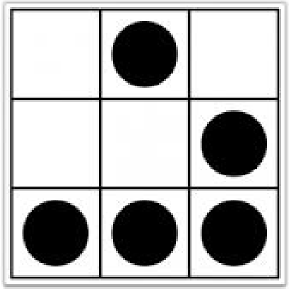
Data Privacy & Security

The New Reality

Executive Briefing for CISA, CISM, CRISC Program
@Binus FX

25 Sept 2018

Eryk Budi Pratama



Agenda

01 Cyber Attack Landscape

02 Data Privacy & Protection Regulation

03 Case Study

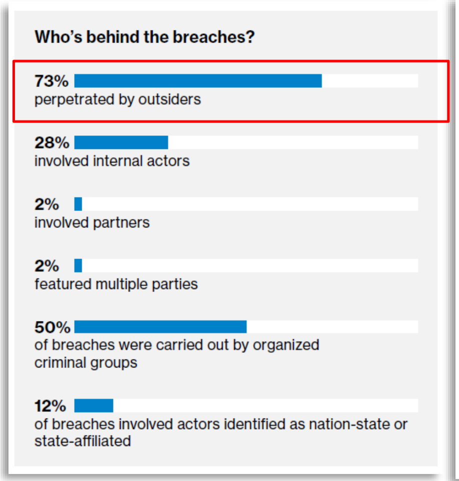
Cyber Attack Landscape

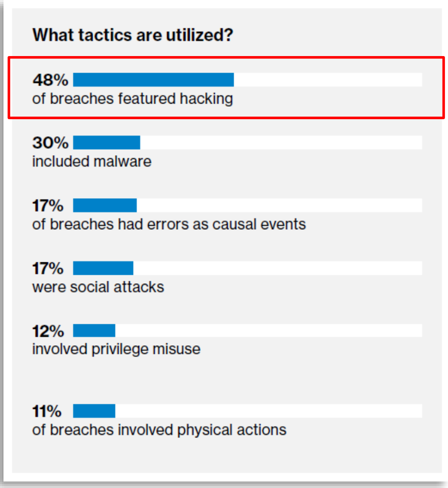
Data Breach Report

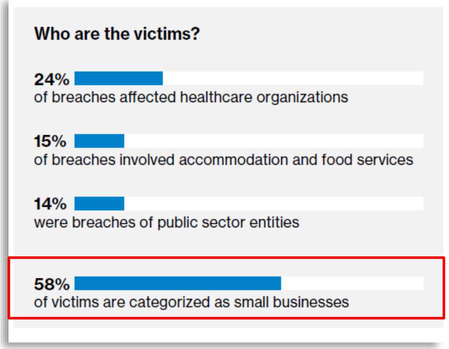
Every year, the incident response team at Verizon Enterprise Solutions releases their highly-anticipated Data Breach Investigations Report (DBIR), providing a wealth of data on real-world security incidents, data breaches, and the trends driving both.

Ransomware is the most common type of malware, found in 39 percent of malware-related data breaches – double that of last year's DBIR – and accounts for more than 700 incidents.

There is a shift in how social attacks, such as financial **pretexting** and **phishing** are used. Attacks such as these, which continue to infiltrate organizations via employees, are now increasingly a departmental issue.







> *"Businesses find it difficult to keep abreast of the threat landscape, and continue to put themselves at risk by not adopting dynamic and proactive security strategies"*

Source: Verizon Data Breach Investigation Report 2018

Data Breach Report - Major Finding

Ransomware is the most prevalent variety of malicious software

It was found in **39 percent** of malware- related cases examined this year, moving up from fourth place in the 2017 DBIR (and 22nd in 2014).

