

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

LEBIH MENDINGAN YANG MANA?

**DOMPET YANG
KETINGGALAN**



**HP YANG
KETINGGALAN**



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 memiliki 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*?

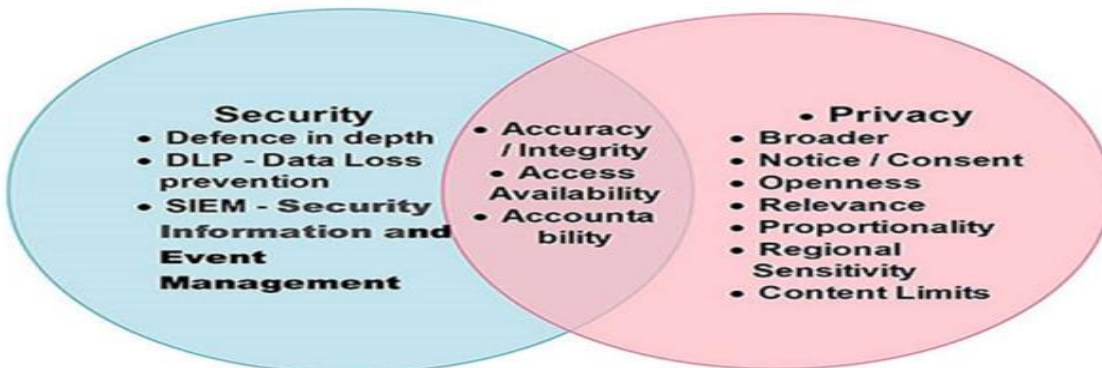
Mengapa asurans atas *cybersecurity* tidak dilakukan?

- 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

Security is not Privacy



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

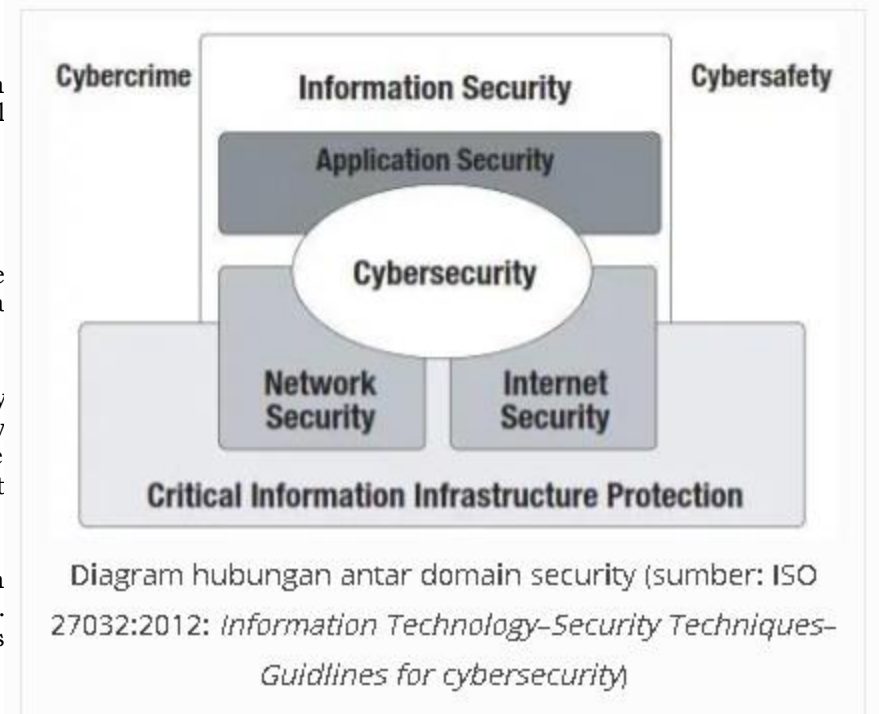
Counters

- 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.

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.



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
 ATTACKS/BREACHES
 New Campaign Combines Extortion, DDoS
 Latest attacks based on the reputation of two prominent APT groups to increase the threat credibility.

BANKinfo Security
 Copycat Hacking Groups Launch DDoS Attacks
 Akamai: Extortionists Target Financial Firms, Use APT Group Personas

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

Security Week
 DDoS Extortionists Claim to Be Armada Collective, Fancy Bear
 Cybercriminals claiming to represent well-known threat groups such as Fancy Bear and Armada Collective have been threatening organizations with distributed denial of service (DDoS) attacks, Akamai warns.

