RBIA Challenge and Cybersecurity Risk Assurance

AGUSTINUS NICHOLAS TOBING,

Agenda

1. RBIA & Cybersecurity – Skeptical Approach
2. Cybersecurity – Definition, Type, Target and Counter Measures
2. Cybersecurity – Best Practices
3. Data Protection vs Data Privacy
4. What is a Data Breach?
5. Personal Identified Information (PII)
6. COVID-19: Medical Data Breach
7. Sample of Global Data Breach
8. Key Challenges in this pandemic.
9. What's Next?
10. Top Cyber Safety Tips

RBIA – Skeptical Approach

Bagaimana pandangan Anda mengenai kualitas dari Laporan Profil Risiko yang disampaikan oleh Unit Kerja Manajemen Risiko/oleh Unit Kerja?

Tantangan yang anda hadapi dalam penerapan audit berbasis risiko?

- Kualitas dari Laporan Profil Risiko: “Save As”
- Siapa yang mengisi atau *update* profil risiko? Sekretaris atau Risk Champions?
- Mekanisme *update* atas Laporan Profil Risiko: No Update
- *Cross Check* dengan hasil assurance dari internal dan external.
- Alignment: *Mapping* dari RBIA ke Rencana Strategic Perusahaan.

RBIA – Skeptical Approach

Menurut pendapat anda, bagaimana auditor mengandalkan RBIA untuk mencapai efektivitas pelaksanaan penugasan assurance?

Apakah Direksi/Dewan Komisaris/Komite Audit memberikan masukan atas laporan profil risiko yang harus ditindaklanjuti di dalam penugasan RBIA?

- Validasi dengan AC, Risk, Compliance dan BoD
- *Benchmark* dengan peers CAE
- Pemahaman atas Risiko pada level BoD, AC, dan BoC: *Annual Refreshment* oleh Line 2 terait top risk dan top issues.

Cybersecurity – Skeptical Approach

Apakah organisasi anda telah melakukan asesmen atas *cybersecurity*?
Apakah Unit Kerja Audit Internal di organisasi Anda memilik sumber daya yang memadai (keterampilan, pengalaman, dan kapasitas) untuk melakukan cybersecurity assurance)?

Apakah unit kerja Audit Internal di organisasi anda melakukan *assurance* atas *cybersecurity* di tahun 2018 dan/atau tahun 2019?

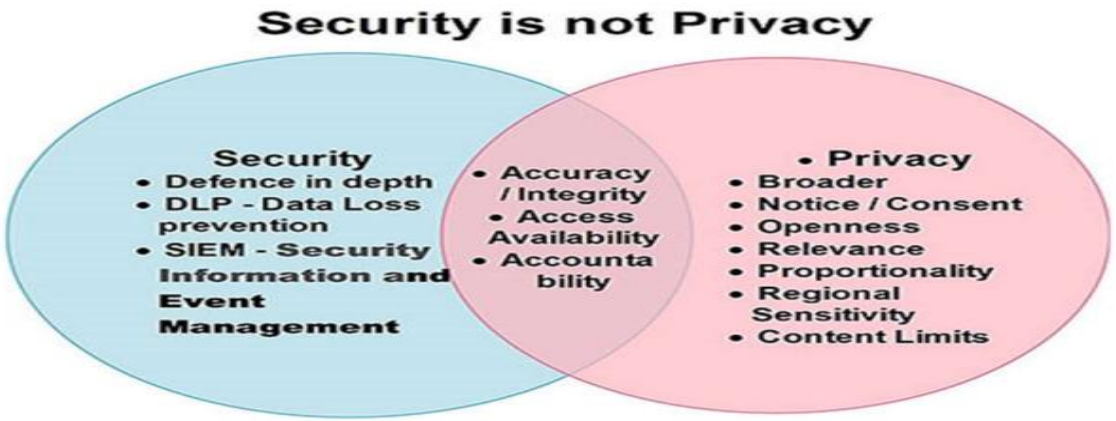
Sejauh mana organisasi anda menggunakan penyedia jasa eksternal untuk *cybersecurity assurance*?

Mengapa asurans atas *cybersecurity* tidak dilakukan?

- Pemahaman atas *definition*, *type* dan *countermeasures* dari *Cybersecurity*
- *Best Practices* dari *Cybersecurity*
- Data Protection, Data Security dan Data Privacy
- *Key Challenges in this Pandemic*

Cybersecurity: - Definition, Type, Target and The Counter Measures

Also referred to as **Information Security**, **Cyber Security (CS)** refers to the **practice of ensuring** the **Confidentiality**, **Integrity**, and **Availability (CIA)** of information. Cyber Security is comprised of an evolving **set of tools**, **risk management approaches**, **technologies**, **training**, and **best practices** designed to protect networks, devices, programs, and data from attacks or unauthorized access



The world of cybersecurity

Threats

- Identity theft
- Information manipulation (e.g. Malware)
- Cyber Assaults/Bullying
- Advanced Persistent Threats (APTs)
- Information theft
- Crime (e.g., Credit card fraud)
- Insider
- Espionage
- Cyber attack
- Transnational
- Attack of software "boomerangs"
- Terrorism

Targets

- Government (Federal, State, and Local); e.g.,
  - E-Government
  - E-Commerce
- Industry; e.g.,
  - Aerospace & Defense
  - Banking & finance
  - Health care
  - Insurance
  - Manufacturing
  - Oil & Gas
  - Power Grid
  - Retail
  - Telecommunications
  - Utilities
- Universities/Colleges
- Individuals

Counters

- Cyber workforce
- Advanced network and resilience controls
- Outbound traffic monitoring
- Dynamic situational awareness
- Open source Information
- Risk intelligence & management
  - Forensic analysis
  - Data analytics
- Financial intelligence (FININT)
- Tighter laws & enforcement
- Expanded diplomacy
- Legislation?

You should assume that your information network has been or will be compromised.

Copyright © 2013 Deloitte Development LLC. All rights reserved

Cybersecurity – Best Practices

- **Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.
- **Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.
- **Information security** protects the integrity and privacy of data, both in storage and in transit.
- **Operational security** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.
- **Disaster recovery and business continuity** define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.
- **End-user education** addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug-in unidentified USB drives, and various other important lessons is vital for the security of any organization.