The human factor continues to be a key weakness

Financial **pretexting** and **phishing** repre sent **98 percent** of **social incidents** a nd **93 percent** of **all breaches** investig ated – with **email** continuing to be the main entry point (96 percent of cases)

Phishing attacks cannot be ignored

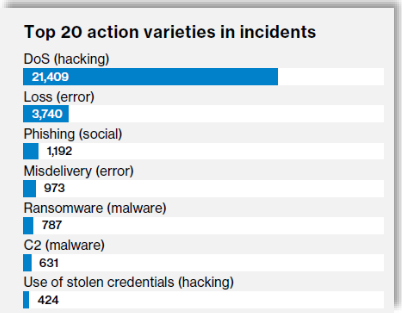
While on average 78 percent of people did not fail a phishing test last year, **4 percent** of people do for any given phishing campaign

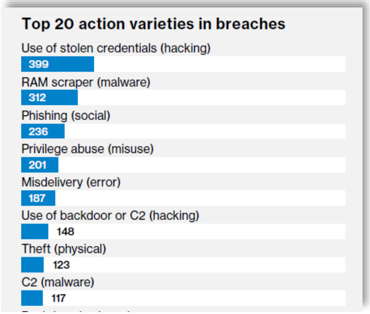
DDoS attacks are everywhere

DDoS attacks can impact anyone and a re often used as camouflage, often being started, stopped and restarted to hide other breaches in progress.

Top 5 Industries

- ❑ Healthcare
- ❑ Accommodation
- ❑ Public
- ❑ Retail
- ❑ Finance





"Cybercriminal only needs ***one victim*** *to get access Into an organization"*

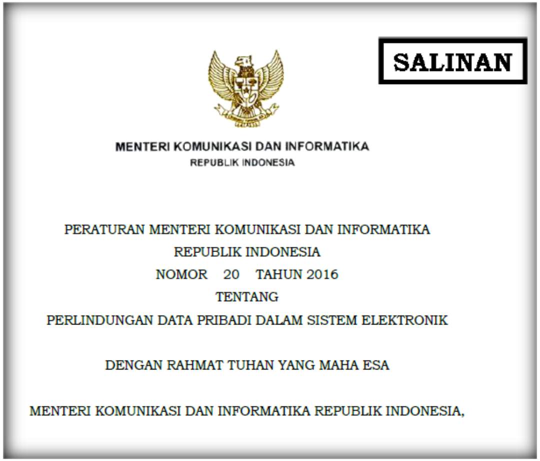
Source: Verizon Data Breach Investigation Report 2018

Cyber Attack Anatomy

Actors	Motivation	Impact to Business
STATE-SPONSORED	ESPIONAGE AND SABOTAGE : Political advantage, economic advantage, military advantage	Disruption or destruction, theft of information, reputational loss
HACKTIVISM	HACKING INSPIRED BY IDEOLOGY: Shifting allegiances – dynamic, unpredictable	Public distribution, reputation loss
THE INSIDER	INTENTIONAL OR UNINTENTIONAL: Grudge, financial gain	Distribution or destruction, theft of information, reputation loss
COMPETITORS	COMPETITION OR RIVALRY: Gain business edge	IP theft, reputation damage
ORGANISED CRIME	GLOBAL, DIFFICULT TO TRACE AND PROSECUTE: Financial advantage	Financial loss

Data Privacy & Protection Regulation

Indonesia Regulation



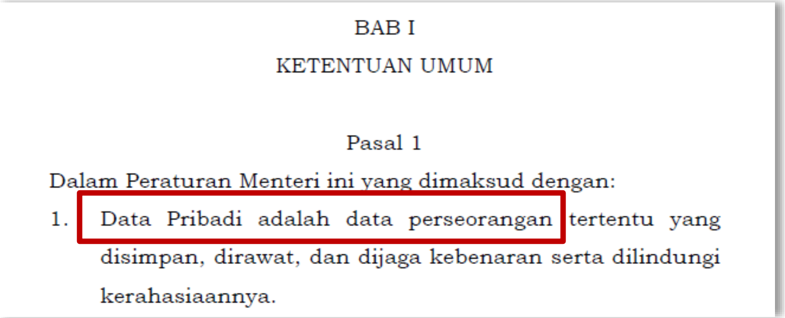
SALINAN

MENTERI KOMUNIKASI DAN INFORMATIKA
REPUBLIK INDONESIA

PERATURAN MENTERI KOMUNIKASI DAN INFORMATIKA
REPUBLIK INDONESIA
NOMOR 20 TAHUN 2016
TENTANG
PERLINDUNGAN DATA PRIBADI DALAM SISTEM ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI KOMUNIKASI DAN INFORMATIKA REPUBLIK INDONESIA,