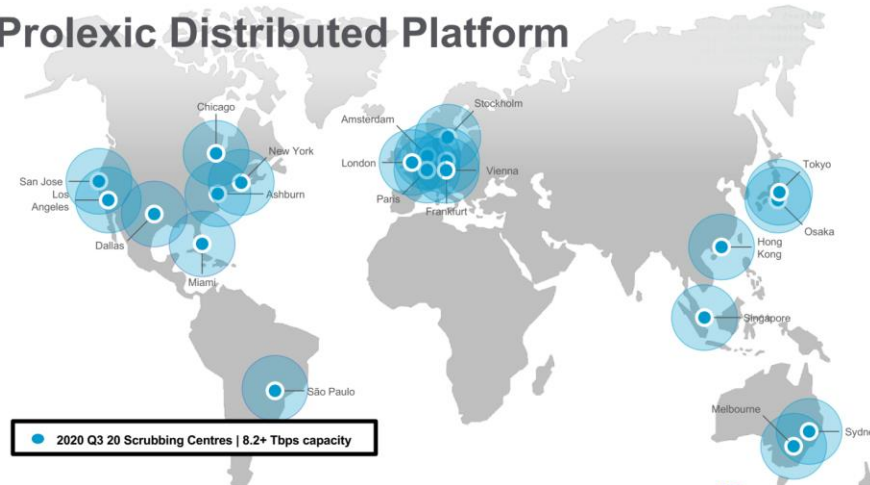
SC magazine
 Fancy Bear imposters extort finance, retail on DDoS threat

SC magazine

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

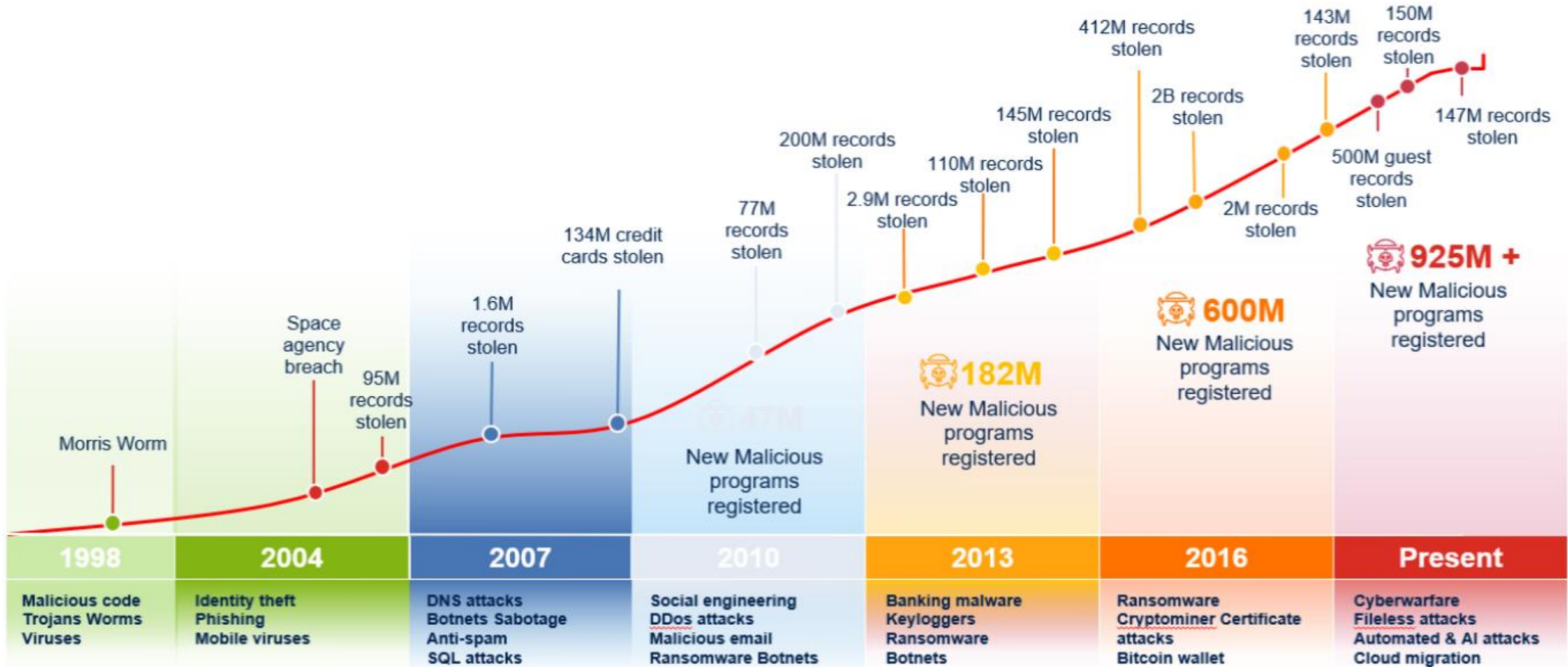
Security firm Akamai says a group of hackers posing as Fancy Bear, the infamous Russian intelligence outfit, have used distributed denial-of-service attacks to try extorting companies in multiple industries over the last week. The attacks tend to start with an email threatening the company with an impending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

