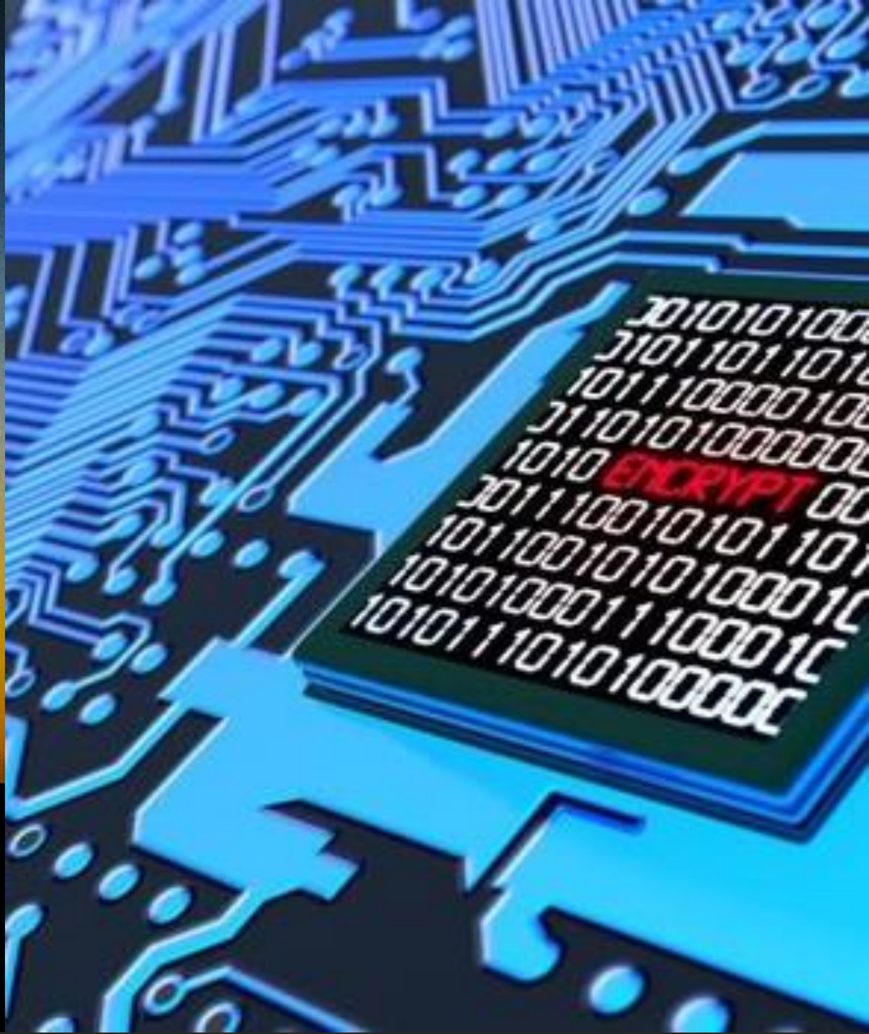
UNIVERSITAS
INDONESIA
Veritas, Probitas, Iustitia

AiCI
ARTIFICIAL INTELLIGENCE
CENTER INDONESIA

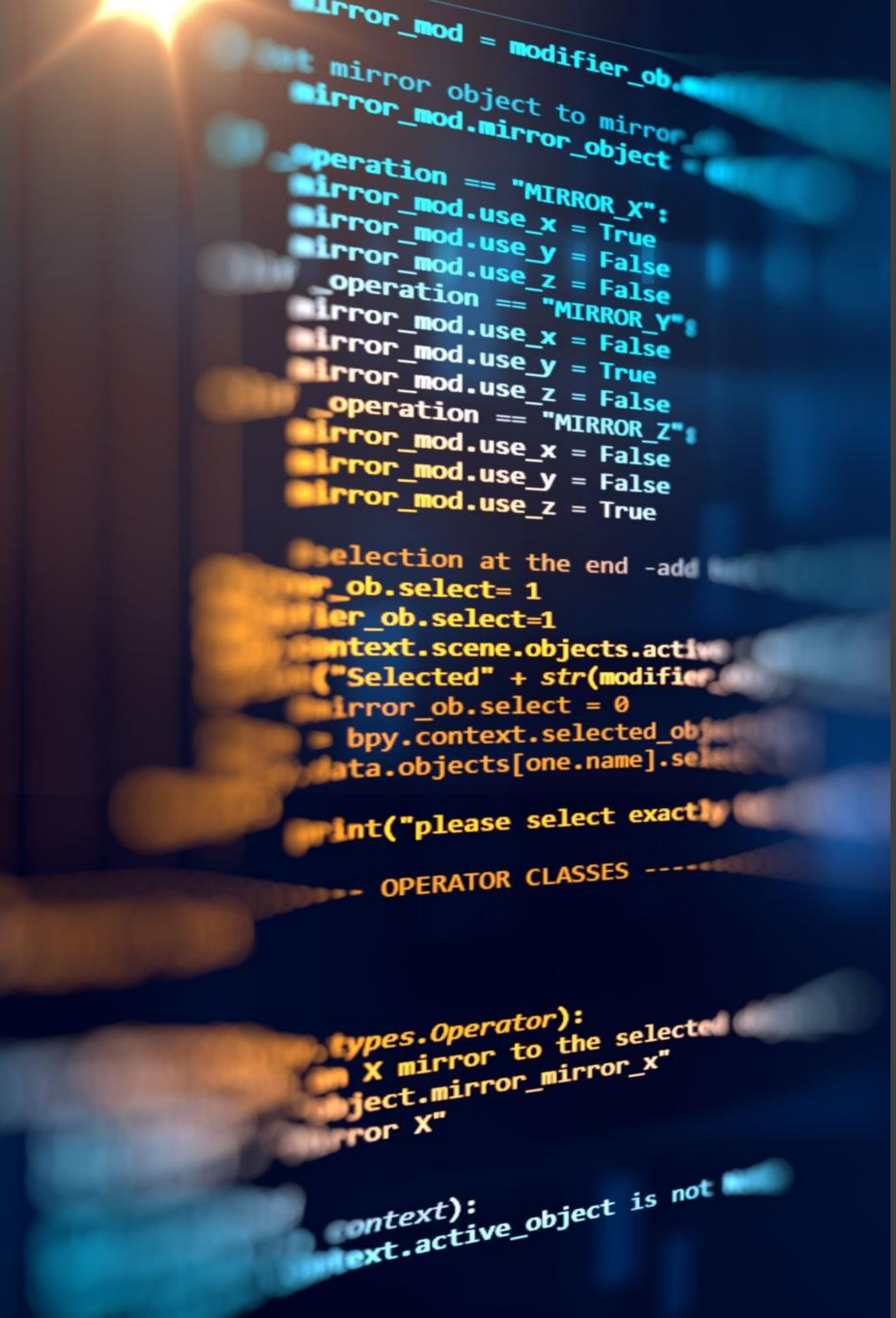


Expert Learning Series

CYBER SECURITY IN INDUSTRIAL PRACTICES

Composed
by Victor Arief Maulana
Indonesia Cyber Awareness Resilience Center
CAMP member ID : 0031

CONFIDENTIAL & LIMITED DISTRIBUTION



Agenda

1	PART -1 : CYBER SECURITY INTRODUCTION
2	PART -2 : CYBER SECURITY FRAMEWORK
3	PART - 3 : USE CASES CYBER SECURITY IN HEALTH CARE
4	PART - 4 : CYBER SECURITY TECHNOLOGY

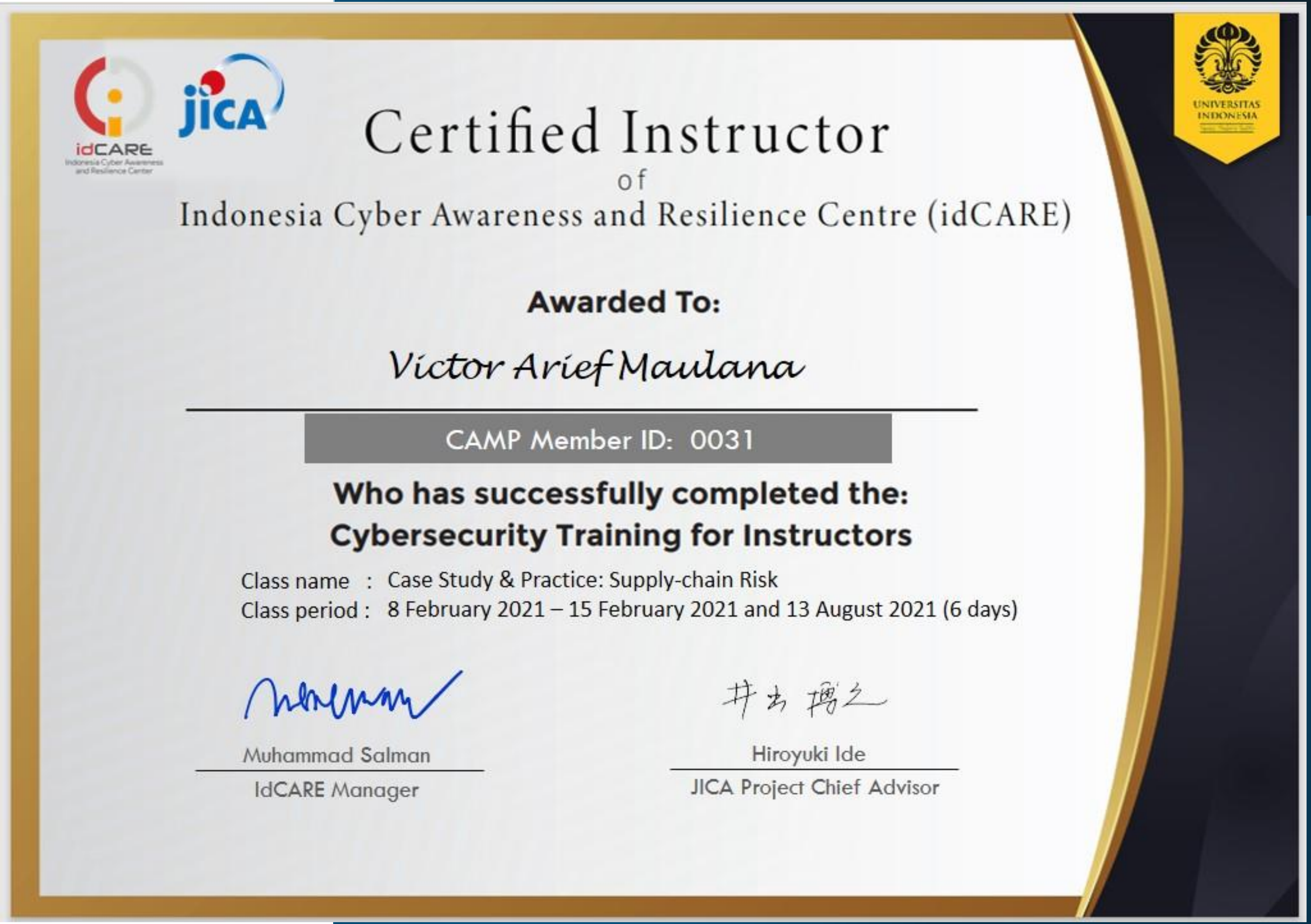
UNIVERSITAS
INDONESIA

CYBER SECURITY IN INDUSTRIAL PRACTICE

M. Anang Jatmiko, M.Pd
Moderator

Zoom Meeting
https://bit.ly/Expertlearning2

Victor Arief Maulana



idCARE
Indonesia Cyber Awareness and Resilience Center

UNIVERSITAS INDONESIA

Certified Instructor

of

Indonesia Cyber Awareness and Resilience Centre (idCARE)

Awarded To:

Victor Arief Maulana

CAMP Member ID: 0031

Who has successfully completed the:
Cybersecurity Training for Instructors

Class name : Case Study & Practice: Supply-chain Risk
Class period : 8 February 2021 – 15 February 2021 and 13 August 2021 (6 days)