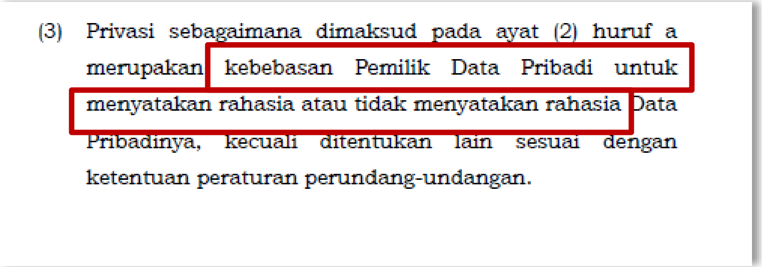
BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Menteri ini yang dimaksud dengan:

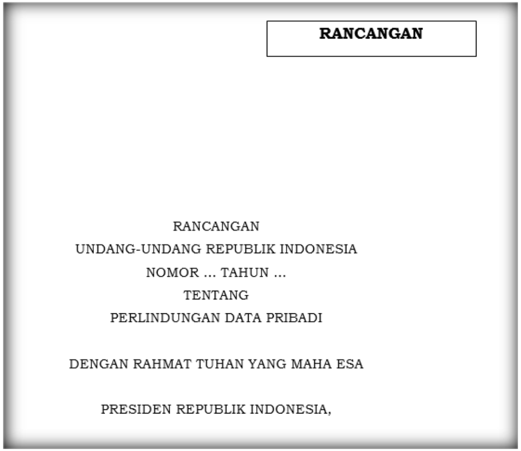
1. Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya.

Pasal 2



(3) Privasi sebagaimana dimaksud pada ayat (2) huruf a merupakan kebebasan Pemilik Data Pribadi untuk menyatakan rahasia atau tidak menyatakan rahasia Data Pribadinya, kecuali ditentukan lain sesuai dengan ketentuan peraturan perundang-undangan.

Indonesia Regulation

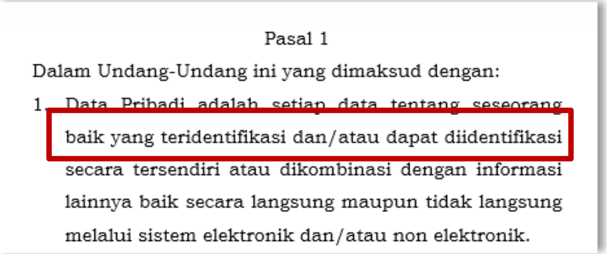


RANCANGAN

RANCANGAN
UNDANG-UNDANG REPUBLIK INDONESIA
NOMOR ... TAHUN ...
TENTANG
PERLINDUNGAN DATA PRIBADI

DENGAN RAHMAT TUHAN YANG MAHA ESA

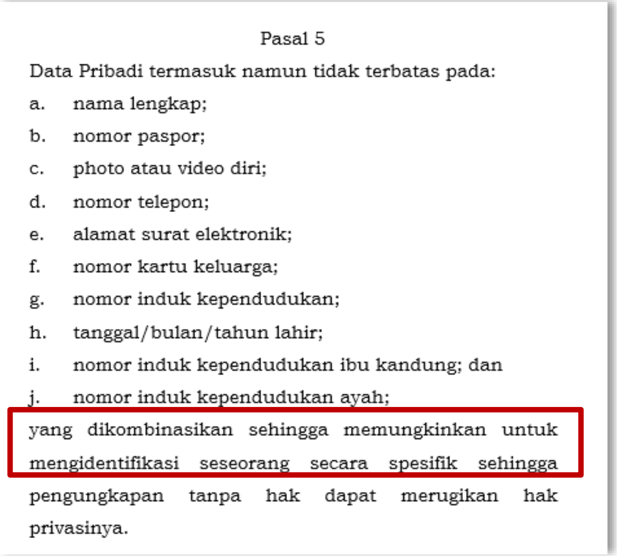
PRESIDEN REPUBLIK INDONESIA,



Pasal 1

Dalam Undang-Undang ini yang dimaksud dengan:

1. Data Pribadi adalah setiap data tentang 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.



Pasal 5

Data Pribadi termasuk namun tidak terbatas pada:

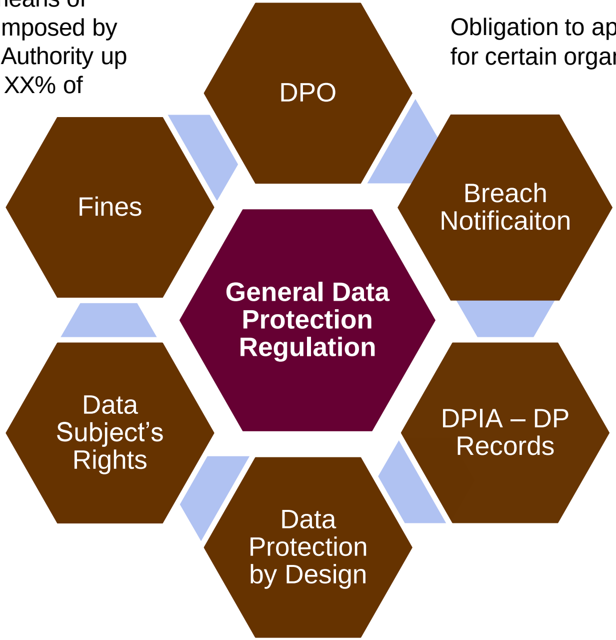
a. nama lengkap;
b. nomor paspor;
c. photo atau video diri;
d. nomor telepon;
e. alamat surat elektronik;
f. nomor kartu keluarga;
g. nomor induk kependudukan;
h. tanggal/bulan/tahun lahir;
i. nomor induk kependudukan ibu kandung; dan
j. nomor induk kependudukan ayah;

yang dikombinasikan sehingga memungkinkan untuk mengidentifikasi seseorang secara spesifik sehingga pengungkapan tanpa hak dapat merugikan hak privasinya.

Global Data Protection Regulation (GDPR)

GDPR provides [LEGAL FORM] for (administrative) fines as a means of enforcement which can be imposed by the competent Supervisory Authority up to a max. of XXmio EUR or XX% of annual worldwide turnover

Obligation to appoint a **Data Protection Officer** for certain organisations/activities



General Data Protection Regulation

DPO

Breach Notificaiton

DPIA – DP Records

Data Protection by Design

Data Subject’s Rights

Fines

Obligation to notify data breaches within **72 hours** to the competent **Supervisory Authority**.

Specific documentary obligations to identify, assess the **privacy impact of and record data processing activities** to be compliant with the GDPR and to be able to prove you are compliant. Prior consultation with the Supervisory Authority is required where the Data Protection Impact Assessment (DPIA) shows the data processing activities will result in a high risk.

Introduction of new rights for the data subject such as the right to data portability, the right to data erasure, …

Introduction of new obligations for **data controllers** and **data processors**. New principles have also been introduced including data minimisation

GDPR Data Controller vs Processor

Data Controller

The responsible party for the fair, transparent, and secure collection and use of personal information.

Example responsibilities include:

- May only collect data for explicit and legitimate purposes
- Must ensure accuracy and security
- Must provide means to rectify/ purge data
- Must respect retention and secure deletion

Data Processor

Entities that possess, manipulate, or otherwise “use” data on behalf of a data controller, but do not exercise responsibility or control over the data.

Example responsibilities include:

- Must only process data on strict instruction from the data controller
- Must maintain security to protect against unauthorized access, disclosure, or loss
- Must formally register as a processor

Joint Controller

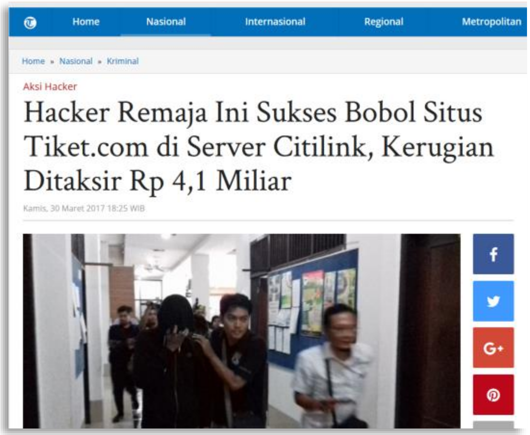
Where two or more controllers jointly determine the purposes and means of the processing of personal data, they are joint controllers.