Prolexic Distributed Platform

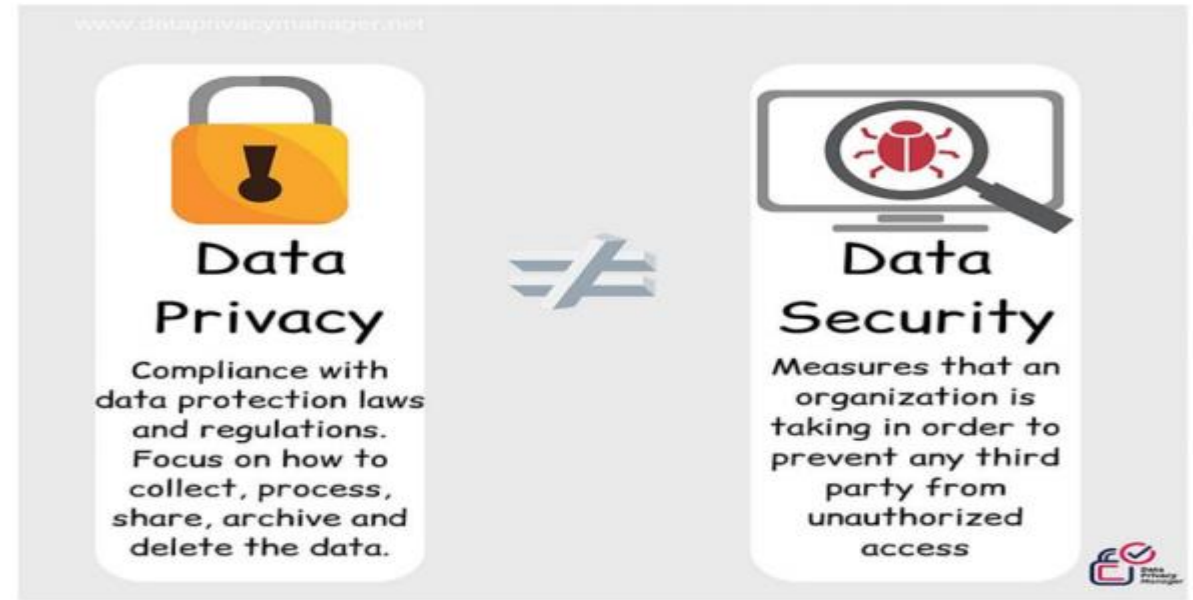


- Cybercriminals leveraging multiple attack vectors
- Targets focusing on overwhelming DNS, Web Application & Network/Data Centre Infrastructure
- Exhibited ability to pivot/morph to bypass controls
- Multi-Vector DDoS Attack Techniques

It's changing so fast...