Muhammad Salman
IdCARE Manager

井出 [illegible]之
Hiroyuki Ide
JICA Project Chief Advisor

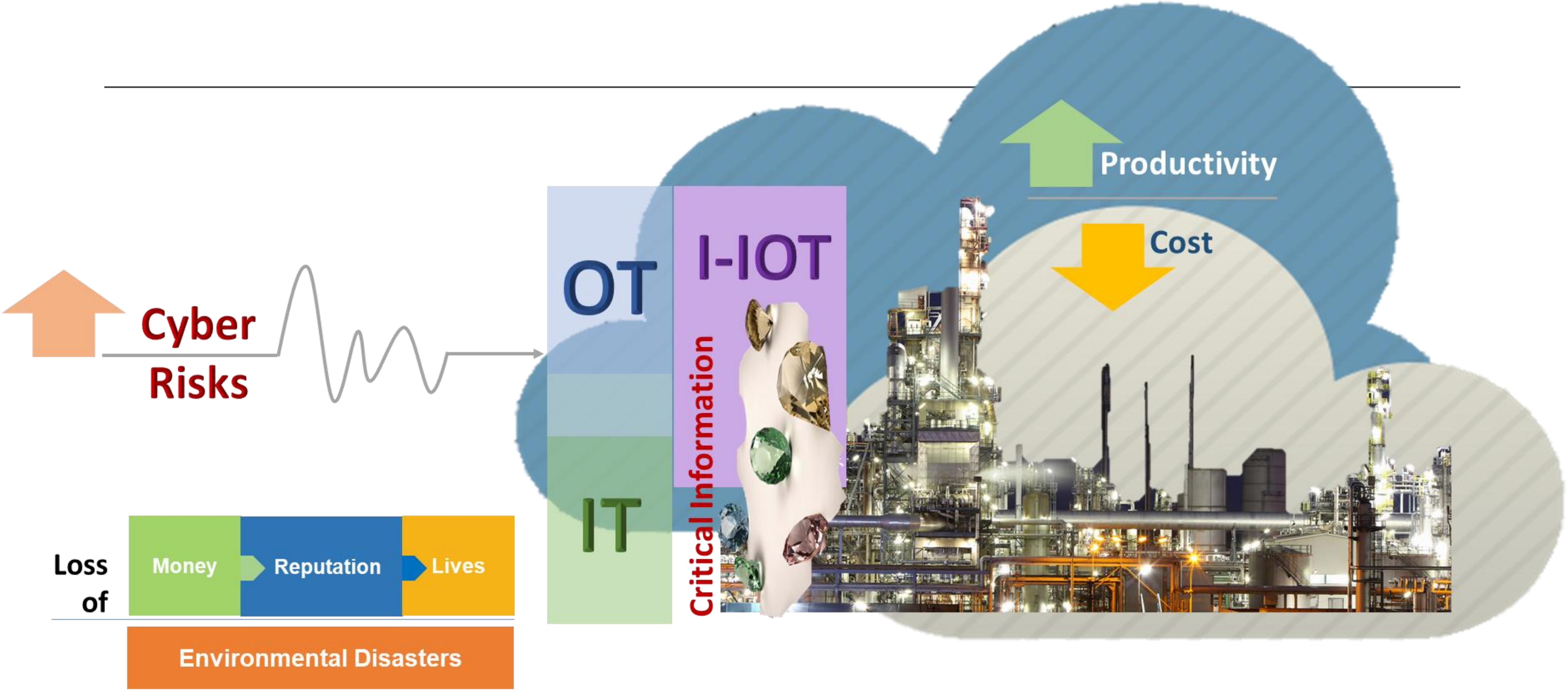
Insight

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

Robert Mueller
FBI Director, 2012

Industry 4.0

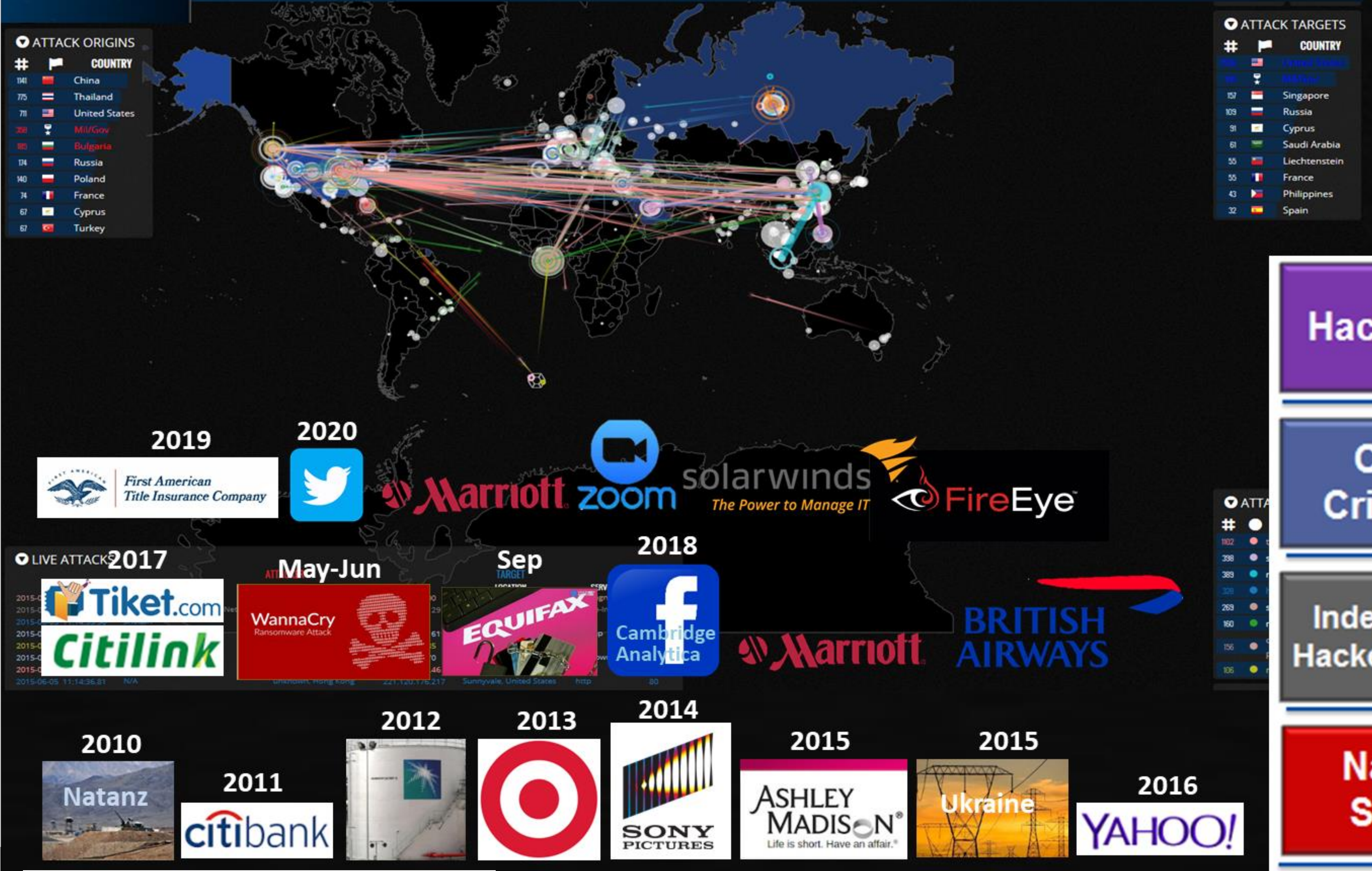
Digital Hyper-Connectivity Breeds Efficiency as well as More Exposures to Cyber Attacks



The Threat is Real

Global Live Attack

http://map.ipviking.com/



ATTACK ORIGINS

#		COUNTRY
1141		China
775		Thailand
711		United States
[illegible]		Mil/Gov
[illegible]		Bulgaria
174		Russia
140		Poland
74		France
67		Cyprus
67		Turkey

ATTACK TARGETS

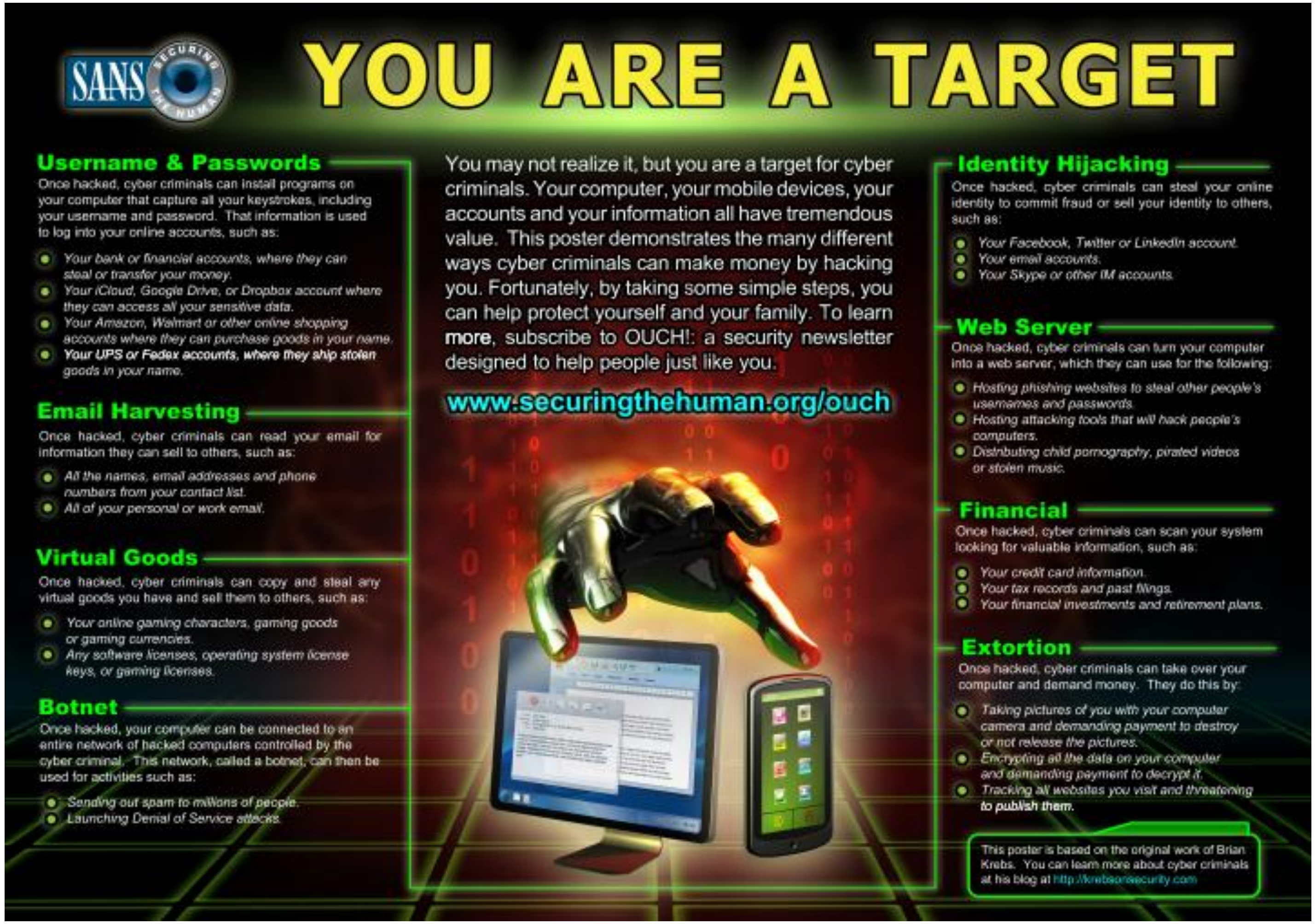
#		COUNTRY
[illegible]		[illegible]
[illegible]		[illegible]
157		Singapore
109		Russia
91		Cyprus
61		Saudi Arabia
55		Liechtenstein
55		France
43		Philippines
32		Spain

Threat Actors

	Sophistication	Motivation
Hacktivists	Low to moderate	Political, ideological, and/or religious beliefs
Cyber Criminals	Moderate to high	Financial gain
Independent Hacker Groups	Low to moderate	Financial gain; nationalism; political or ideological beliefs
Nation-States	Moderate to high	Espionage; nationalism; financial gain

One Sure Fact of Life by today and onwards :

Cyber Attack is real and present danger



YOU ARE A TARGET

Username & Passwords

Once hacked, cyber criminals can install programs on your computer that capture all your keystrokes, including your username and password. That information is used to log into your online accounts, such as:

- *Your bank or financial accounts, where they can steal or transfer your money.*
- *Your iCloud, Google Drive, or Dropbox account where they can access all your sensitive data.*
- *Your Amazon, Walmart or other online shopping accounts where they can purchase goods in your name.*
- ***Your UPS or Fedex accounts, where they ship stolen** goods in your name.*

Email Harvesting

Once hacked, cyber criminals can read your email for information they can sell to others, such as:

- *All the names, email addresses and phone numbers from your contact list.*
- *All of your personal or work email.*

Virtual Goods

Once hacked, cyber criminals can copy and steal any virtual goods you have and sell them to others, such as:

- *Your online gaming characters, gaming goods or gaming currencies.*
- *Any software licenses, operating system license keys, or gaming licenses.*

Botnet

Once hacked, your computer can be connected to an entire network of hacked computers controlled by the cyber criminal. This network, called a botnet, can then be used for activities such as:

- *Sending out spam to millions of people.*
- *Launching Denial of Service attacks.*

You may not realize it, but you are a target for cyber criminals. Your computer, your mobile devices, your accounts and your information all have tremendous value. This poster demonstrates the many different ways cyber criminals can make money by hacking you. Fortunately, by taking some simple steps, you can help protect yourself and your family. To learn more, subscribe to OUCH!: a security newsletter designed to help people just like you.

www.securingthehuman.org/ouch

Identity Hijacking

Once hacked, cyber criminals can steal your online identity to commit fraud or sell your identity to others, such as:

- *Your Facebook, Twitter or LinkedIn account.*
- *Your email accounts.*
- *Your Skype or other IM accounts.*

Web Server

Once hacked, cyber criminals can turn your computer into a web server, which they can use for the following:

- *Hosting phishing websites to steal other people's usernames and passwords.*
- *Hosting attacking tools that will hack people's computers.*
- *Distributing child pornography, pirated videos or stolen music.*

Financial

Once hacked, cyber criminals can scan your system looking for valuable information, such as:

- *Your credit card information.*
- *Your tax records and past filings.*
- *Your financial investments and retirement plans.*

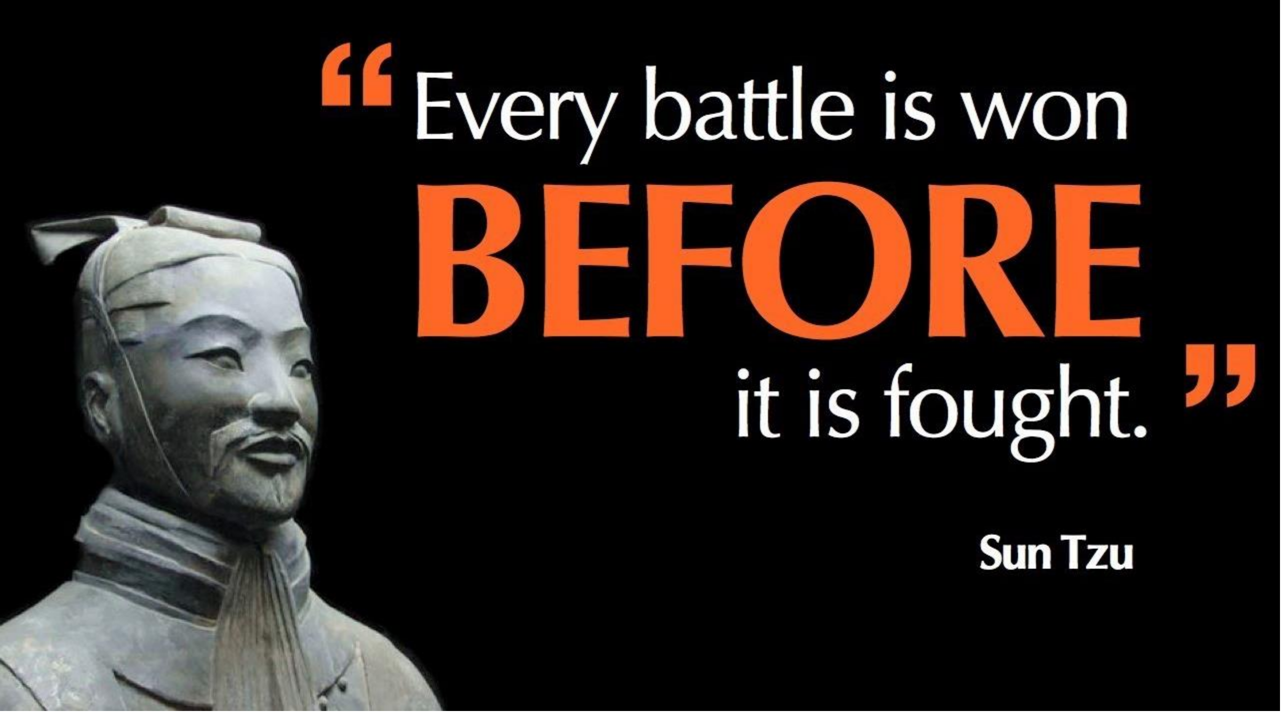
Extortion

Once hacked, cyber criminals can take over your computer and demand money. They do this by:

- *Taking pictures of you with your computer camera and demanding payment to destroy or not release the pictures.*
- *Encrypting all the data on your computer and demanding payment to decrypt it.*
- *Tracking all websites you visit and threatening **to publish them.***

This poster is based on the original work of Brian Krebs. You can learn more about cyber criminals at his blog at http://krebsonsecurity.com

Understanding Cyber Attack Situations



Major attack types you need to know at least

- DDoS
- Vulnerability Exploit
- APT Phishing attack
- Account Hijack
- Malware
- Web Defacement
- Ransomware
- Banking Trojan

CORE
TIERS
CYBERSECURITY
FRAMEWORK
PROFILE

The Cybersecurity Framework

Three Primary Components

Core

Desired cybersecurity outcomes organized in a hierarchy and aligned to more detailed guidance and controls

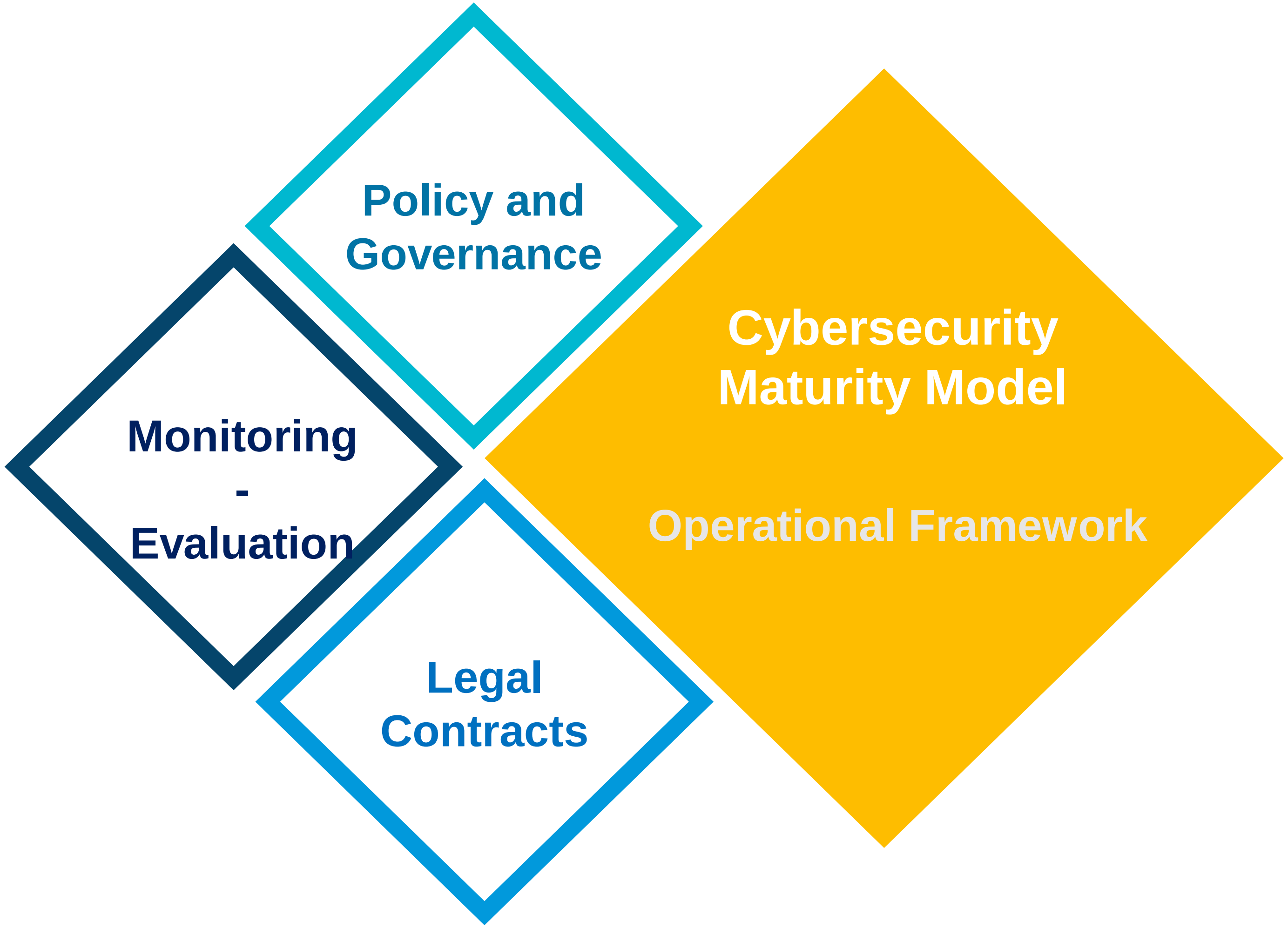
Profiles

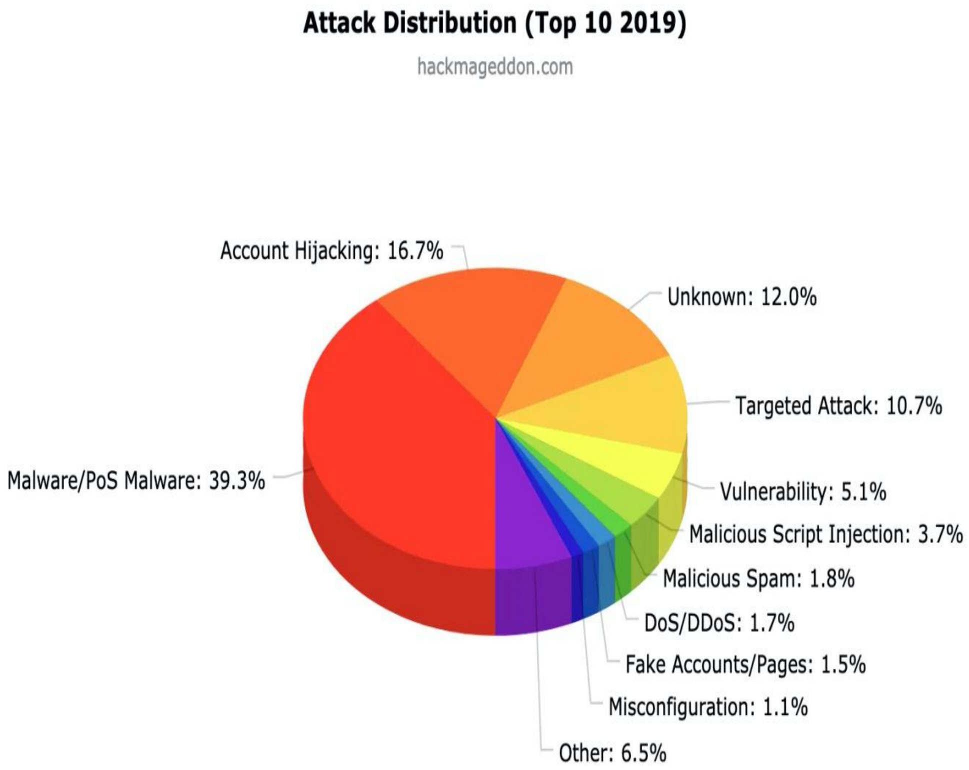
Alignment of an organization's requirements and objectives, risk appetite and resources *using* the desired outcomes of the Framework Core

