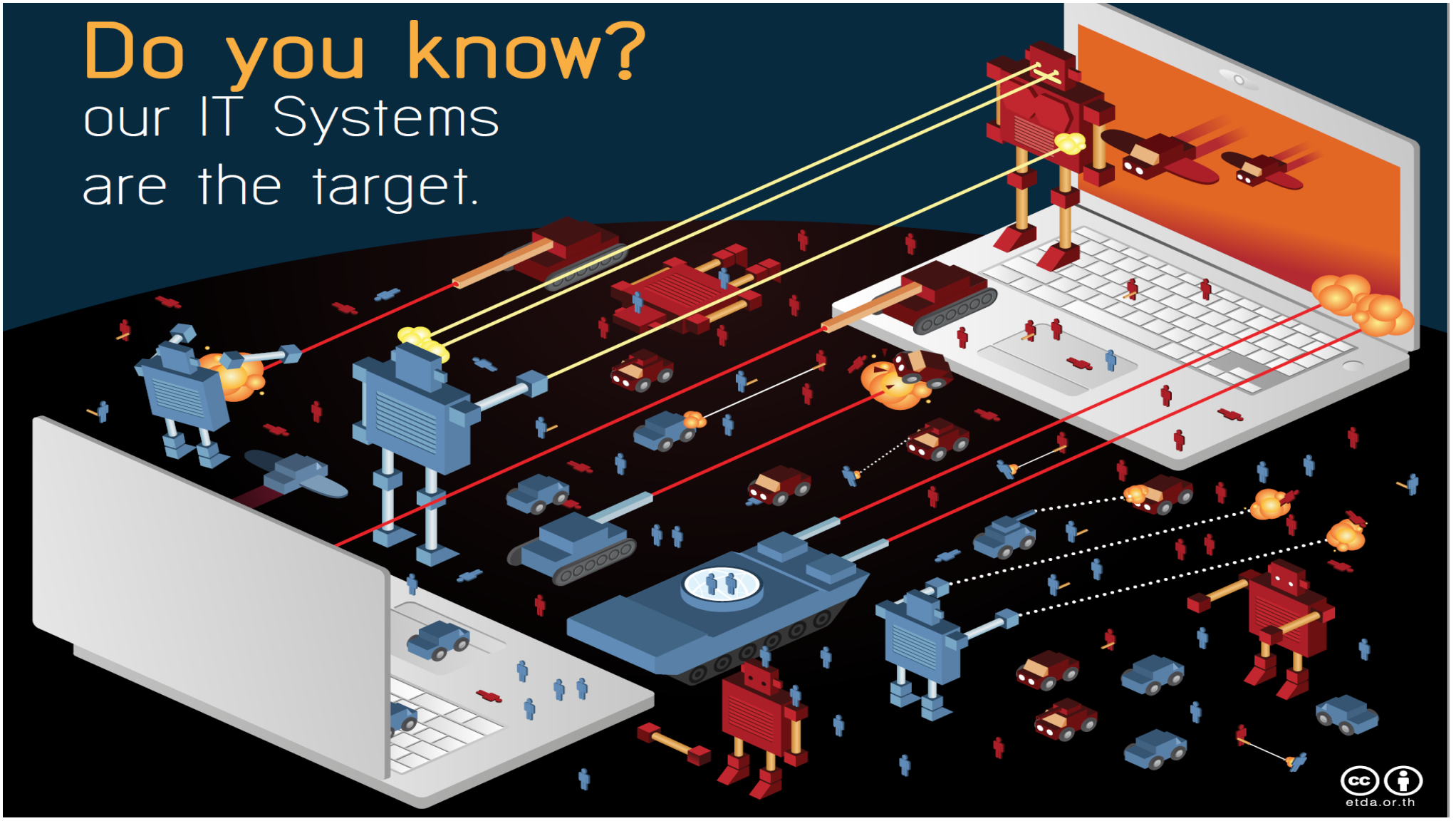
DARKTRACE

AI catches Maze ransomware



Ref : darktrace.com

SO


Do you know?
our IT Systems
are the target.
etda.or.th

Source : http://www.greenpest.com.au/ec2c-internal-monitors-termite-windows/

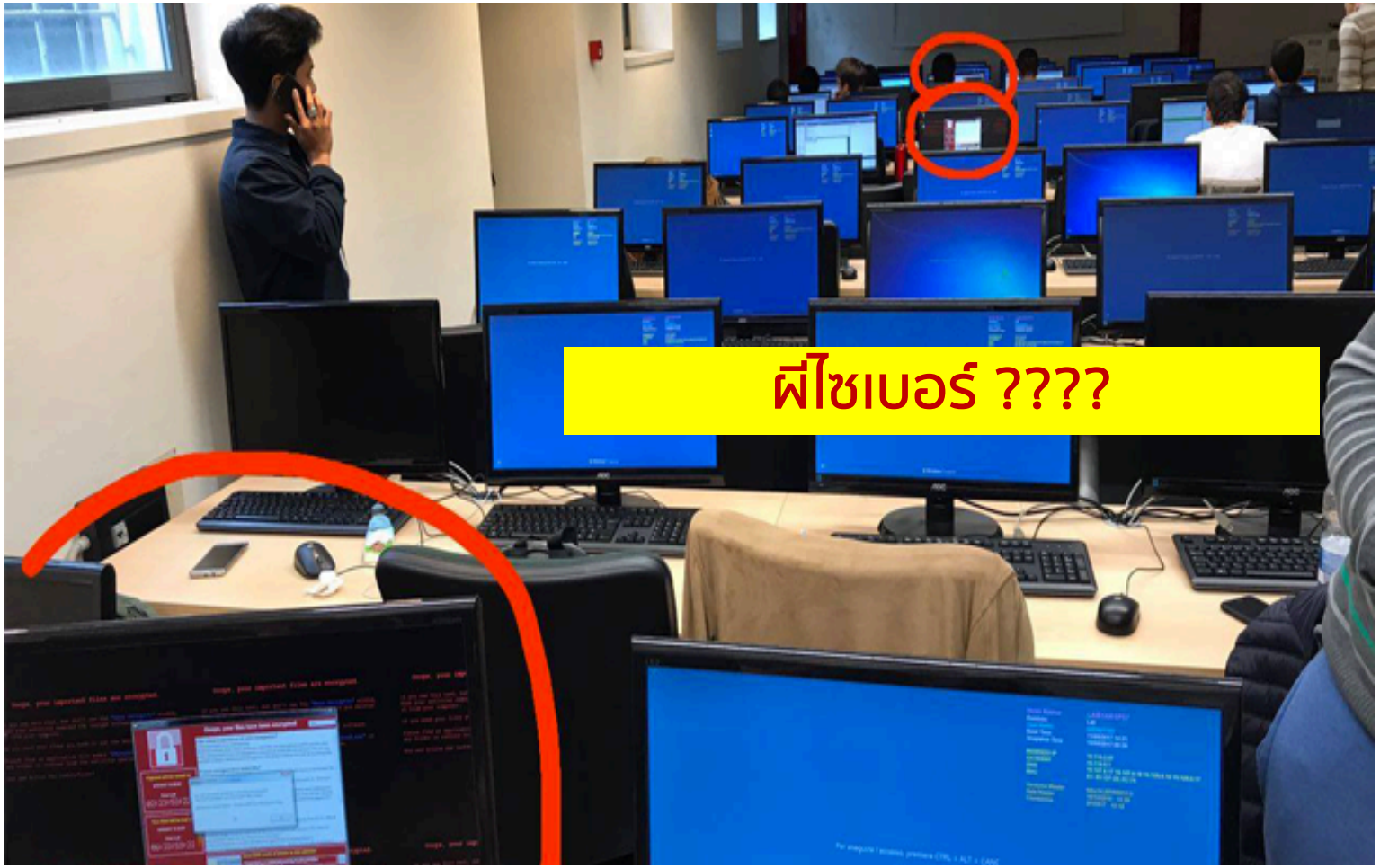
บ้านที่ขาดการดูแลรักษา ย่อมมีโอกาสให้เกิดการบุกรุกจากสิ่งแปลกปลอมภายนอกได้ง่าย ยิ่งปล่อยไว้นานความเสียหายย่อมเกิดขึ้นอย่างต่อเนื่องและทวีความรุนแรงมากขึ้นเรื่อยๆ


Hacker ก็เหมือน...ปลวก
เดินกระซวกทุกที่ ที่มีช่องโหว่
Source : http://www.essentialpest.com/termite-damage/

Hacker ก็เหมือน...ผี

รู้ว่ามี แต่ไม่เคยเห็น

Source : http://shock.mthai.com/wp-content/uploads/2015/12/ผีในจังหวัดชลบุรี.jpg


ผีไซเบอร์ ????