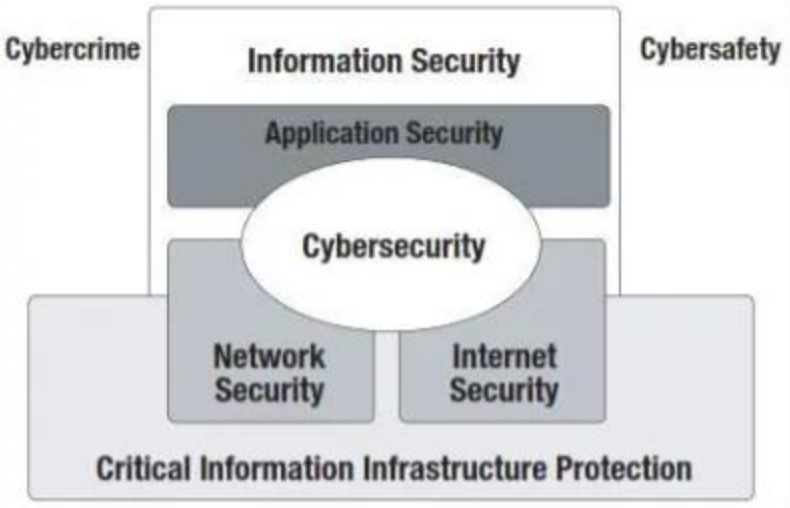


Diagram hubungan antar domain security (sumber: ISO 27032:2012: *Information Technology–Security Techniques–Guidlines for cybersecurity*)

Campaign Targets:

- Starting 8/12, Akamai customers began receiving DDoS extortion letters to prevent impending volumetric attacks
- Campaign initially targeted financial services institutions & some ecommerce, but has more recently shifted to extort other industries including gaming, gambling, high tech and travel & hospitality

Threat Actors:

- One group claims to represent Russian sponsored **Fancy Bear (APT 28)** and another the **Armada Collective**
- Attackers are requesting payment of 10 Bitcoin (~120k) and 20 Bitcoin (~240k) respectively, and increasing the extortion demands if payment deadlines are missed

"If you report this to media and try to get some free publicity by using our name, instead of paying, attack will start permanently and will last for a long time. (sic)"

- Armada Collective

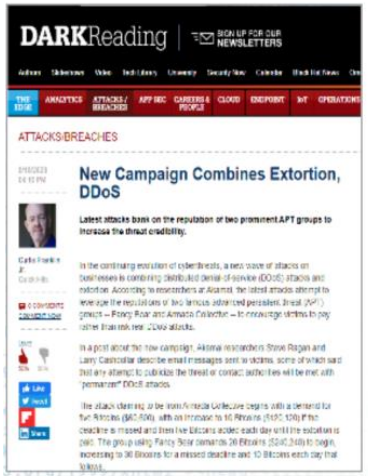
"...your websites and other connected services will be unavailable for everyone. Please also note that this will severely damage your reputation among your customers. [...] We will completely destroy your reputation and make sure your services will remain offline until you pay. (sic)"

- Fancy Bear

Excerpts of extortion emails from attackers claiming to be Fancy Bear and Armada Collective

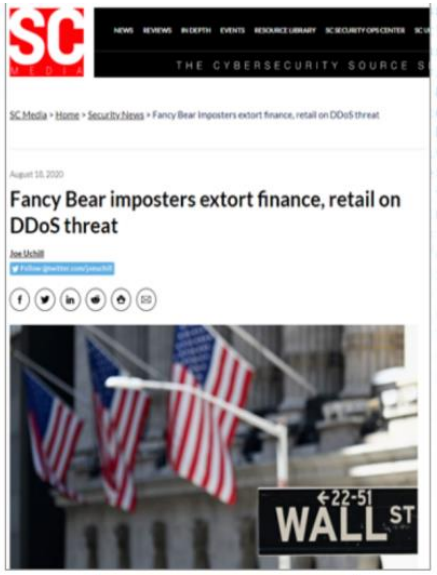
Media Coverage

DARKReading



BANKinfo Security

Security Week



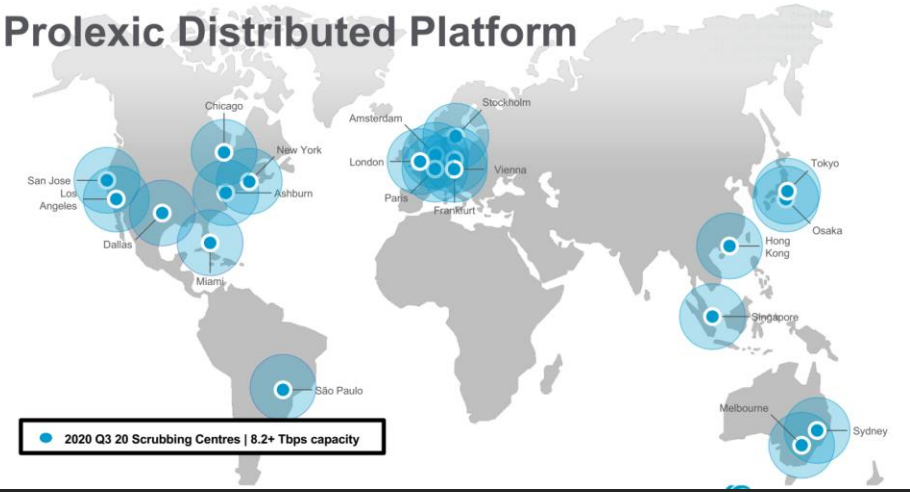
SC magazine

"These are defendable attacks," says Ragan, especially if providers know to look for the initial flood of UDP packets.

