



BADAN SIBER DAN  
SANDI NEGARA

# KEAMANAN SPBE PADA TRANSFORMASI DIGITAL

**Aris Munandar**  
Direktorat Keamanan Siber dan Sandi Pemerintah Daerah

# OVERVIEW REVOLUSI



– 18th Century

## Industry 1.0

Produksi secara mekanis dengan peralatan bertenaga uap dan air



19th Century

## Industry 2.0

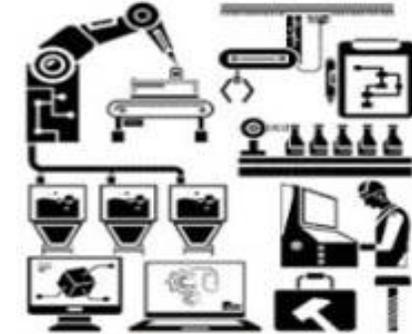
Produksi massal dengan model perakitan yang butuh tenaga kerja dan listrik



20th Century

## Industry 3.0

Produksi otomatis menggunakan teknologi IT dan elektronik



Today

## Industry 4.0/5.0/Digital Transform

Produksi dengan teknologi cerdas berbasis internet, cloud dan Big Data, AI

## Teknologi Digital Pendorong Revolusi



Internet of Things



Cloud Computing



Augmented Reality/  
Wearable Device



Big Data



Autonomous Robots  
& Smart Sensor

*Kita sepakati bahwa Transformasi Digital terkait erat dengan :*

***Smart Manufacturing dan Internet of Things (IoT) serta Big Data Serta AI***

# TANTANGAN TRANSFORMASI DIGITAL

## TECHNICAL CHALLENGE

## CLASSIC CHALLENGE

**Interoperability, Orchestration and Automation**



**The Indonesian Government**



**Customer understanding**

**Data Processing**



**Digital Transformation Challenges**



**Cultural and Organizational Change :**

- Siloed initiatives
- Many applications