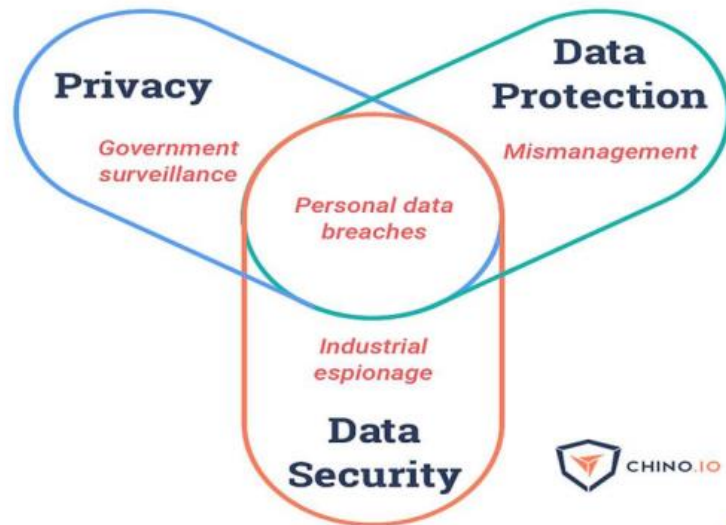
Data Protection vs Data Privacy



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 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

“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 tidak kepada pihak lain.”

Personal Identified Information (PII)



COVID 19 – Medical Data Breach

UNCLASSIFIED TLP:WHITE

Medical Data Uses

▶ Medical records purchased on the dark web can be used in a variety of malicious ways

Medical Identity Theft
Utilizing someone else's personal medical information to obtain medical services

- Prescriptions for drugs
- Surgeries and medical procedures
- False medical insurance claims

"Weaponizing" healthcare data
Using sensitive healthcare data to threaten, extort, or influence individuals

- leverage for ransom payments
- Can be real or doctored data
- Public figures and VIPs highly susceptible

Financial Fraud
Using PII in medical records to establish credit/banking profiles for financial gain.

- Healthcare organizations often carry financial data of individuals
- Loans and lines of credit often require data found in medical records
- False tax return claims

Cyber Campaigns
Using healthcare data to support hacking campaigns

- Contact information can be targeted for phishing and scams
- Credential/authentication information can be used for access/privilege escalation

Source: [Malware, creditcards, creditinfocenter](#)

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

UNCLASSIFIED 4/11/2019 8

HEALTHCARE INFORMATION IS 10 TIMES MORE VALUABLE

ON THE BLACK MARKET THAN SOCIAL SECURITY & CREDIT CARD INFORMATION.

WHY ?

NOT EASILY CHANGED	BASIS FOR INSURANCE/ CREDIT FRAUD	TARGET FOR OVERSEAS INTELLIGENCE
HIGH QUALITY AND DEEPLY PERSONAL	OBTAINING ILLICIT PRESCRIPTION DRUGS	BLACKMAIL POSSIBILITIES

REMEDIES

WATCH YOUR HEALTH INSURANCE PLAN FOR UNUSUAL ACTIVITY	MONITOR YOUR CREDIT FOR UNAUTHORIZED ACCOUNTS/INQUIRIES	STAY HEALTHY TO KEEP A SMALL DIGITAL FOOTPRINT
---	---	--

The Importance of Identity Management in Health Care

The health care industry can no longer afford to ignore the need for Identity Management. Ensuring the identities of their members are being authenticated and ongoing demographic information managed, is critical in light of the escalating rates of medical identity theft, data breaches, and benefit fraud.

Millions of new people are accessing the health care system through different channels

12.7 million people enrolled through the Health Insurance Marketplaces as of Jan 31, 2016.¹

the health care industry led the way in number of records breached by industry with **84.4 million records** in the first half-period of 2015.²

The Ponemon Institute estimates the annual economic impact of Medical Identity Theft is **\$11.6 billion**³

Half of all organizations have little or no confidence in their ability to detect all patient data loss or theft.⁴

49% agree they have sufficient technologies to effectively prevent or quickly detect unauthorized patient data access, loss or theft.⁴

Sources:
1) Data Source: Health Insurance Marketplace Open Enrollment Snapshot <https://www.cms.gov/Newsroom/MediaReleaseDatabase/Fact-sheets/2016-Fact-sheets-items/2016-02-04.html>
2) Healthcare Hackle Account for Most Data Breaches in 2015, Healthcare Information, September 8, 2015, <http://www.healthcare-informatics.com/news-items/healthcare-hackle-account-most-data-breaches-2015>
3) The Growing Problem of Medical Identity Theft, Security Intelligence, February 3, 2016, <https://securityintelligence.com/the-growing-problem-of-medical-identity-theft/>
4) FBI's Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute, May 2015, <https://www.ponemon.org/news-2016>

mcol

Sample of Global Data Breach

Losing the Battle for Data Privacy



Deep Root Analytics
2017

Data from Deep Root Analytics and other Republican contractors, including names, birth dates, addresses, voter registration details, and social media posts