You Fancy, huh? **Cyber Scoop Newsletter**

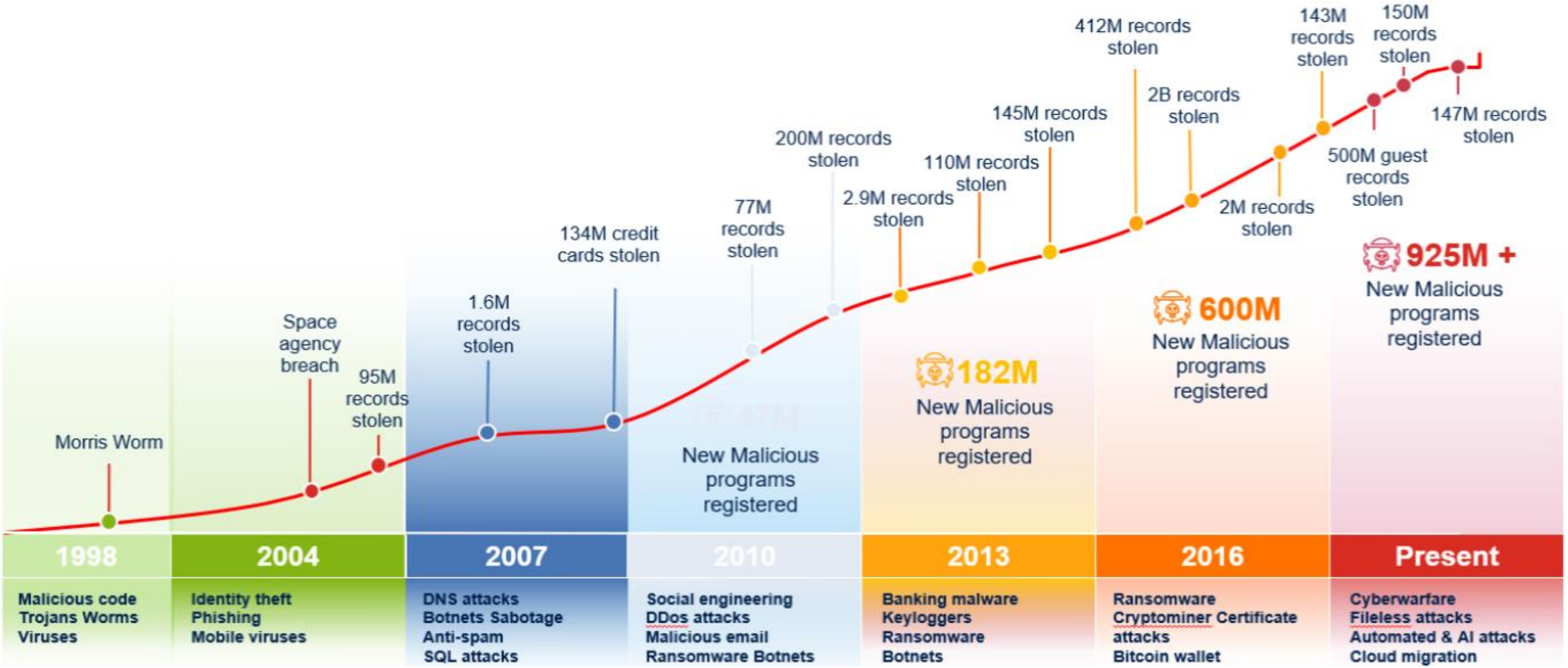
Security firm Akamai says a group of hackers posing as Fancy Bear, the infamous Russian intelligence outfit, have used distributed denial-of-service attacks to try extorting companies in multiple industries over the last week. The attacks tend to start with an email threatening the company with an impending DDoS attack that can only be prevented by paying a ransom of more than $240,000. If the victims doesn't pay, scammers threatened to increase the demand to $365,000. Akamai doesn't recommend paying the fee. **Read it here.**