Considerations include:

- Joint controllers must, by means of an "arrangement" between them, apportion data protection compliance responsibilities between themselves
- A summary of the arrangement must be made available for the data subject. The arrangement may designate a contact point for data subjects

Case Study

Tiket.com



Home • Nasional • Kriminal

Aksi Hacker

Hacker Remaja Ini Sukses Bobol Situs Tiket.com di Server Citilink, Kerugian Ditaksir Rp 4,1 Miliar

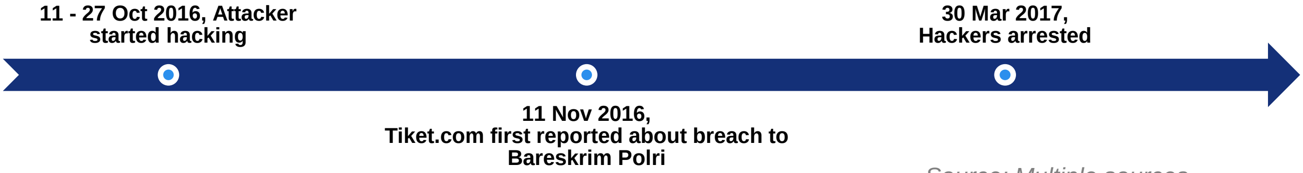
Kamis, 30 Maret 2017 18:25 WIB

Financial Loss: IDR 6,1 Billion

Summary

- Attacker 1: Hacked Tiket.com website and successfully obtain **username** and **password** of Tiket.com account
- Attacker 1: Login to Citilink server using stolen Tiket.com credential to obtain **booking code** of Citilink tickets
- Attacker 2: Enter Citilink flight ticket order data from the buyer, then the data is entered into the Citilink airline sales application
- Attacker 3: Find other potential buyers using Facebook; all buyers data forwarded to Attacker 2 to be submitted into Citilink sales application

Timeline



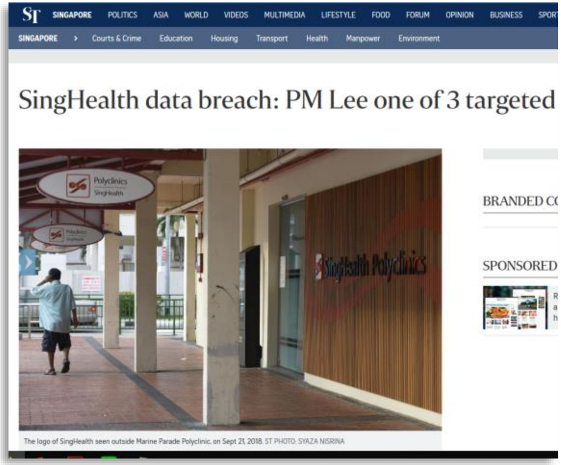
11 - 27 Oct 2016, Attacker started hacking

11 Nov 2016, Tiket.com first reported about breach to Bareskrim Polri

30 Mar 2017, Hackers arrested

Source: Multiple sources

SingHealth



SingHealth data breach: PM Lee one of 3 targeted

The logo of SingHealth seen outside Marine Parade Polyclinic, on Sept 21, 2018. ST PHOTO: SYAZA NISRINA