200 M Users

Uber

57 M Users

Uber
2017

EQUIFAX

Equifax Breach
2017

Social Security numbers and other sensitive info



143 M Users

Careem

14 M Users

Careem
2018

timehop

21 M Users

Timehop
2018



Aadhaar Breaches
2018

Names, ID numbers, bank details, phone numbers, email addresses, and other private details

>1.1 Billion Accounts



50 M Users

Facebook
2018

EXACTIS

Exactis
2018

Phone numbers, email addresses, and other "highly personal characteristics" like interests, habits, and gender of children



340 M Records



Cambridge Analytica
2018

Facebook profiles, personality traits, and social media identities



87 M Users

myfitnesspal

My Fitness Pal
2018

Usernames, email addresses, and hashed passwords



150 M Users

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%	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

Google search results for 'ktp elektronik'. The search bar shows 'ktp elektronik' and the results include various articles and images related to electronic Indonesian National ID cards (KTP elektronik).

Articles shown include:

- Ribuan Warga Belum Miliki KTP elektronik... indopa.co.id
- Apa dan Bagaimana Penggunaan KTP ... radiodola.com
- Ingat, e-KTP Jadi Syarat Mutlak Pemilu 2019! wartaekonomi.co.id
- Ketahui Cara Membuat KTP ... snansialku.com
- 5 Kesalahan Persepsi soal Kepemilikan e-K... makassar.tribunnews.com

Images include photos of people holding their KTP elektronik cards, some showing the physical card and others showing the digital version on a smartphone.

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

Version 5.3.1 may request access to

- 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)
- Telephone: read phone status and identity
- Microphone: record audio
- Storage: modify or delete the contents of your SD card, read the contents of your SD card
- Other: control vibration

JD.ID Your Online Shopp...

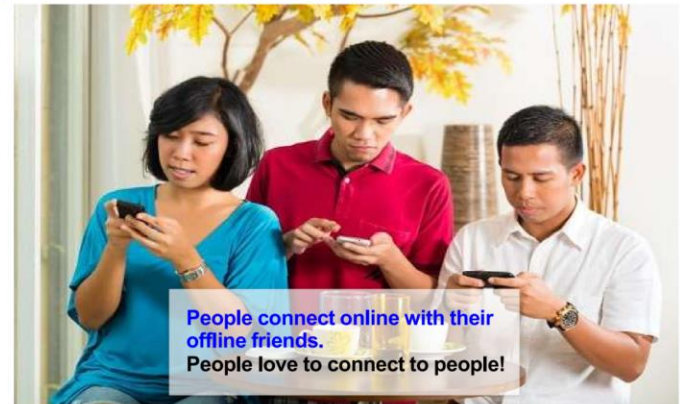
App permissions

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
<ul style="list-style-type: none"> Identity & access management Information security organization Training awareness & personnel 	<ul style="list-style-type: none"> Information risk management Policy and compliance framework Information asset management Business continuity and DR Physical and environment sec Incident & threat management Systems dev. & ops management 	<ul style="list-style-type: none"> Network Endpoints Database Application infrastructure Systems Messaging and content Data



WHAT DO YOUR DEVICES KNOW ABOUT YOU?

Whether it's a computer on your desk or a phone in your pocket, your devices retain a lot of personal data. And all of that information may be vulnerable to cybercriminals.

WINDOWS PCs | MACS | ANDROID TABLETS | SMART PHONES

Passwords Web browser autofill Stored in the file system	Credit Card Numbers Web browser autofill Downloaded credit card statements	Social Security Number Downloaded tax documents
Deleted Files All deleted files, including ones no longer in recycle bin or trash, can be recovered until physical storage space overwritten.	Text Messages Text log stored on phone	Phone Calls Call log stored on phone
Bank Account Info Downloaded bank statements	Name and Address Web browser autofill Windows Contacts Address Book Contact manager	Recently Visited Sites Browser's cache Browser's history Cookies
Recent Files List kept by operating system Various applications keep their own recent file lists	Current Location Readable off your GPS	Recent Locations Photos Navigation apps
Contacts Windows Contacts Address Book Contact manager	KNOWING WHAT INFORMATION YOUR DEVICE CONTAINS IS THE FIRST STEP TO PROTECTION.	