Implementation Tiers

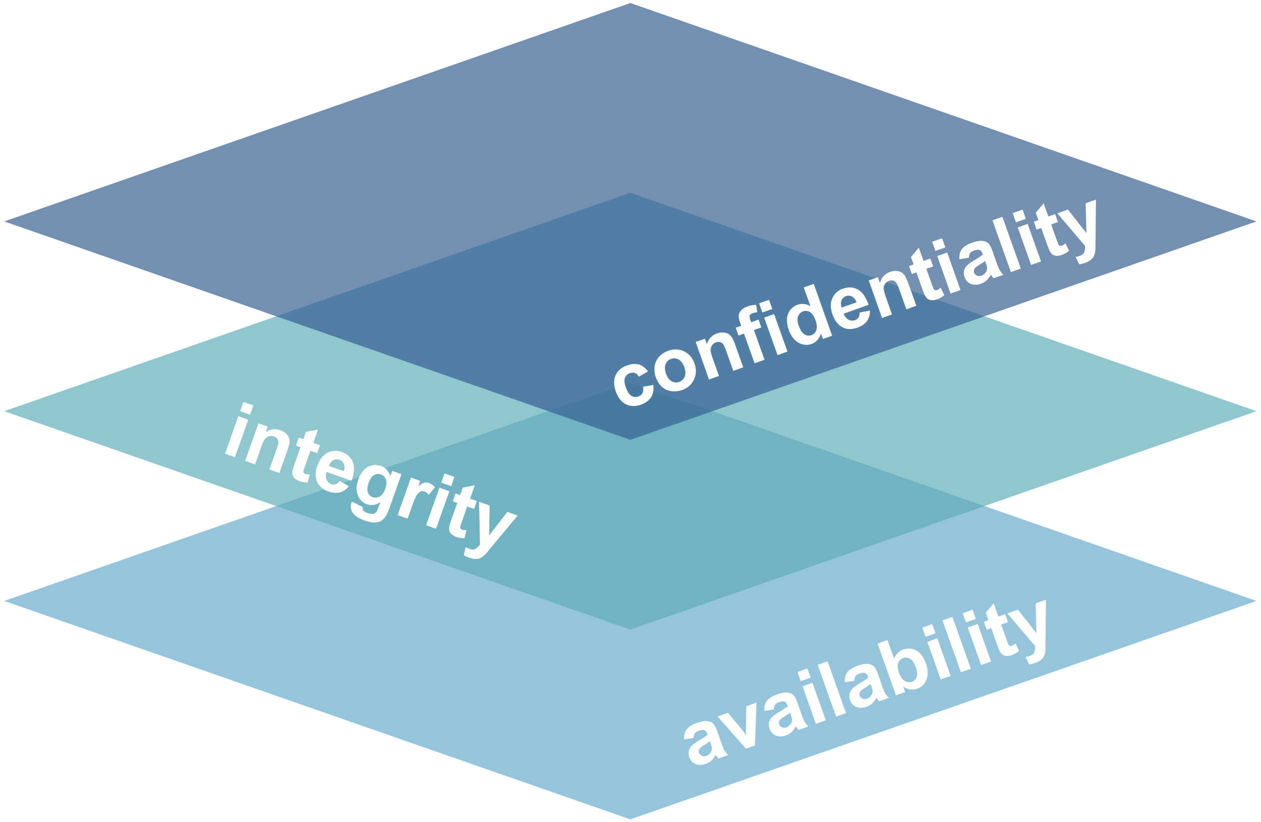
A qualitative measure of organizational cybersecurity risk management practices

The Methods to Survive from Cyber Attack





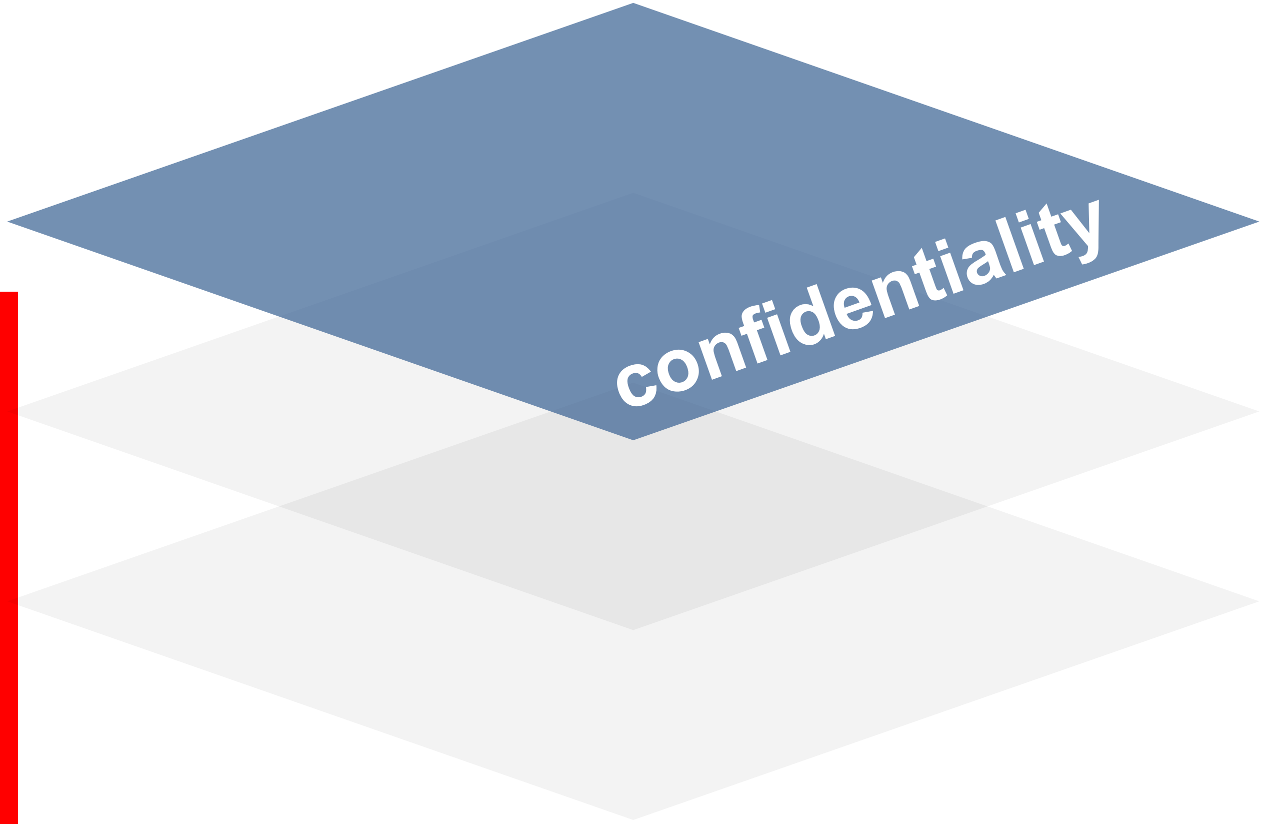
Cybersecurity Objectives



More
NIST Special Publication 800-12, revision 1
An Introduction to Information Security
section 1.4

An Introduction to Information Security

Confidentiality

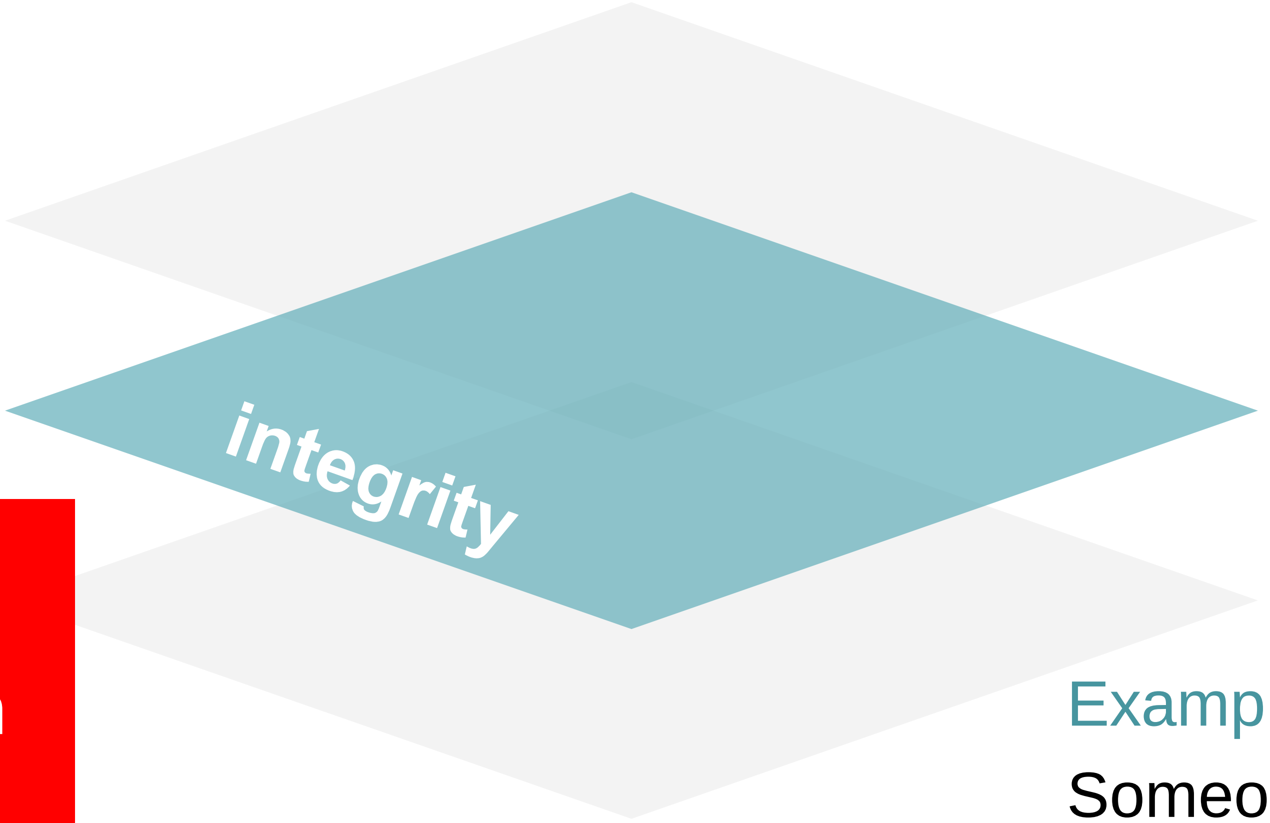


Protecting information from unauthorized access and disclosure

Example:

Criminal steals customers' usernames, passwords, or credit card information

Integrity



Protecting information from unauthorized modification

Example:

Someone alters payroll information or a proposed product design

Availability

availability

Example:

Your customers are unable to access your online services

Preventing disruption in how information is accessed

An Introduction to Information Security

Cybersecurity Threats

- Phishing Attacks
- Ransomware
- Hacking
- Imposter Scams
- Environmental events

More
NIST Interagency Report 7621, revision 1 | *Small Business Information Security: The Fundamentals,* section 2.1

Phishing Attacks

- Social engineering attack involving trickery
- Designed to gain access to systems or steal data
- Targeted phishing is “spear phishing”
- Variants include “vishing” – attacks by telephone and “smishing” those using SMS or text

Example:
An email about a delayed shipment causes you to click a link and download malware to your network

Ransomware

- *Type of software with malicious intent and a threat to harm your data*
- The author or distributor requires a ransom to undo the damage
- *No guarantee the ransom payment will work*
- Ransom often needs to be paid in cryptocurrency

Example:
WannaCry was one of the most devastating ransomware attacks in history, affecting several hundred thousand machines and crippling banks, law enforcement agencies, and other infrastructure.

An Introduction to Information Security

Hacking

- *Unauthorized access to systems and information*
- *Website attack such as DDOS*
- *Access denied to authorized users*
- *Stolen funds or intellectual property*

Example:
Newspaper kiosk’s point-of-sale system was hacked; malware installed. Every customer’s credit card information was sent to criminals.