Prolexic Distributed Platform

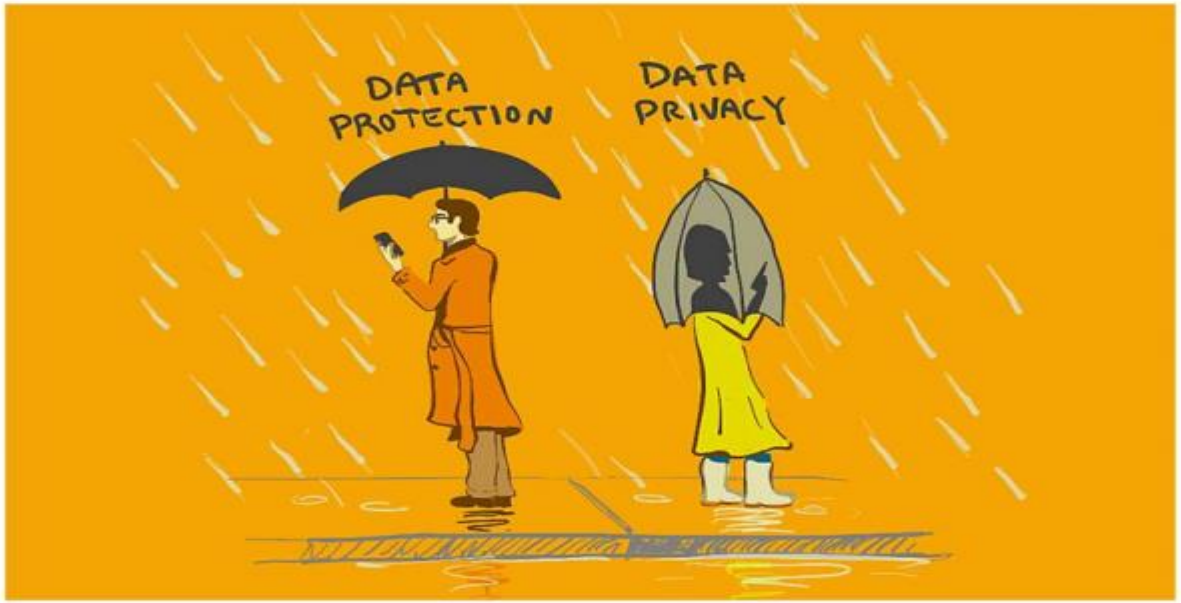


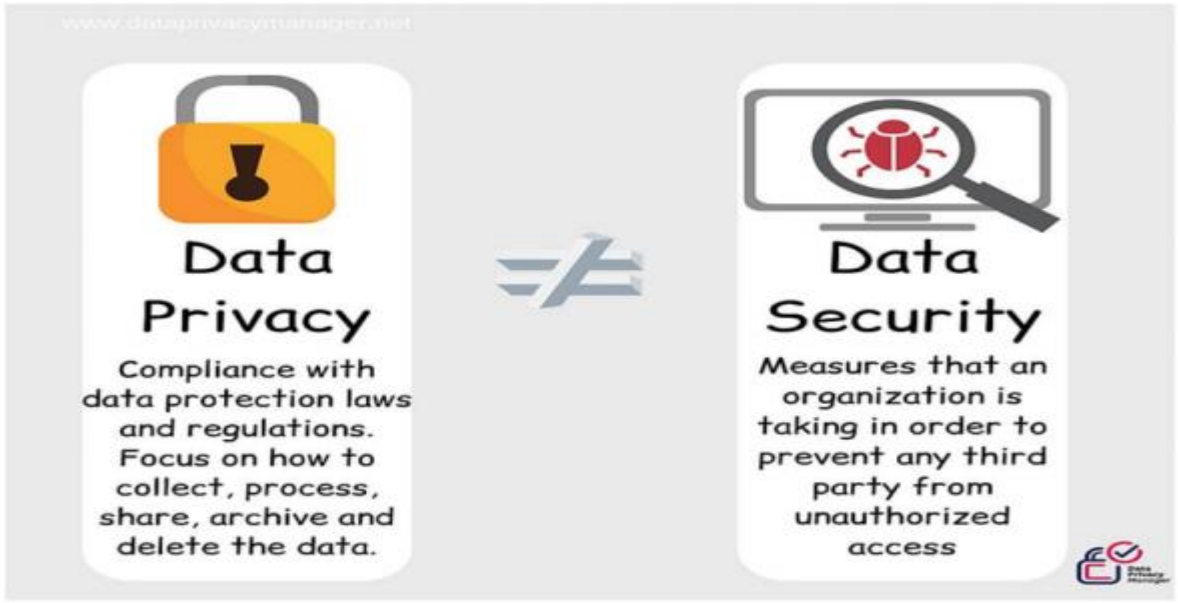
- Cybercriminals leveraging multiple attack vectors
- Targets focusing on overwhelming DNS, Web Application & Network/Data Centre Infrastructure
- Exhibited ability to pivot/morph to bypass controls
- Multi-Vector DDoS Attack Techniques

It’s changing so fast…



Data Protection vs Data Privacy

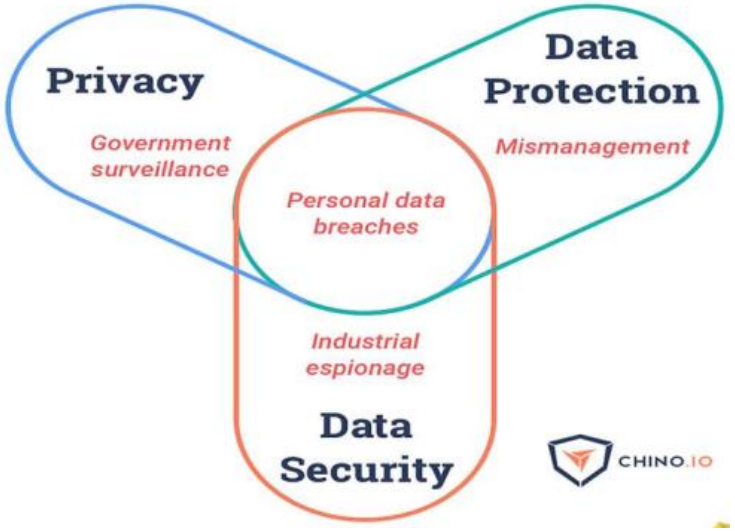




Data privacy is a part of data security and is related to the proper handling of data – how you collect it, how you use it, and maintaining compliance.

Data security is about access and protecting data from unauthorized users through different forms of encryption, key management, and authentication.

What is a Data Breach?



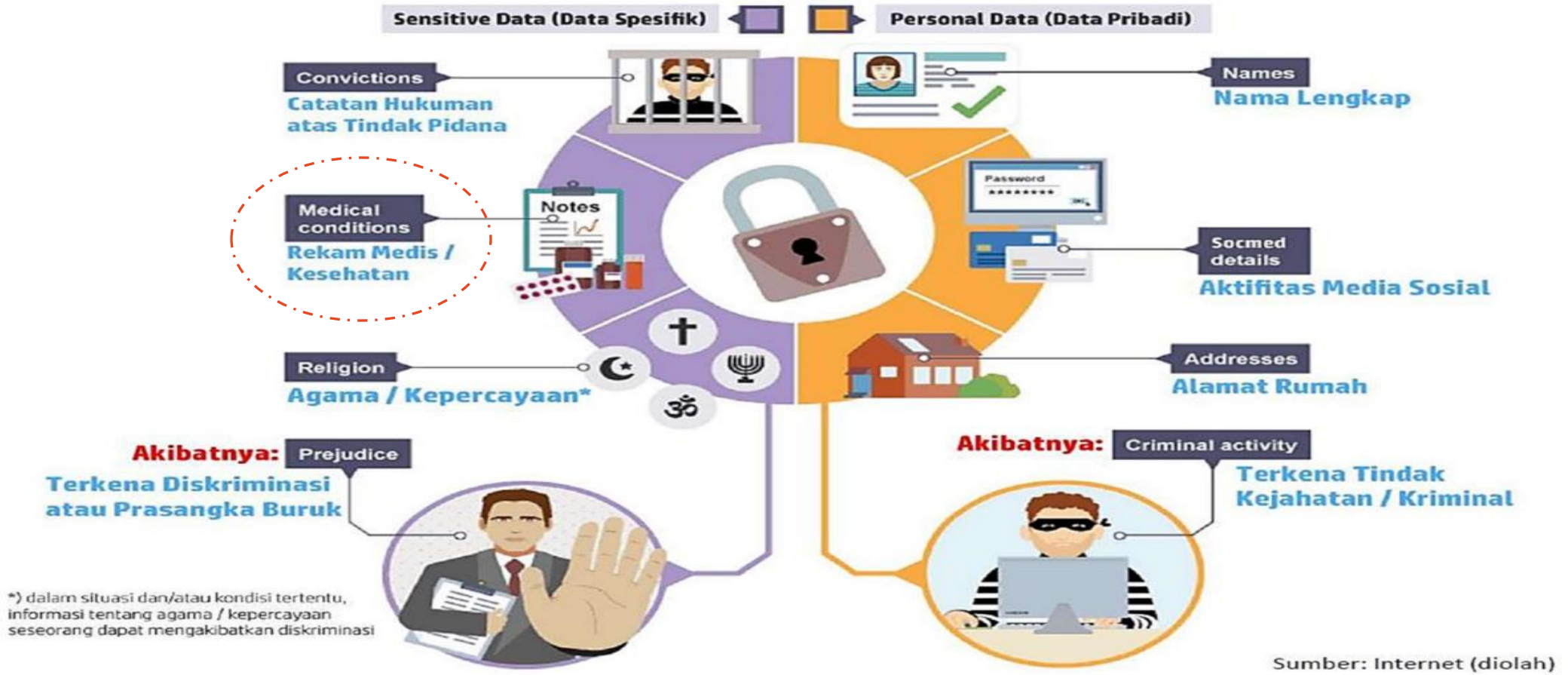
"Data pribadi adalah setiap **data tentang kehidupan** seseorang baik yang teridentifikasi dan / atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan / atau non elektronik".