CYBER CRIME STATISTICS

Average monetary cost to victim of cyber crime: \$128	Email scams sent daily: 75 MILLION	Daily victims of scam emails: 2,000	Percent of Americans who have experienced cyber crime: 73%	Percentage of Americans who believe that cyber-criminals will not be brought to justice: 78%	Percentage of Americans who expect to escape cyber crime in their lifetime: 2%
---	--	---	--	--	--

SOURCE: CYBER CRIME WATCH



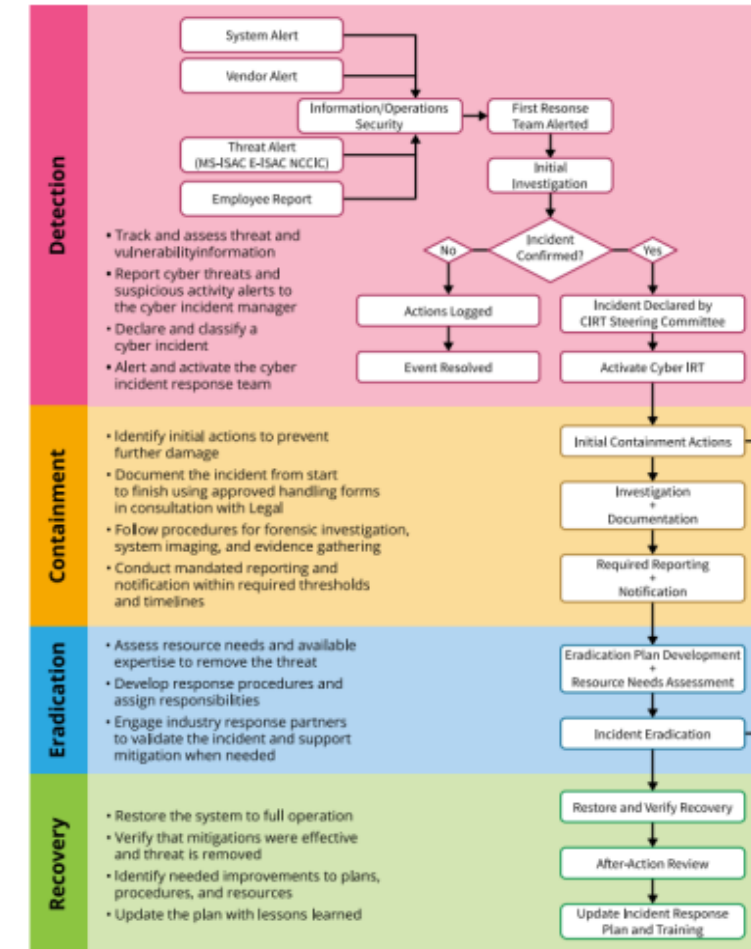
What's Next?

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

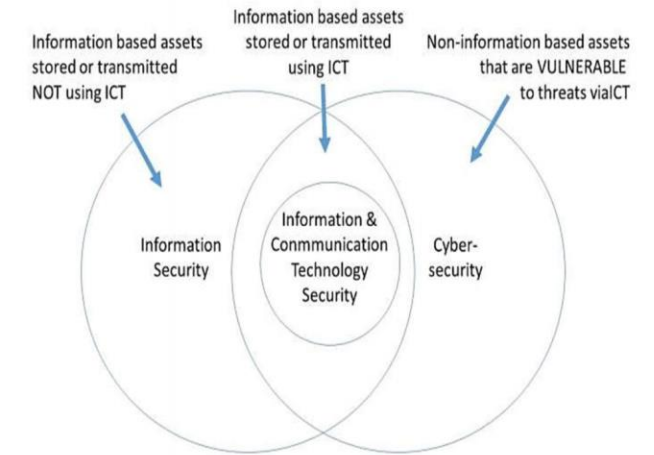
Cyber Incident Handling Process



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



Terima kasih

QUESTIONS?