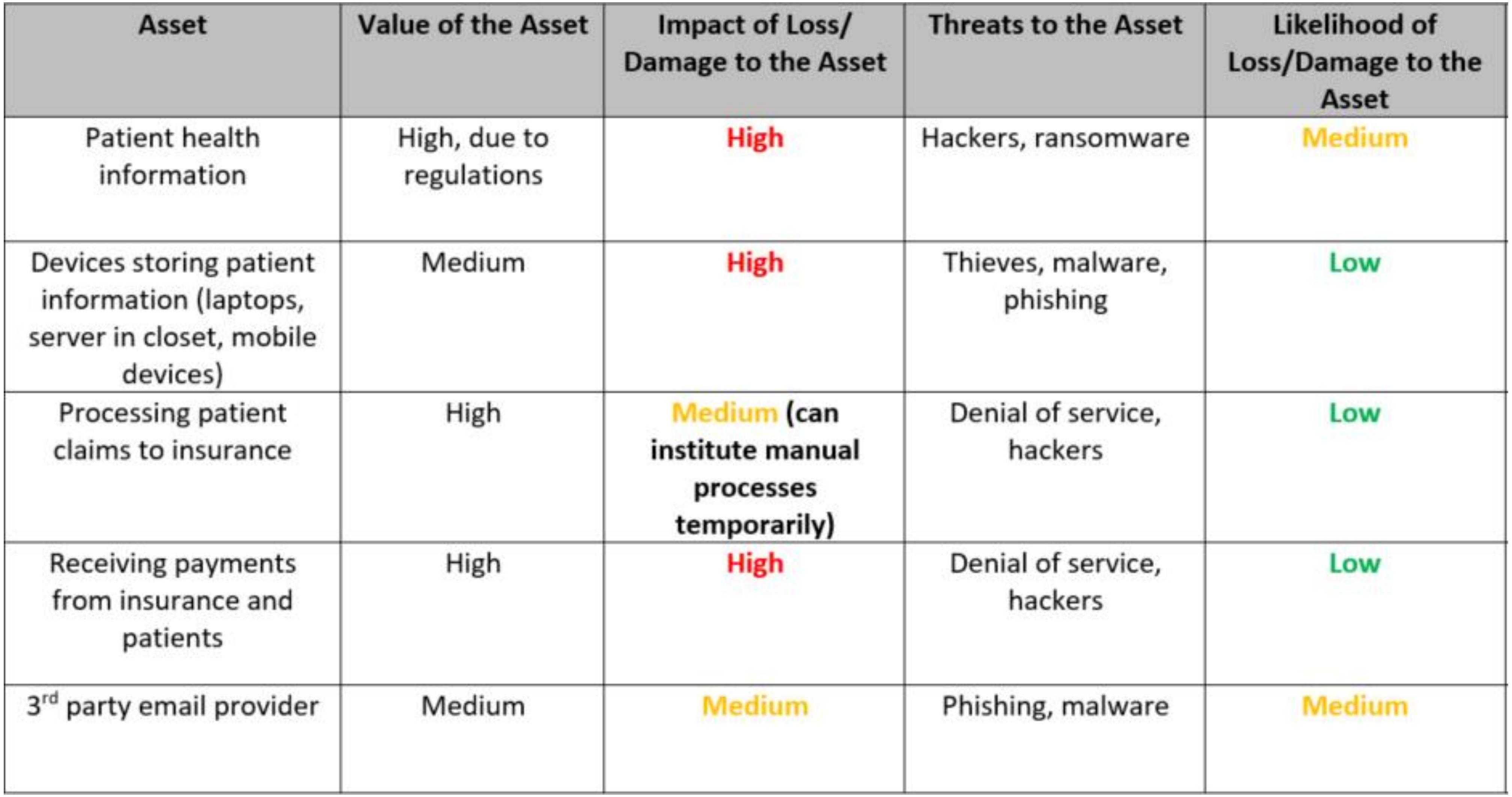
Imposter Scams

- Someone “official” calls or emails to report a crisis situation
- They represent the IRS, a bank, the lottery or technical support
- There will be a sense of urgency and a dire penalty or loss if you don’t act

Example:

IRS scams – You receive a phone call claiming to be the IRS, reporting you owe money and need to pay or else get hit with a fine.

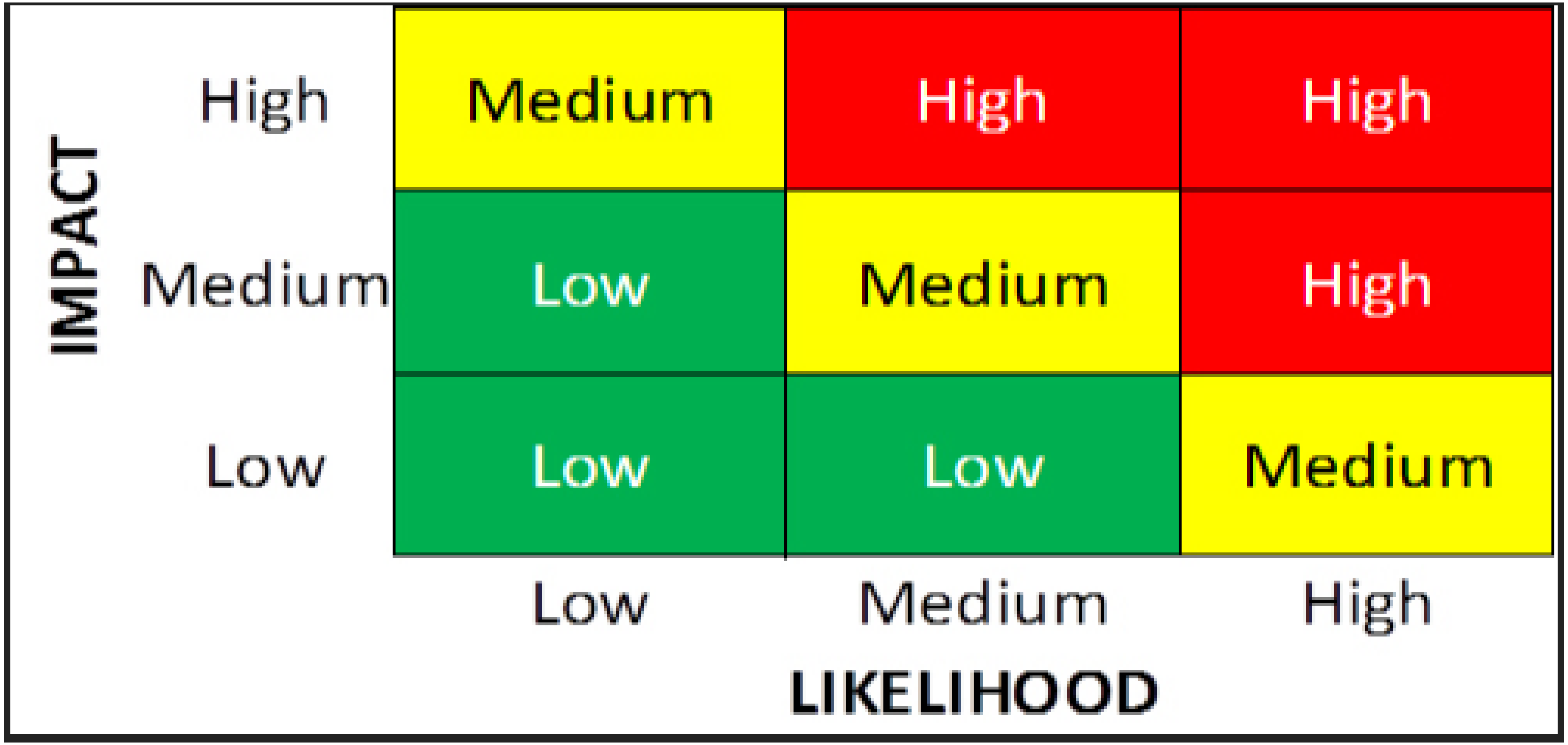
Identify likelihood of loss or damage to the asset



Asset	Value of the Asset	Impact of Loss/ Damage to the Asset	Threats to the Asset	Likelihood of Loss/Damage to the Asset
Patient health information	High, due to regulations	High	Hackers, ransomware	Medium
Devices storing patient information (laptops, server in closet, mobile devices)	Medium	High	Thieves, malware, phishing	Low
Processing patient claims to insurance	High	Medium **(can institute manual processes temporarily)**	Denial of service, hackers	Low
Receiving payments from insurance and patients	High	High	Denial of service, hackers	Low
3rd party email provider	Medium	Medium	Phishing, malware	Medium

Identify Priorities and Potential Solutions

Prioritize Assets - Risk Matrix



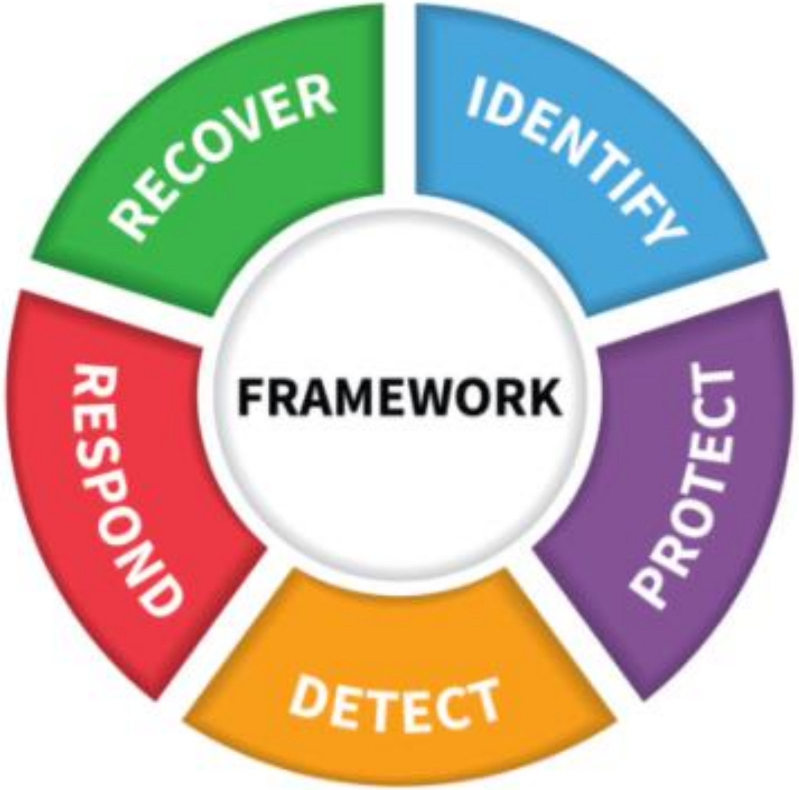
IMPACT	High	Medium	High	High
	Medium	Low	Medium	High
	Low	Low	Low	Medium
		Low	Medium	High
			LIKELIHOOD	

NIST Cyber Security Framework (CSF)

Key Framework Attributes

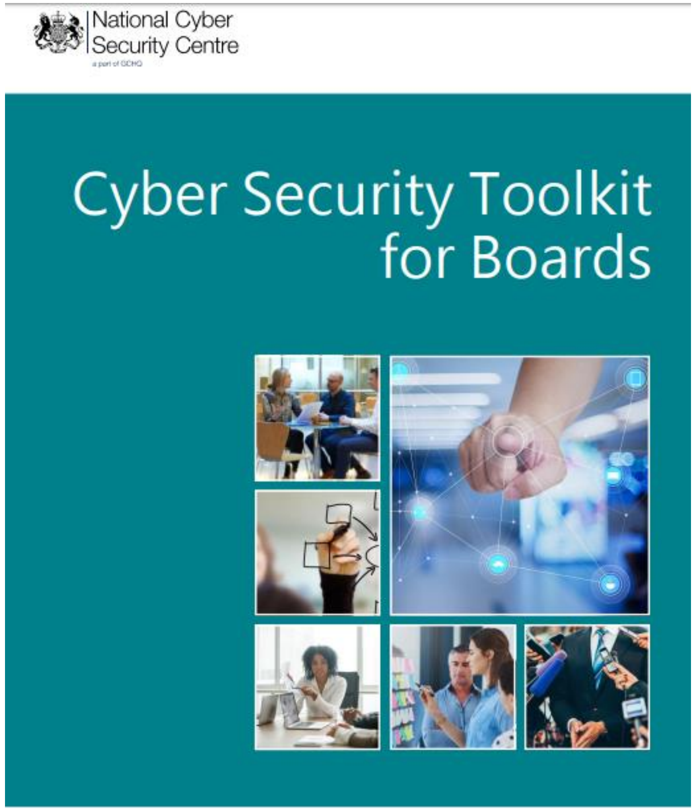
Principles of Current and Future Versions of the Framework

- Common and accessible language
- Adaptable to many technologies, lifecycle phases, sectors and uses
- Risk-based
- Based on international standards
- Living document
- Guided by many perspectives – private sector, academia, public sector



Board Leadership

Good cyber security protects that ability to function, and ensures organisations can exploit the opportunities that technology brings. Cyber security is therefore central to an organization's health and resilience, and this places it firmly within **the responsibility of the Board**.