Data Loss: 1,5 Million patients' records

Summary

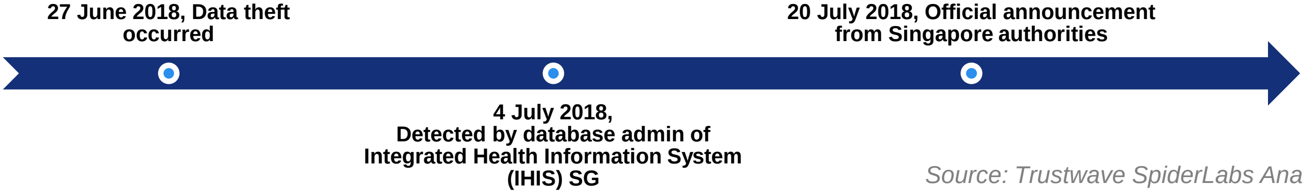
SingHealth was targeted by a major cyber-attack, resulting in a breach which affected about **1.5 million patients' records**. The breach was described as unprecedented in scale and the **most serious breach** of **personal data** in the history of Singapore.

This breach affects **PII data** for patients that visited SingHealth's specialist outpatient clinics and polyclinics from May 1st 2015 to July 4th The stolen records included **patient's name**, **address**, **gender**, **race**, **date of birth** and **National Registration Identity Card (NRIC) number**. The medical prescription records of 160,000 patients were also stolen

The cyber-attack was reported as **deliberate**, **well-planned**, and **targeted** Singapore's Prime Minister's medical records repeatedly

Potential attack actor:
Advanced adversarial groups mostly which operates within a region in Asia

Timeline

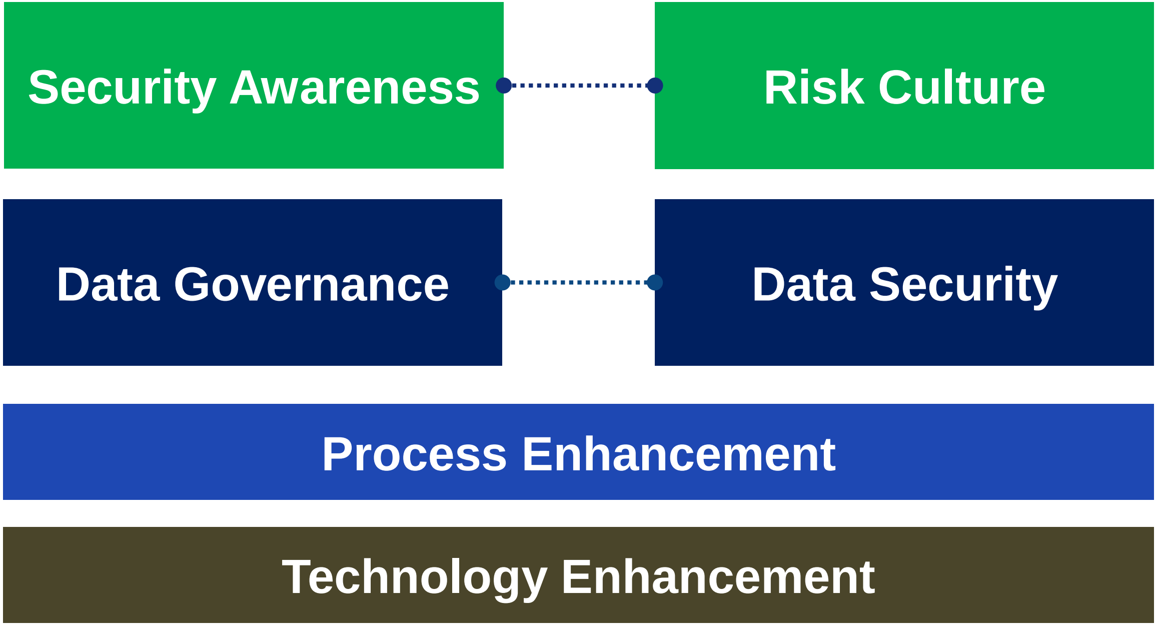

27 June 2018, Data theft occurred

4 July 2018,
Detected by database admin of Integrated Health Information System (IHIS) SG

20 July 2018, Official announcement from Singapore authorities

Source: Trustwave SpiderLabs Analysis

Lesson Learned



Security Awareness

Risk Culture

Data Governance

Data Security

Process Enhancement

Technology Enhancement

“Humans are (still) the weakest cybersecurity link “

Thank You

eryk.pratama@gmail.com

https://proferyk.blogspot.co.id