"Privasi adalah hak individu untuk menentukan apakah data pribadi akan dikomunikasikan atau tidakkepada pihak lain."

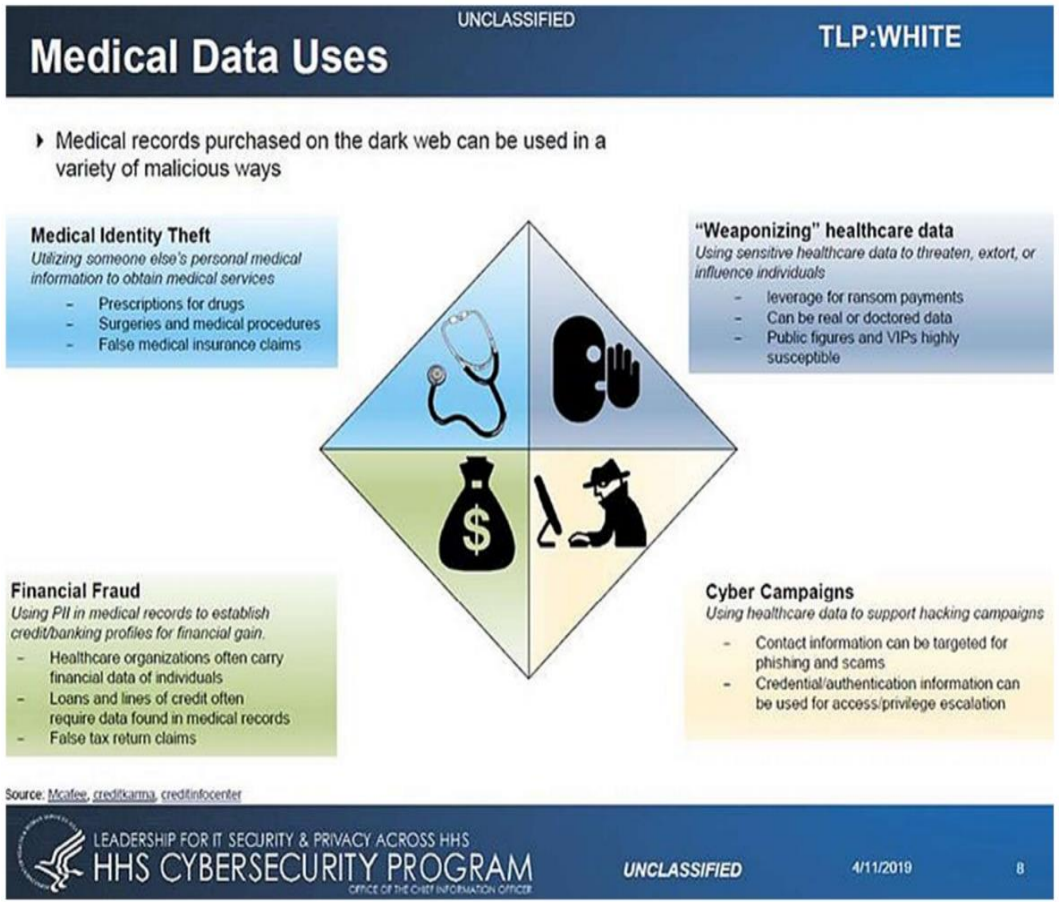
**Draft RUU PDP*

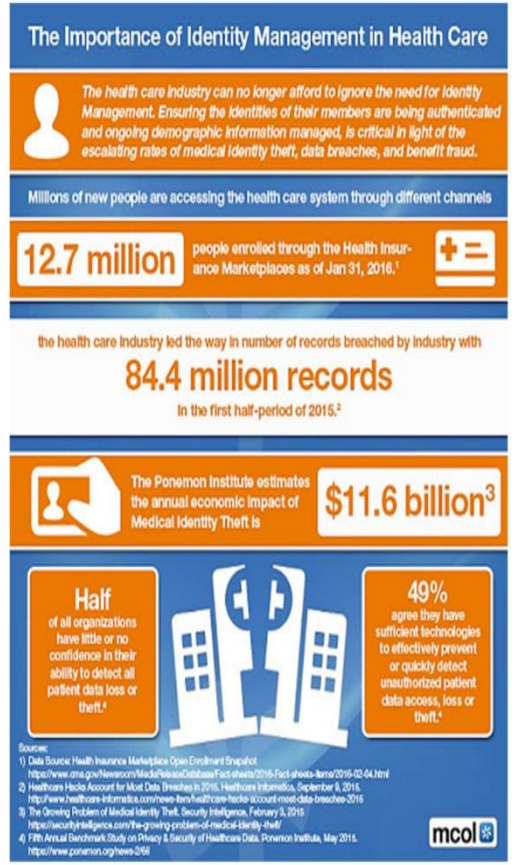
Data Privacy is PII and subject of **Data Protection. Data security** is about protecting any type of data from unauthorized access. **Data protection** is about protecting personal data from both access and misuse. **Data protection can only be achieved with good data security**. However, it also needs organizational measures, like privacy policies and consent management.