National Cyber Security Centre
a part of GCHQ

Cyber Security Toolkit for Boards

Experts at Cyber Security Center of Excellence in Indonesia

Guiding Principles & Coaching for CISO (Chief Information Security Officer) Roles

For a large enterprise, the CISO(Chief Information Officer) or his /her direct reports will:

- •Direct and approve the design of security systems;
- •Ensure that disaster recovery and business continuity plans are in place and tested;
- •Review and approve security policies, controls and cyber incident response planning;
- •Approve identity and access policies;
- •Review investigations after breaches or incidents, including impact analysis and recommendations for avoiding similar vulnerabilities;
- •Maintain a current understanding the IT threat landscape for the industry;

CONFIDENTIAL & LIMITED DISTRIBUTION

What should the board do?

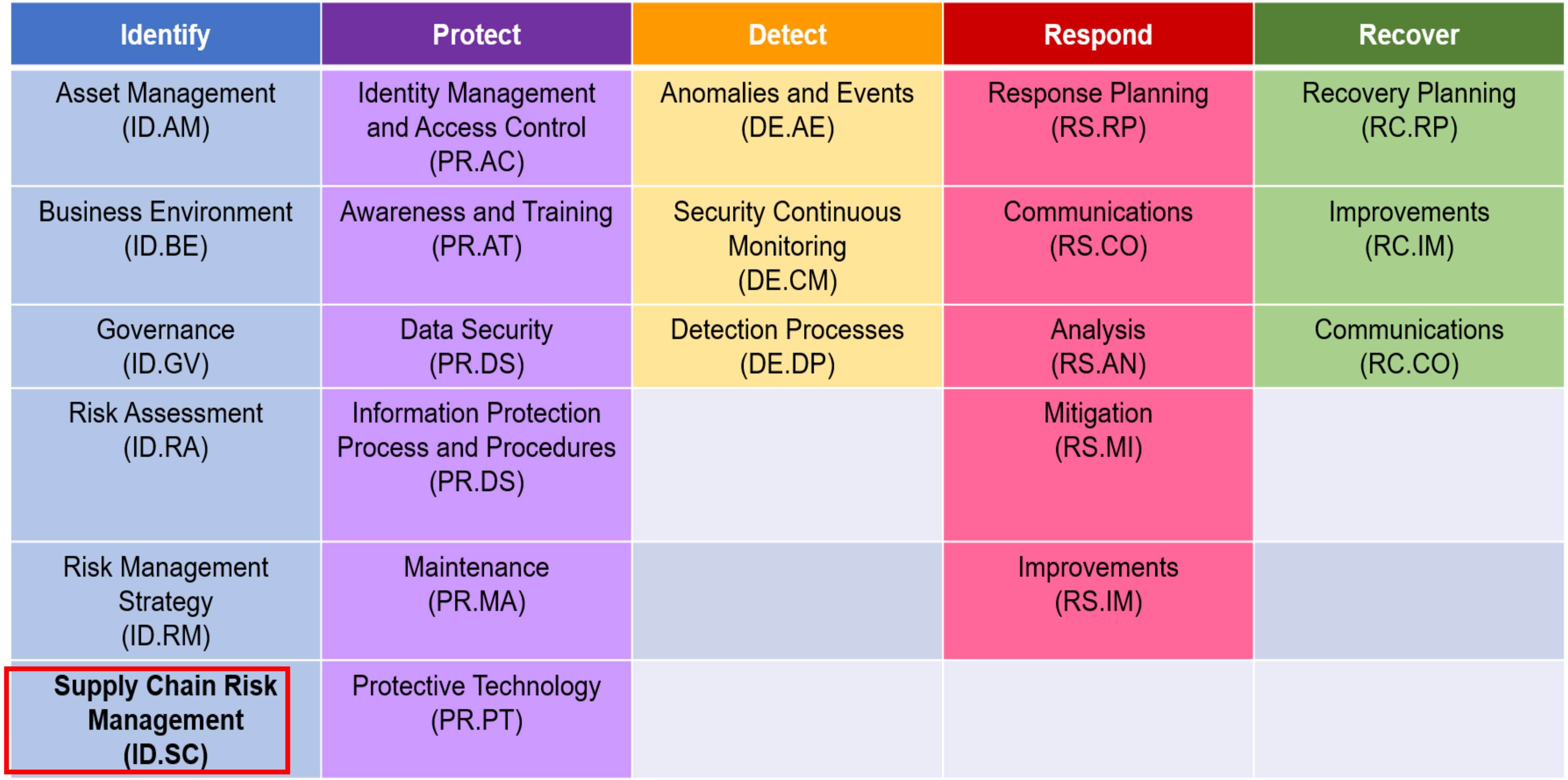
1. Embedding cyber security into your structure and objectives
   - Integrate cyber security into your organization's objectives and risks
   - Reflect this in your structure
   - Engage with your experts
2. Growing cyber security expertise
   - Baseline your current skills
3. Developing a positive cyber security culture
   - Lead by example
4. Establishing your baseline and identifying what you care about most
   - Work out what you care about the most

What should the board do?

5. Understanding the cyber security threat
   - Get an understanding of the threat
6. Risk management for cyber security
   - Integrate cyber security into organisational risk management processes
   - Don't make reducing risk levels the measure of success
7. Implementing effective cyber security measures
   - Get a little bit technical
8. Collaborating with suppliers and partners
   - Build cyber security into every decision
9. Planning your response to cyber incidents
   - Ensure you have a plan
   - Understand your role in incident management
   - Get involved in exercises
   - Drive a 'no blame' culture

NIST Cyber Security Framework (CSF)

The Framework Core *Functions and Categories*



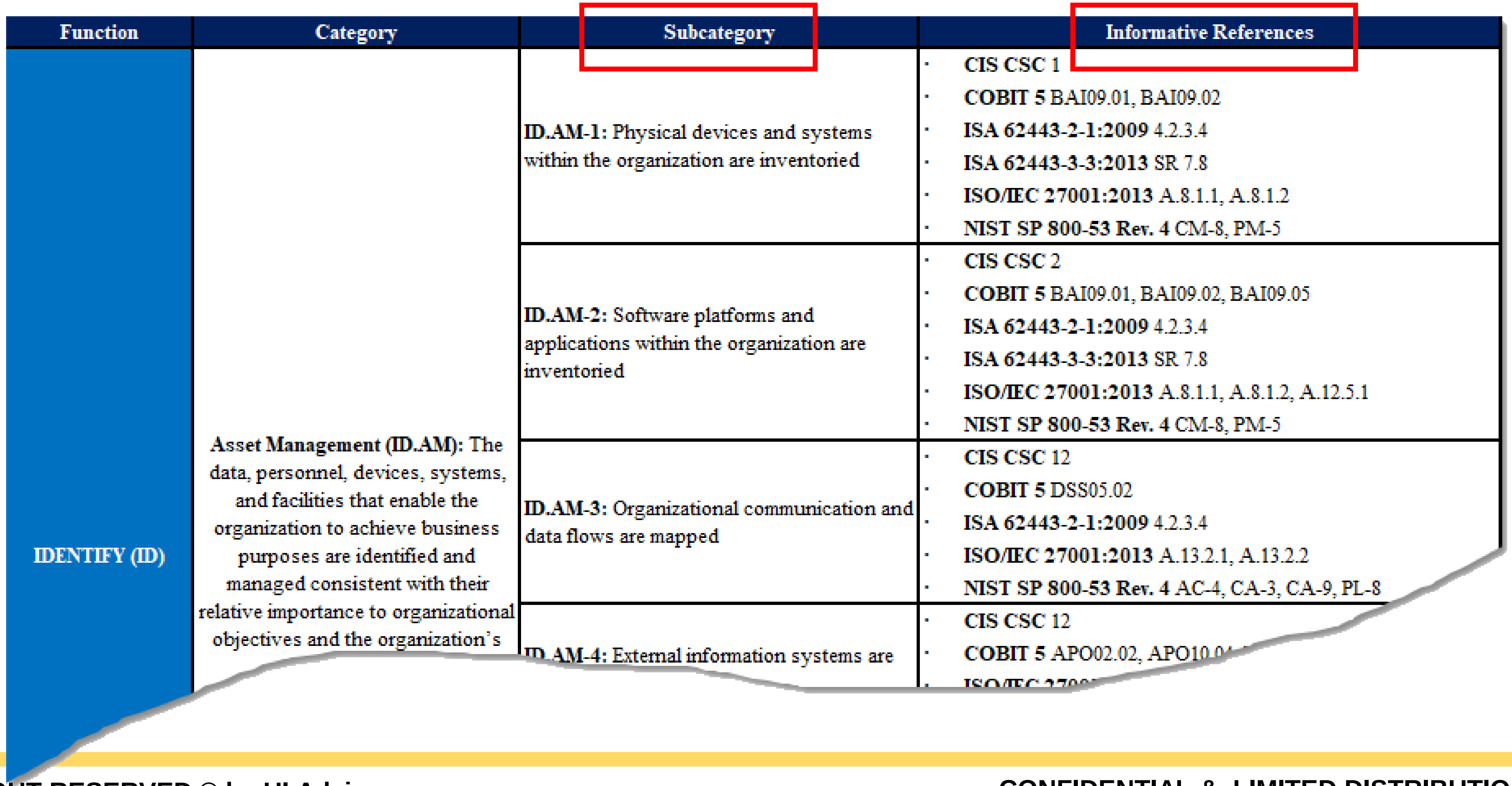
Identify	Protect	Detect	Respond	Recover
Asset Management (ID.AM)	Identity Management and Access Control (PR.AC)	Anomalies and Events (DE.AE)	Response Planning (RS.RP)	Recovery Planning (RC.RP)
Business Environment (ID.BE)	Awareness and Training (PR.AT)	Security Continuous Monitoring (DE.CM)	Communications (RS.CO)	Improvements (RC.IM)
Governance (ID.GV)	Data Security (PR.DS)	Detection Processes (DE.DP)	Analysis (RS.AN)	Communications (RC.CO)
Risk Assessment (ID.RA)	Information Protection Process and Procedures (PR.DS)		Mitigation (RS.MI)	
Risk Management Strategy (ID.RM)	Maintenance (PR.MA)		Improvements (RS.IM)	
Supply Chain Risk Management (ID.SC)	Protective Technology (PR.PT)			

NIST Cyber Security Framework (CSF)

Framework core has attributes “Category”, “Subcategory” and “Informative References”

Subcategory=Expected outcome

Informative References=References to Standards



Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s	**ID.AM-1:** Physical devices and systems within the organization are inventoried	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	· **CIS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 · **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	· **CIS CSC** 12 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are	· **CIS CSC** 12 · **COBIT 5** APO02.02, APO10.0 · **ISO/IEC 2700**