- Internal resistance to change

**Cyber Security Risks**



**Budget constraints**



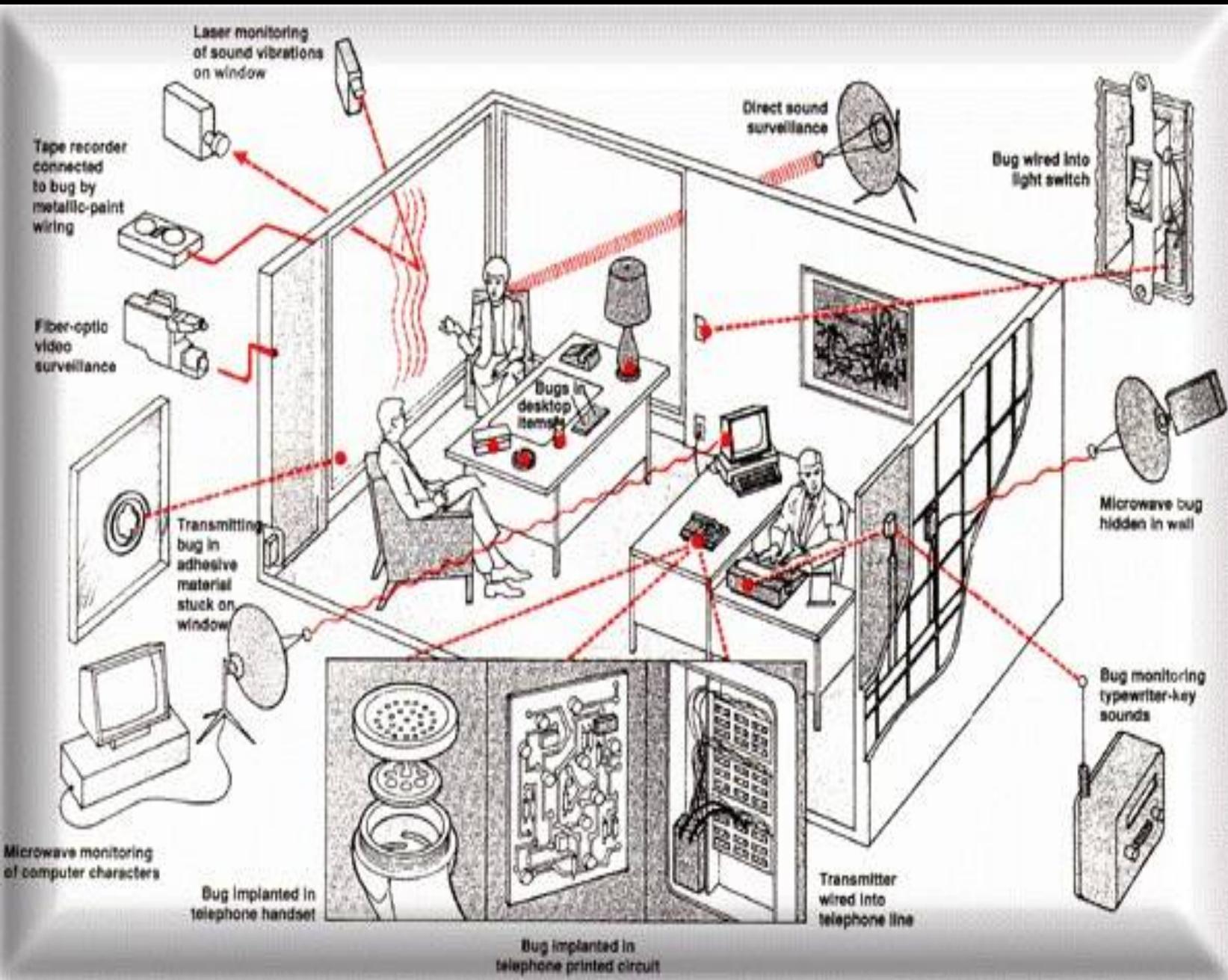


“Kita harus siaga menghadapi ancaman **kejahatan siber**, termasuk kejahatan penyalahgunaan data. **Data/Informasi** adalah jenis kekayaan baru bangsa kita, kini data lebih berharga dari minyak... Dalam bidang pertahanan keamanan, kita juga harus tanggap dan siap menghadapi **perang siber.**”

Pidato Kenegaraan Presiden RI dalam rangka HUT ke 74  
Proklamasi Kemerdekaan RI di Depan Sidang Bersama DPD dan DPR RI  
16 Agustus 2019



# ILUSTRASI : ANCAMAN OLD VERSION – NON SPBE



## INFORMATION COLLECTION

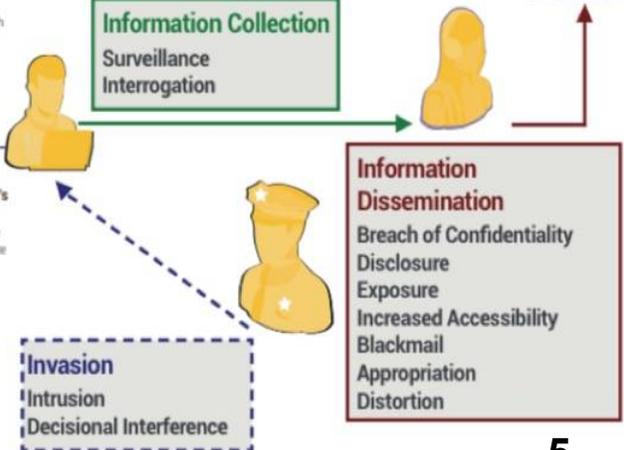
- Surveillance**  
Watching, listening to, or recording of an individual's activities  
A website monitoring cursor movements of a visitor while visiting the website.
- Interrogation**  
Questioning or probing for personal information  
An interviewer asking an inappropriate question, such as marital status, during a employment interview.

Based on Dan Solove's A Taxonomy of Privacy  
[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=667622](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622)

- Information Processing**
- Aggregation
  - Insecurity
  - Identification
  - Secondary Use
  - Exclusion