Personal Identified Information (PII)

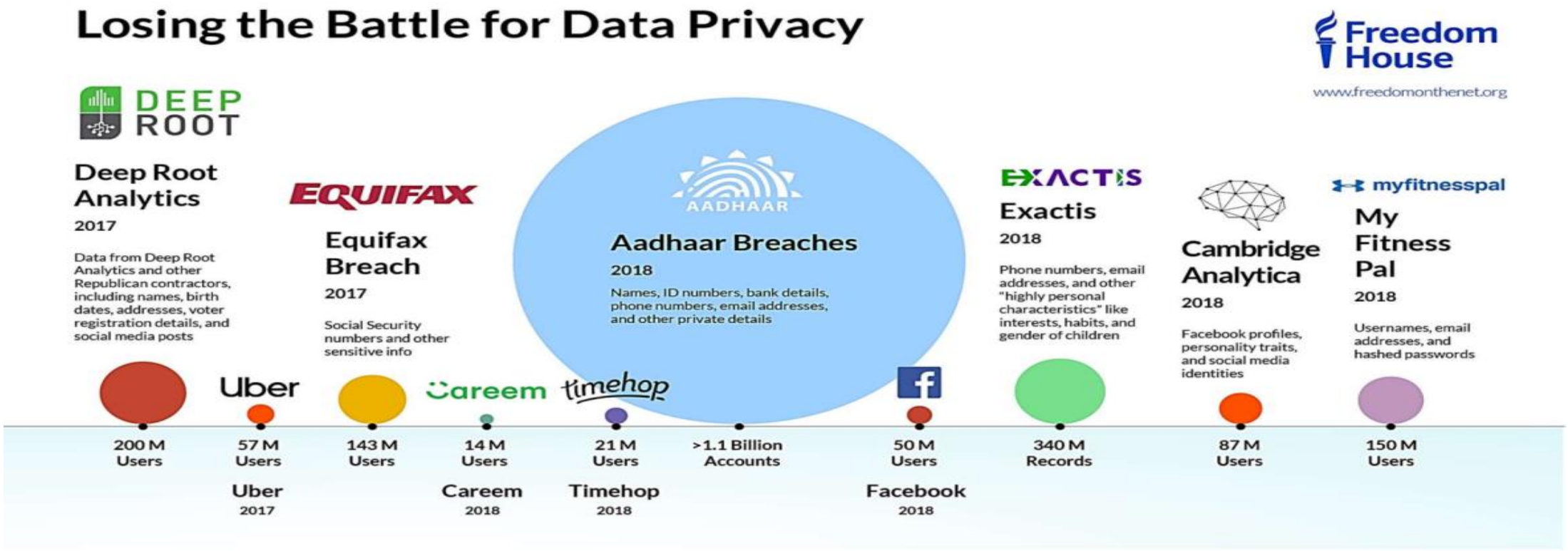


COVID 19 – Medical Data Breach





Sample of Global Data Breach



clario.

The companies that know most about you

#	Company	% of personal data collected	Email	Name	Age	Gender/Sex	Sexual Orientation	Marital Status	Race	Religious Belief	Live Location	Home Address	Employment Status	Job Title	Pet/Animal Ownership	Mobile Number	Landline Number	Type of Phone/Device	Hobbies	Interests	Height	Weight	Next of Kin	Mother's Maiden Name	Current Employers	Past Employers	Bank Account Details	Salary	Social Profile (Friends)	Social Profile (Hobbies)	Social Profile (Interests)	Country of Birth	Allergies/Intolerances	Health & Lifestyle Info
1	Facebook	70.59%	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•		•	•		•	•	•				
2	Instagram	58.82%	•	•	•	•					•	•	•	•	•	•		•	•	•	•			•	•			•	•				
3	Tinder	55.88%	•	•	•	•	•	•			•		•	•	•	•		•	•	•	•						•	•	•				
4	Grindr	52.94%	•	•	•	•	•	•			•		•	•	•	•		•	•	•	•							•	•				
5	Uber	52.94%	•	•	•	•					•	•	•	•		•	•	•	•	•						•	•	•	•				
6	Strava	41.18%	•	•	•	•					•	•				•		•				•	•				•	•	•				
7	Tesco	38.24%	•	•	•	•		•				•				•	•	•									•	•	•				
8	Spotify	35.29%	•	•	•							•				•	•	•			•						•	•	•				
9	MyFitnessPal	35.29%	•	•	•							•				•	•	•				•	•				•						•
10	Jet2	35.29%	•	•	•	•		•	•			•				•	•	•									•				•		
11	Credit Karma	32.35%	•	•	•								•	•		•		•				•	•				•	•					
12	Lidl Plus	32.35%	•	•	•							•	•		•	•	•	•									•						•
13	Netflix	26.47%	•	•	•								•			•	•	•			•						•						

https://www.google.com/search?q=ktp+elektronik&tbm=isch&tbs=rimg:CW9nsVsPI8R0IghvZ7FbD5fEdCoSCW9nsVsPI8R0EQ0Pktgam8pN&tbo=u&ved=2ahUKEwi56IHC89...

Google ktp elektronik Login

Semua Gambar Berita Maps Video Lainnya Setelan Alat SafeSearch

Ukuran Warna Hak penggunaan Jenis Waktu Gambar yang terkait Fitur lainnya Hapus

nik wna perekaman ktp mencoblos cimahi penghayat kepercayaan ilustrasi kependudukan pekanbaru ektp jateng dukcapil disdukcapil


Ribuan Warga Belum Miliki KTP elektroni...
indopos.co.id


Apa dan Bagaimana Penggunaan KTP ...
radioidola.com


Ingat, e-KTP Jadi Syarat Mutlak Pemilu 2019!
wartaekonomi.co.id


Ketahui Cara Membuat KTP ...
finansialku.com


5 Kesalahan Persepsi soal Kepemilikan e-K...
makassar.tribunnews.com

Nama Platform

needs access to

- Device & app history
- Identity
- Contacts
- Location
- Photos/Media/Files
- Camera
- Wi-Fi connection information
- Device ID & call information

Google Play | G Pay ACCEPT

Bukalapak - Jual Beli On...
App permissions

Version 4.37.6 may request access to

- **Camera**
  - take pictures and videos
- **Contacts**
  - read your contacts
  - find accounts on the device
- **Location**
  - access precise location (GPS and network-based)
  - access approximate location (network-based)
- **Microphone**
  - record audio
- **Telephone**
  - read phone status and identity
- **Storage**
  - modify or delete the contents of your SD card
  - read the contents of your SD card

Tokopedia - Jual Beli O...
App permissions

Version 3.26.1 may request access to

- **Camera**
  - take pictures and videos
- **Contacts**
  - read your contacts
- **Location**
  - access precise location (GPS and network-based)
  - access approximate location (network-based)
- **Telephone**
  - directly call phone numbers
  - read phone status and identity
- **Storage**
  - modify or delete the contents of your SD card
- **Other**
  - control vibration
  - This app can appear on top of other