KEBIJAKAN TERKAIT
PENGAMANAN DATA PRIBADI

UU No.36 Th.2009 Ttg Kesehatan

UU No.11 Th. 2008 Ttg ITE

UU No. 29 th 2004 Ttg Praktek Kedokteran

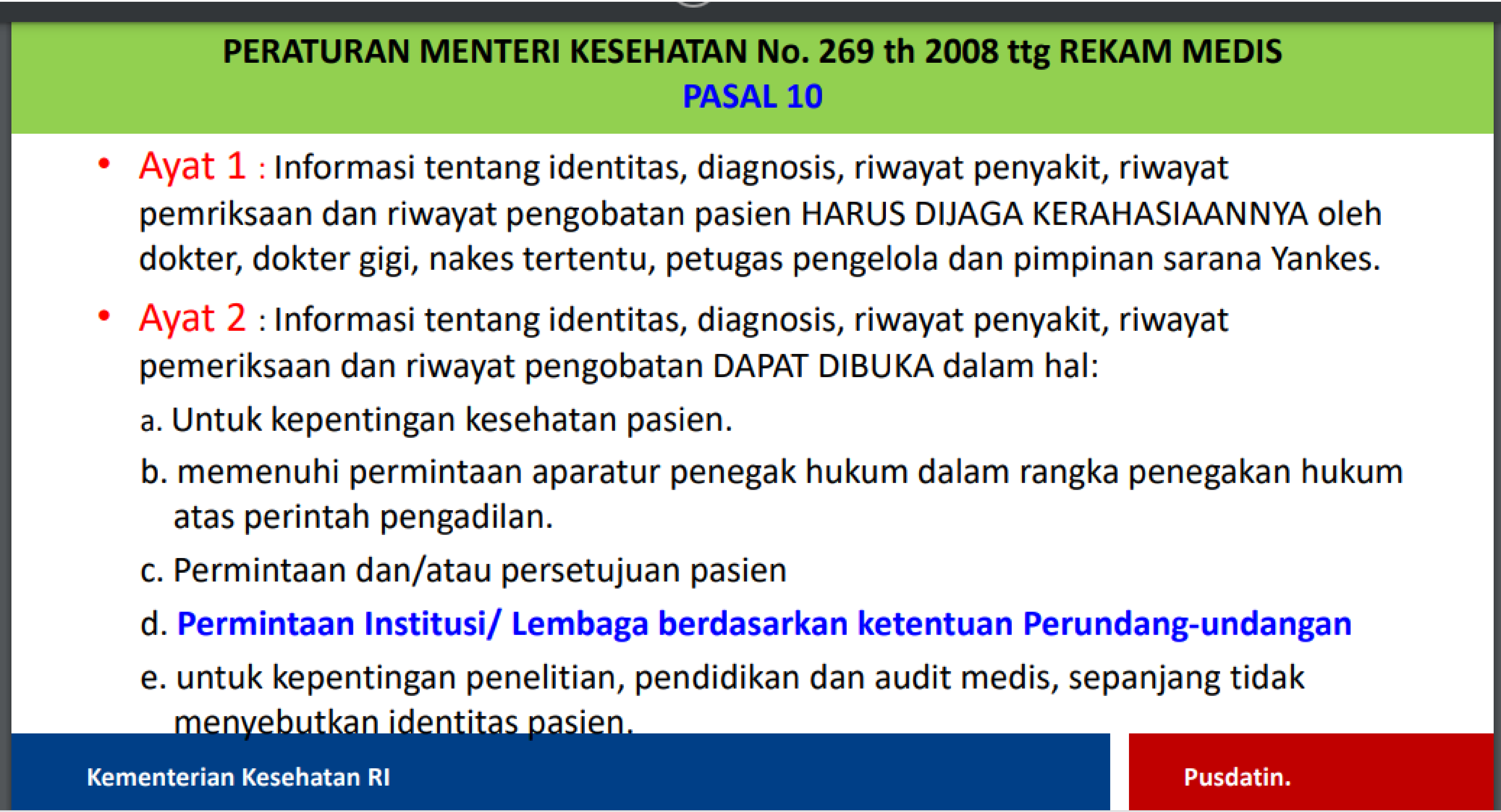
PP no. 71 th 2019 Ttg PSTE

Permenkominfo 20 /2016 Ttg Perlindungan Data Pribadi Dalam Sistem Elektronik

Permenkes No.1 th 2015 ttg Informasi yang dikecualikan

Permenkes No.269 Th 2008 ttg REKAM MEDIS

ISO/IEC 27002 Tahun 2007 Ttg Manajemen Keamanan Informasi



PERATURAN MENTERI KESEHATAN No. 269 th 2008 ttg REKAM MEDIS

PASAL 10

- Ayat 1 : Informasi tentang identitas, diagnosis, riwayat penyakit, riwayat pemriksaan dan riwayat pengobatan pasien HARUS DIJAGA KERAHASIAANNYA oleh dokter, dokter gigi, nakes tertentu, petugas pengelola dan pimpinan sarana Yankes.
- Ayat 2 : Informasi tentang identitas, diagnosis, riwayat penyakit, riwayat pemeriksaan dan riwayat pengobatan DAPAT DIBUKA dalam hal:

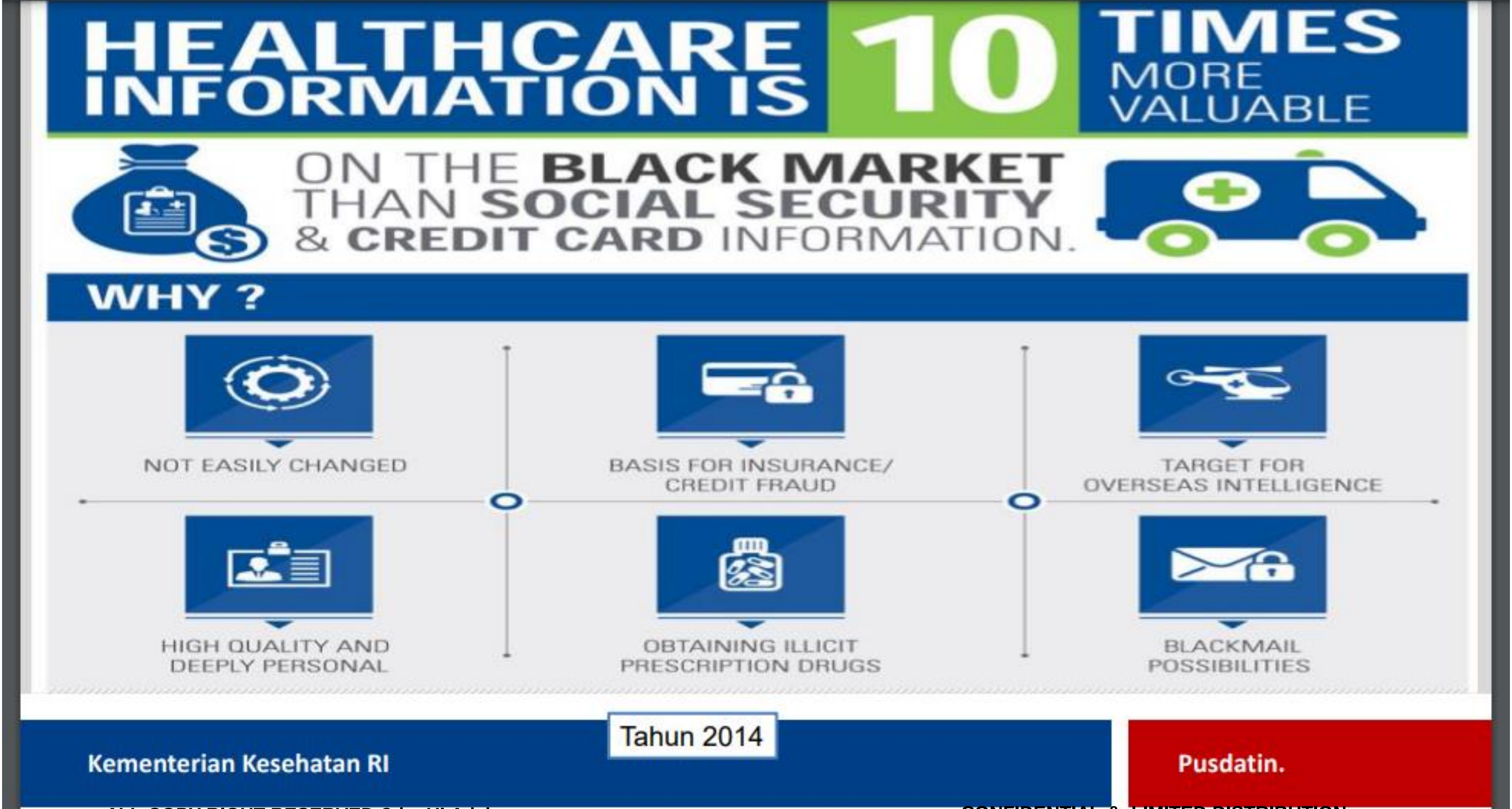
  a. Untuk kepentingan kesehatan pasien.

  b. memenuhi permintaan aparatur penegak hukum dalam rangka penegakan hukum atas perintah pengadilan.

  c. Permintaan dan/atau persetujuan pasien

  d. **Permintaan Institusi/ Lembaga berdasarkan ketentuan Perundang-undangan**

  e. untuk kepentingan penelitian, pendidikan dan audit medis, sepanjang tidak menyebutkan identitas pasien.



HEALTHCARE INFORMATION IS 10 TIMES MORE VALUABLE

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

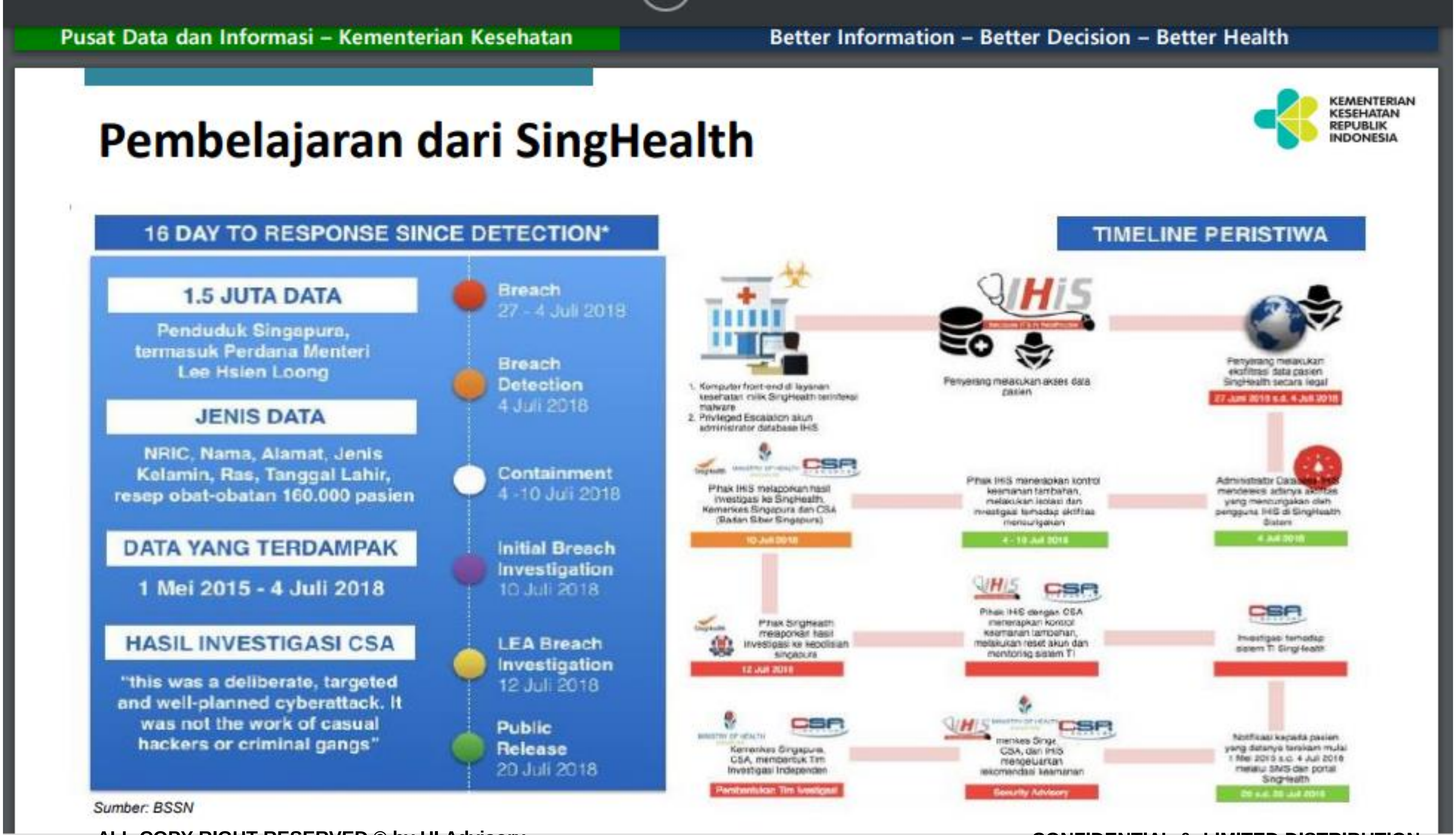
WHY ?