THEN

Cybersecurity is everybody's business

List of concerns

ประชาชน/พนักงาน

- รหัสผ่าน/การใช้งานที่มีความเสี่ยง
- ใช้บริการระบบ E-Platform (ความเสี่ยง โดนหลอกกรอกข้อมูลส่วนบุคคล)
- รู้ว่าต้องทำอย่างไรเมื่อเกิดเหตุกับตัวเอง

องค์กร/บริษัท

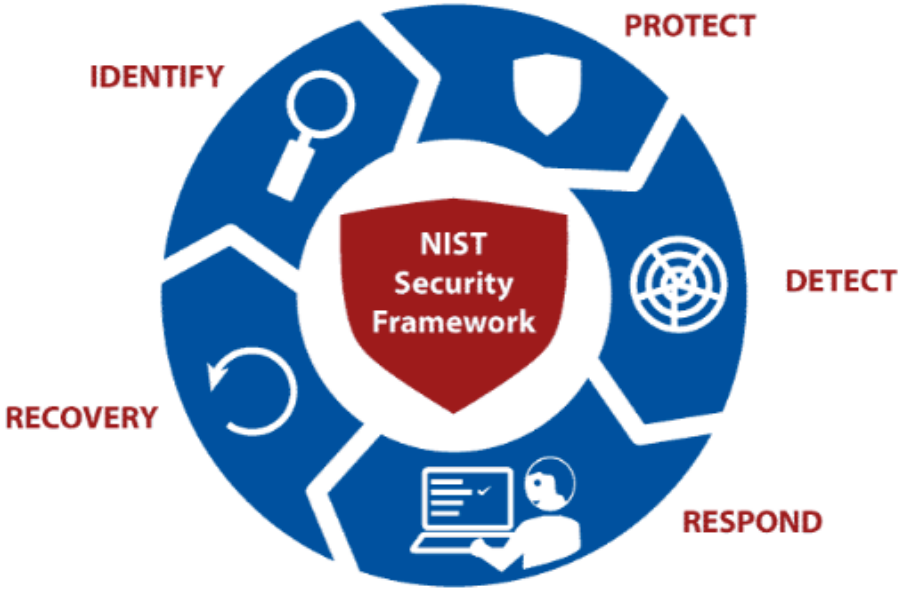
- ระบบสำคัญไม่ได้รับการดูแลที่ดีและเข้าใจ
- จัดเก็บข้อมูลบริษัท/ลูกค้า (ความเสี่ยง ข้อมูลถูกขโมย เสียความน่าเชื่อถือ)
- การทำให้สอดคล้องตามมาตรฐาน/กฎหมาย

ประเทศ

- โครงสร้างพื้นฐานด้านสารสนเทศที่สำคัญเป็นเป้าหมาย
- การประเมินผลกระทบ/ความเสี่ยง (ความเสี่ยง ส่งผลต่อความเป็นอยู่ของประชาชน)
- กลไกการควบคุมดูแล/มาตรฐานขั้นต่ำ

Why don’t you follow a best practice

Even that, no one can guarantee 100% safe



Ref : NIST SP800-53 Cybersecurity Framework

Identify :
- Risk assessment
- Inventory of assets

Protect :
- Measures
- Firewall policy

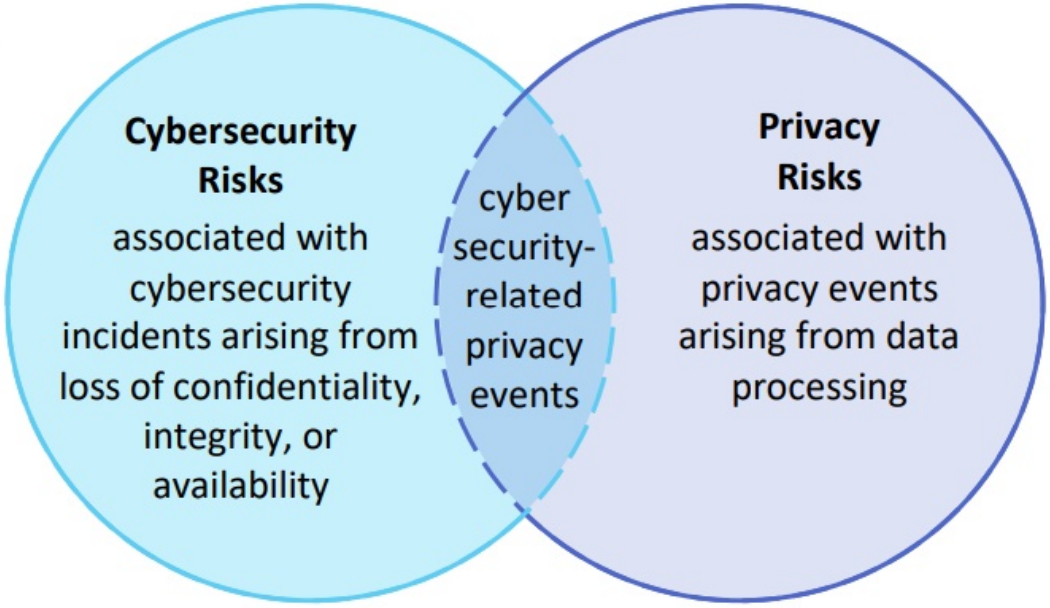
Detect :
- SOC
- IDS
- Threat hunting
- VA/PT