GOJEK
App permissions

Version 3.25.2 may request access to

- **Camera**
  - take pictures and videos
- **Contacts**
  - read your contacts
  - find accounts on the device
  - modify your contacts
- **Location**
  - access precise location (GPS and network-based)
  - access approximate location (network-based)
- **Telephone**
  - directly call phone numbers
  - read phone status and identity
- **Storage**
  - modify or delete the contents of your SD card
  - read the contents of your SD card
- **Other**

Shopee: #2019PilihSho...
App permissions

- **Calendar**
  - add or modify calendar events and send emails to guests without owners' knowledge
  - Read calendar events and details
- **Camera**
  - take pictures and videos
- **Contacts**
  - read your contacts
- **Location**
  - access precise location (GPS and network-based)
  - access approximate location (network-based)
- **Microphone**
  - record audio
- **Storage**
  - modify or delete the contents of your SD card
  - read the contents of your SD card
- **Other**

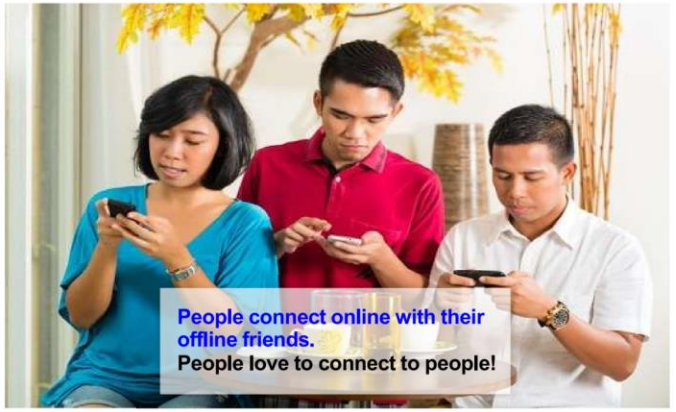
JD.ID Your Online Shopp...
App permissions

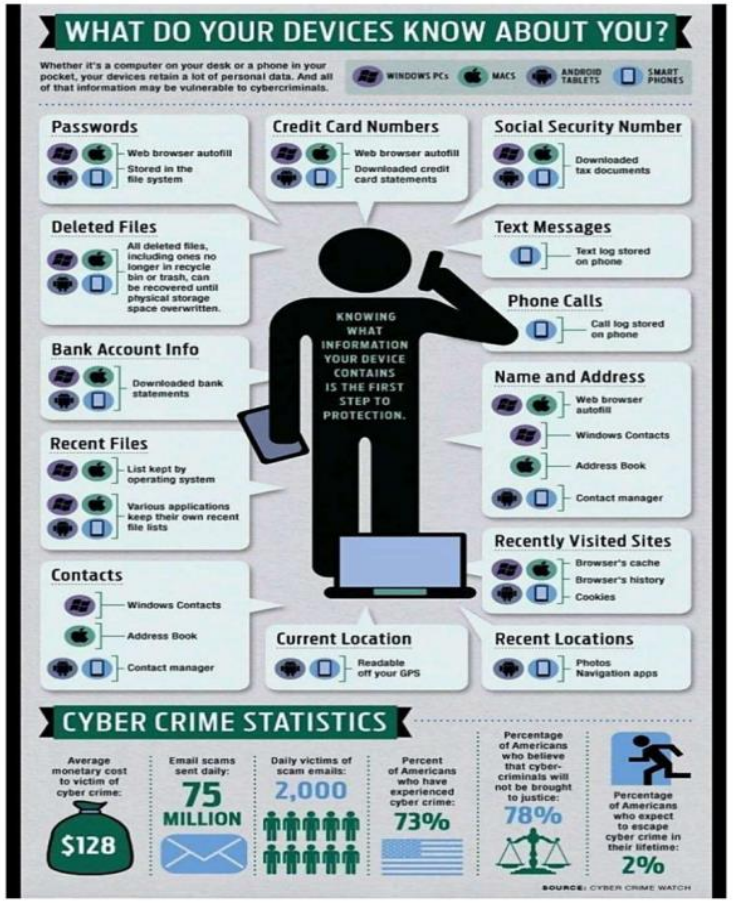
Version 5.3.1 may request access to

- **Camera**
  - take pictures and videos
- **Contacts**
  - read your contacts
  - find accounts on the device
- **Location**
  - access precise location (GPS and network-based)
  - access approximate location (network-based)
- **Telephone**
  - read phone status and identity
- **Storage**
  - modify or delete the contents of your SD card
  - read the contents of your SD card
- **Other**
  - control vibration

Key Challenges in this pandemic

People	Process	Technology
▪ *Identity & access management*	▪ *Information risk management*	▪ *Network*
▪ *Information security organization*	▪ *Policy and compliance framework*	▪ *Endpoints*
▪ *Training awareness & personnel*	▪ *Information asset management*	▪ *Database*
	▪ *Business continuity and DR*	▪ *Application infrastructure*
	▪ *Physical and environment sec*	▪ *Systems*
	▪ *Incident & threat management*	▪ *Messaging and content*
	▪ *Systems dev. & ops management*	▪ *Data*