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

Tahun 2014

Kementerian Kesehatan RI

Pusdatin.



Pusat Data dan Informasi – Kementerian Kesehatan

Better Information – Better Decision – Better Health

KEMENTERIAN KESEHATAN REPUBLIK INDONESIA

Pembelajaran dari SingHealth

16 DAY TO RESPONSE SINCE DETECTION*

1.5 JUTA DATA

Penduduk Singapura, termasuk Perdana Menteri Lee Hsien Loong

JENIS DATA

NRIC, Nama, Alamat, Jenis Kelamin, Ras, Tanggal Lahir, resep obat-obatan 160.000 pasien

DATA YANG TERDAMPAK

1 Mei 2015 - 4 Juli 2018

HASIL INVESTIGASI CSA

"this was a deliberate, targeted and well-planned cyberattack. It was not the work of casual hackers or criminal gangs"

- Breach 27 - 4 Juli 2018
- Breach Detection 4 Juli 2018
- Containment 4 -10 Juli 2018
- Initial Breach Investigation 10 Juli 2018
- LEA Breach Investigation 12 Juli 2018
- Public Release 20 Juli 2018

Sumber: BSSN

TIMELINE PERISTIWA

1. Komputer front-end di layanan kesehatan milik SingHealth terinfeksi malware
2. Privileged Escalation akun administrator database IHiS

Penyerang melakukan akses data pasien

Penyerang melakukan ekfiltrasi data pasien SingHealth secara legal

27 Juni 2018 s.d. 4 Juli 2018

Administrator Database IHiS mendeteksi adanya aktifitas yang mencurigakan oleh pengguna IHiS di SingHealth Sistem

4 Juli 2018

Pihak IHiS menerapkan kontrol keamanan tambahan, melakukan isolasi dan investigasi terhadap aktifitas mencurigakan

4 - 10 Juli 2018

Pihak IHiS melaporkan hasil investigasi ke SingHealth, Kemenkes Singapura dan CSA (Badan Siber Singapura)

10 Juli 2018

Pihak SingHealth melaporkan hasil investigasi ke kepolisian singapura

12 Juli 2018

Pihak IHiS dengan CSA menerapkan kontrol keamanan tambahan, melakukan reset akun dan monitoring sistem TI

Investigasi terhadap sistem TI SingHealth

Notifikasi kepada pasien yang datanya terekam mulai 1 Mei 2015 s.d. 4 Juli 2018 melalui SMS dan portal SingHealth

26 s.d. 30 Juli 2018

menkes Singa. CSA, dan IHiS mengeluarkan rekomendasi keamanan

Security Advisory

Kemenkes Singapura, CSA, membentuk Tim Investigasi Independen

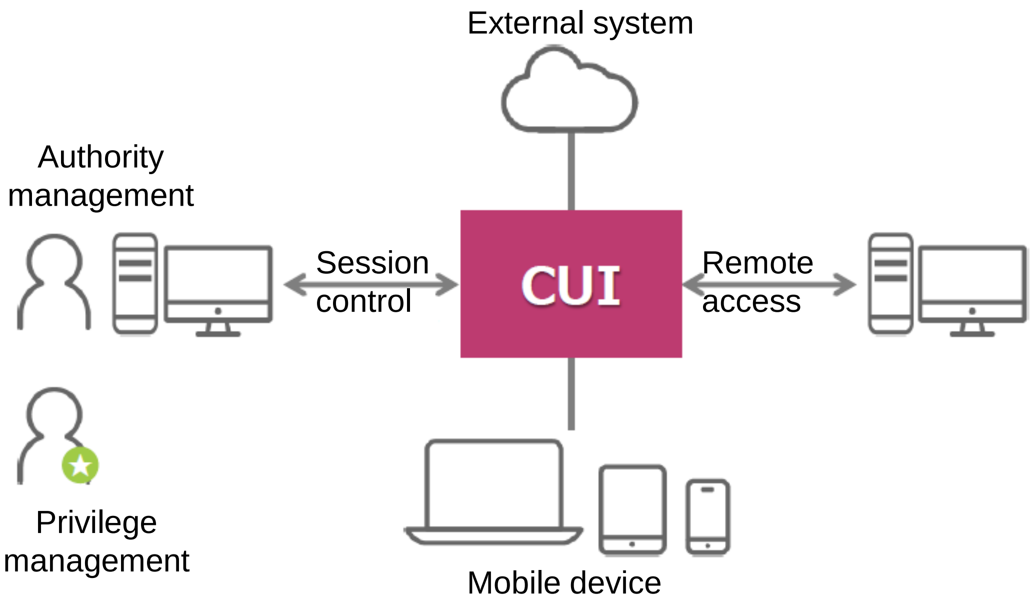
Pembentukan Tim Investigasi

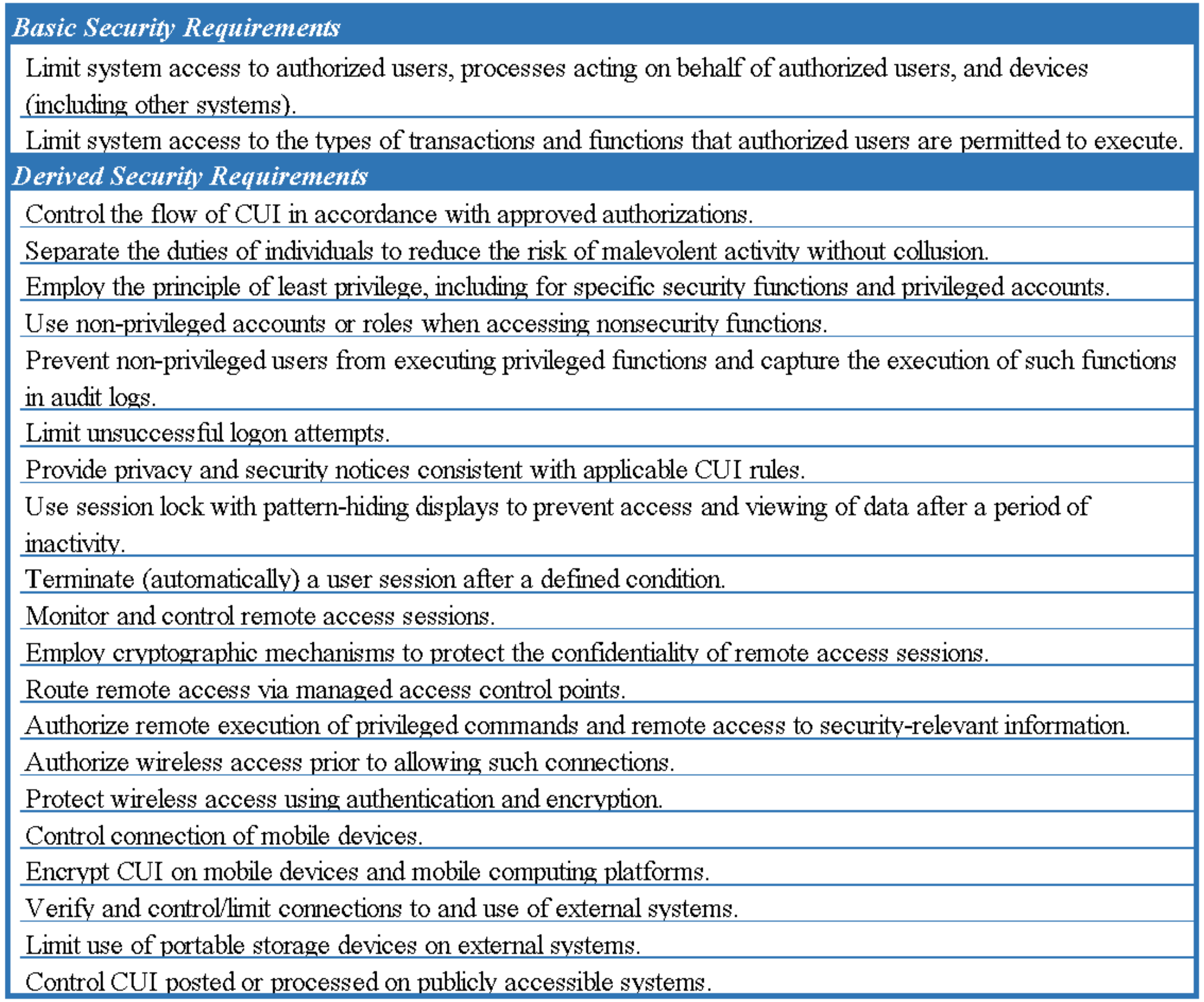
Security Strengthening Solution

Securing Access Control

Restrict persons / functions to access CUI

Stipulate controls who can access the CUI and how to access the CUI from the perspectives of authority management, session control, remote access, privilege management, mobile devices, external systems, etc.





Basic Security Requirements
Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
Limit system access to the types of transactions and functions that authorized users are permitted to execute.
Derived Security Requirements
Control the flow of CUI in accordance with approved authorizations.
Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
Employ the principle of least privilege, including for specific security functions and privileged accounts.
Use non-privileged accounts or roles when accessing nonsecurity functions.
Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.
Limit unsuccessful logon attempts.
Provide privacy and security notices consistent with applicable CUI rules.
Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.
Terminate (automatically) a user session after a defined condition.
Monitor and control remote access sessions.
Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
Route remote access via managed access control points.
Authorize remote execution of privileged commands and remote access to security-relevant information.
Authorize wireless access prior to allowing such connections.
Protect wireless access using authentication and encryption.
Control connection of mobile devices.
Encrypt CUI on mobile devices and mobile computing platforms.
Verify and control/limit connections to and use of external systems.
Limit use of portable storage devices on external systems.
Control CUI posted or processed on publicly accessible systems.

OTP Authentication (“ Security Box “ + OTP)

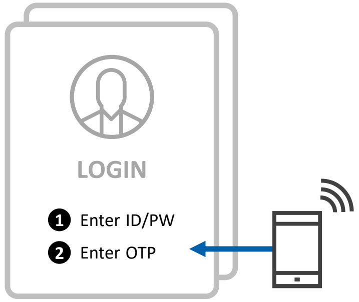
SECURITY SOFTWARE ENGINEERING DESIGN BY AiCI TEAM

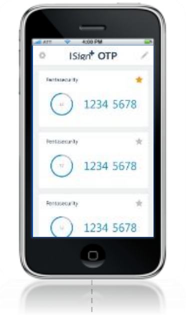
Secure authentication OTP

- Two factor authentication with in-house mobile OTP for SSO integrated business application
- External OTP (e.g., smart card, usb token) device integration

Multi factor authentication (ID/PW + OTP)

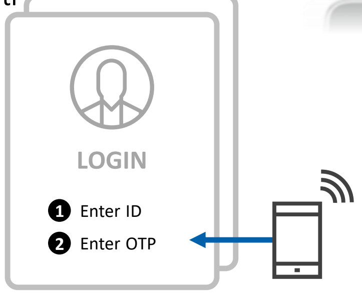
- **Benefit**
  - ✓ Prevents illegal login by leakage of ID/PW
- **Case**
  1. User authentication on online game site
  2. Prevention for duplicate ID/PW login on e-learning site





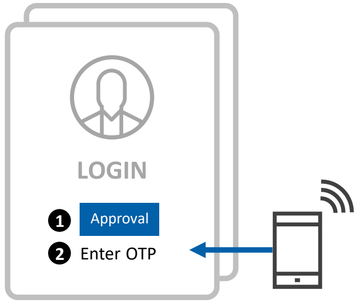
Single factor authentication (ID + OTP)

- **Benefit**
  - ✓ Prevents password replay attack
  - ✓ Security-enhancement than ID/PW
  - ✓ Convenience-enhancement than multi -factor authentication
- **Case**
  1. ID/PW leakage prevention



Additional authentication feature (for approval process)

- **Benefit**
  - ✓ Prevents illegal approval by unauthorized user
- **Case**
  1. Business approval
  2. Payment approval on e-commerce



THANK YOU

ALL COPY RIGHT RESERVED ©

CONFIDENTIAL & LIMITED DISTRIBUTION