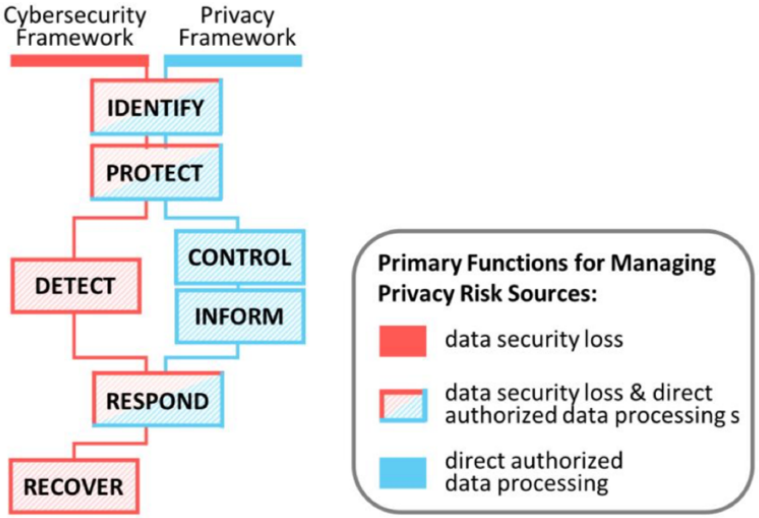
Respond :
- Incident handling **

Recovery :
- Recovery plan
- Backup / Restore procedure

Beware of conflict in Cybersecurity and Privacy risks

Relationship





Ref : NIST Privacy Framework

Key takeaway

Don’t worry but be ready for cybersecurity issues

- Cybersecurity is an important measure to **ensure smooth business operations and to maintain reputation**. It also involves increasing opportunities for creating more trust with stakeholder
- There are **a lot of threats and cybersecurity challenges** nowadays, new malwares and new vulnerabilities coming every second, with or without targeting
- You may start to follow best practices and cybersecurity frameworks to **ensure that appropriate measures are taken**

Key takeaway (cont.)

Don’t worry but be ready for cybersecurity issues

- Some **publications** are useful for your organizations
  - **Establishing a Computer Security Incident Response Team** by ThaiCERT (https://www.thaicert.or.th/downloads/files/Establishing_a_CSIRT_th.pdf)
  - Cybersecurity checklist with **Cyberplanner** (https://www.fcc.gov/cyberplanner)
  - **Cybersecurity for small business** (https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity)

#Cybersecurity ชั่วโมงเดียวคงไม่พอ
รอตามกันต่อที่ #ADTE ครับ

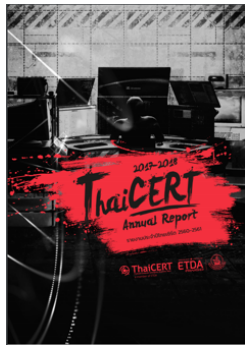
ADTE by ETDA

Register here

ADTE Virtual Opening Day
MAY 12, 2021

ETDA สพธอ

Cyber security publication



And More ...

www.etda.or.th / www.thaicert.or.th

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

ETDA
สพธอ
www.etda.or.th

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
Ministry of Digital Economy and Society

Telephone:	+66-2-123-1212
Report Incident:	report@thaicert.or.th
General Inquiry:	office@thaicert.or.th
Follow the news:	www.facebook.com/thaicert
	www.twitter.com/thaicert

Thailand Computer Emergency Response Team (ThaiCERT)
Electronic Transactions Development Agency

ETDA สพธอ