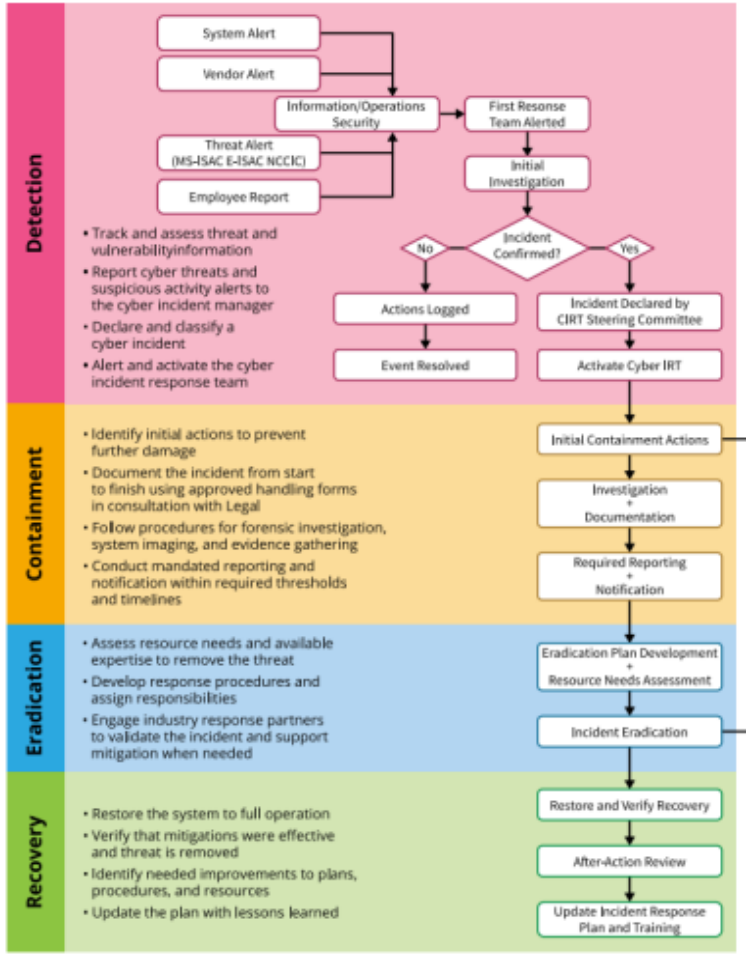
What's Next?

- Establish a Cyber Incident Response Team: Role, Committee, 24/7 Contact List of Personnel, and Technical Response.
- Critical System Classification: Network scheme, system, account permission list, and configuration.
- Incident Handling: Detection, Containment, Eradication and Recovery
- Classify Severity of Incidents
- Strategic Communication: Socialization and "need to know" basis.
- Exercise, Train, Test and Update the Plan
- Mystery Shopping

Sample Cyber Incident Severity Levels

Operational System (OT) and Business Impact	Level 5	**Cyber or cyber-physical event that directly impacts power delivery at one or multiple utilities**	Utility can no longer provide a critical operational service to all or a subset of users	Critical electric infrastructure information was compromised	Unpredictable; additional resources and outside help are needed	Poses an imminent threat to the provision of wide-scale critical infrastructure services
	Level 4	**Compromise of network or system that controls power generation and delivery and could lead to an outage at one or multiple utilities**	Utility can no longer provide a critical business service to all system users or can no longer provide a critical operational service to a subset of users	Critical electric infrastructure information was compromised	Unpredictable; additional resources and outside help are needed	Likely to result in a significant impact to the public health or safety, national security, economic security, foreign relations, or civil liberties
Business System (IT) Impacts	Level 3	**Compromise or denied availability to a business-critical enterprise system or service (e.g., corrupt or destroy data)**	Utility can no longer provide a critical business service to a subset of system users	Sensitive, PII, or proprietary information was accessed, changed, exfiltrated, deleted, or made unavailable	Unpredictable; additional resources and outside help may be needed	Likely to result in a demonstrable impact to the public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence
	Level 2	**Compromise of security to non-critical enterprise business systems**	Minimal effect; the utility can still provide all critical business services to all users, but has lost efficiency or lost some non-critical services	Non-PII or proprietary information was accessed or exfiltrated	Predictable with existing or additional resources	May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence
	Level 1	**Suspected security threat or isolated incident with minimal impact (e.g., unidentified server on network, successful phishing attempt with no loss of data)**	Minimal effect; the utility can still provide all critical services to all users, but has lost efficiency	Sensitive information at-risk but not exfiltrated	Predictable with existing or additional resources	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence
	Level 0	**Notification of suspicious behavior**	No effect to the organization's ability to provide all services to all users	No information was exfiltrated, changed, or deleted		Unsubstantiated or inconsequential event

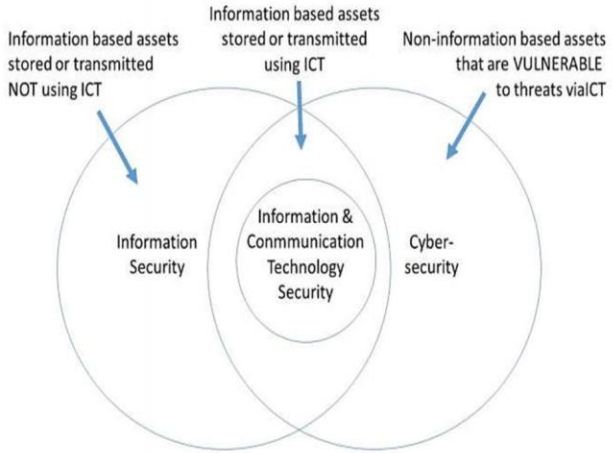
Cyber Incident Handling Process



Top Cyber Safety Tips

- **Update your software and operating system:** This means you benefit from the latest security patches.
- **Use anti-virus software:** Security solutions will detect and removes threats. Keep your software updated for the best level of protection.
- **Use strong passwords:** Ensure your passwords are not easily guessable.
- **Do not open email attachments from unknown senders:** These could be infected with malware.
- **Do not click on links in emails from unknown senders or unfamiliar websites:** This is a common way that malware is spread.
- **Avoid using unsecure WiFi networks in public places:** Unsecure networks leave you vulnerable to man-in-the-middle attacks.
- **Beware of** "un-pacthed vulnerabilities in systems and applications", "weak and compromised credentials", "lack of multi-factor authentication", and "inadequate network segmentation".

1. Unpatched vulnerabilities in systems and applications	2. Weak and compromised credentials	3. Lack of multi-factor authentication	4. Inadequate network segmentation
Vulnerability scans should be regularly performed to identify unpatched systems and applications for patching	Annual cyber security awareness training and on-going release of cyber security newsletter to promote best practices in protecting credentials.	Multi-factor Authentication should be required for remote access to protect against criminals using weak and compromised credentials.	Network segmentation should be implemented to separate networks into zones to limit access and protect critical systems and applications
Patch management tools should be used to enable large scale and rapid rollout of patches to vulnerable systems and applications	Privileged credentials should be centrally stored and managed.	Multi-factor Authentication should be extended to privileged access and critical systems / applications.	More granular network segmentation should be implemented to prevent attackers from moving laterally inside the network



Terima kasih

QUESTIONS?