## INVASION

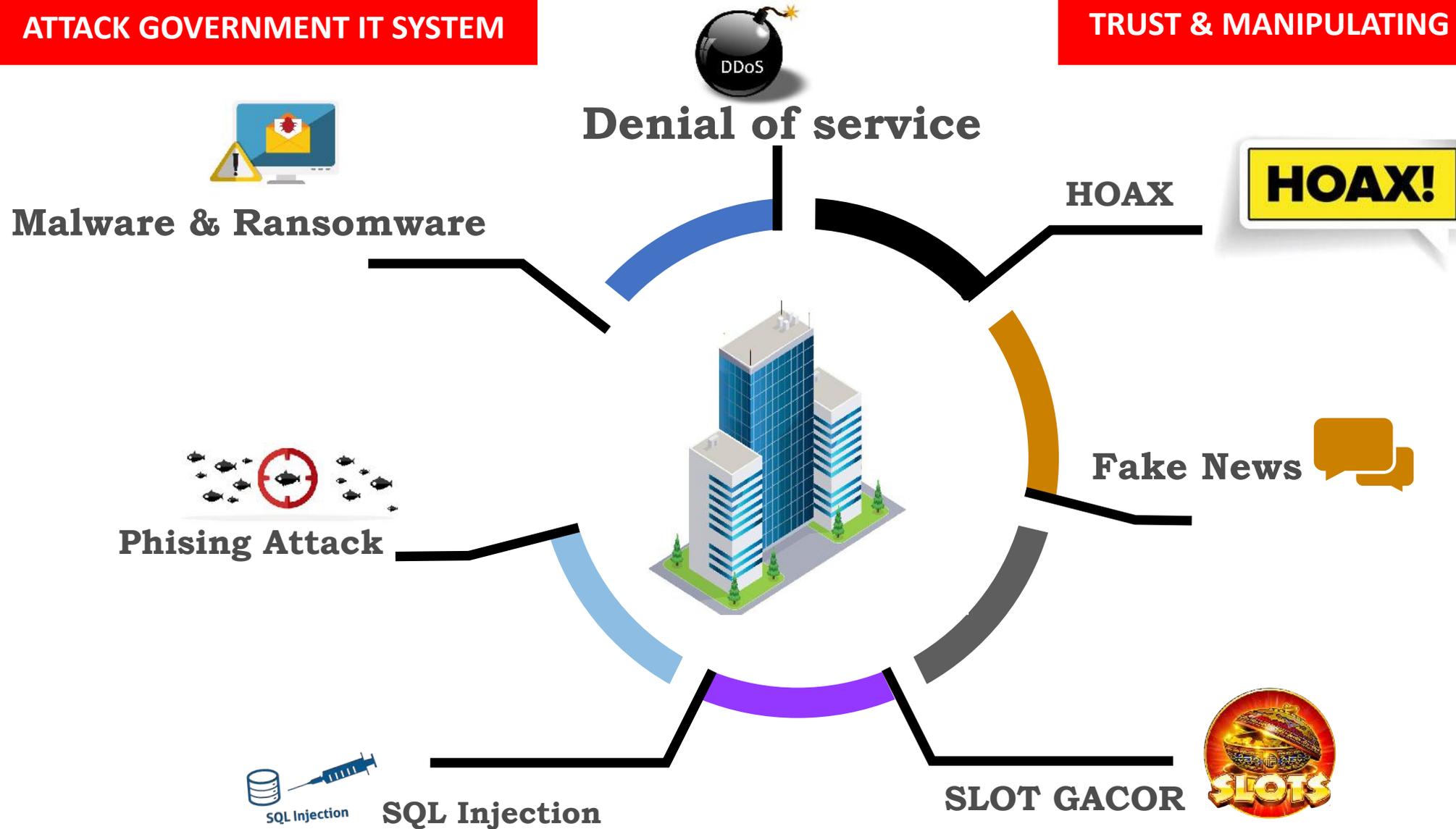
- Intrusion**  
Disturbing an individual's tranquility or solitude  
An augmented reality game directing players onto private residential property
- Decisional Interference**  
Intruding into an individual's decision regarding their private affairs  
A payment processor deciding transactions for contraceptives.



# ANCAMAN ERA TRANSFORMASI DIGITAL

ATTACK GOVERNMENT IT SYSTEM

TRUST & MANIPULATING PUBLIC OPINION



# SERANGAN SIBER BERSIFAT TEKNIS

Menyerang Lapisan Jaringan Logika melalui metode teknis yang intrusif dengan tujuan mendapatkan akses ilegal, ke dalam jaringan dan sistem pihak sasaran guna menghancurkan, mengubah, mencuri, dan memasukkan informasi

## TEKNIK



WEB  
DEFACEMENT



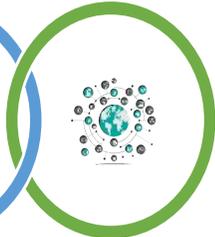
PHISHING



SQL  
INJECTION



BRUTE  
FORCE  
ATTACK



MALWARE  
ATTACK  
(Ransomware)



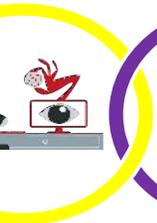
DOS dan  
DDoS



MAN IN THE  
MIDDLE  
ATTACK



CROSS SITE  
SCRIPTING



DNS (Domain  
Name Server)  
ATTACK



# What kind of information a phisher steals

Mailing addresses



ID number



Location and contact details



**Personal data**

Credit card number



Number of accounts



E-commerce information



**Financial information**

Social media



Email accounts



**Access credentials**



**Main means of propagation**



Malware infection



Social media



Telephone calls



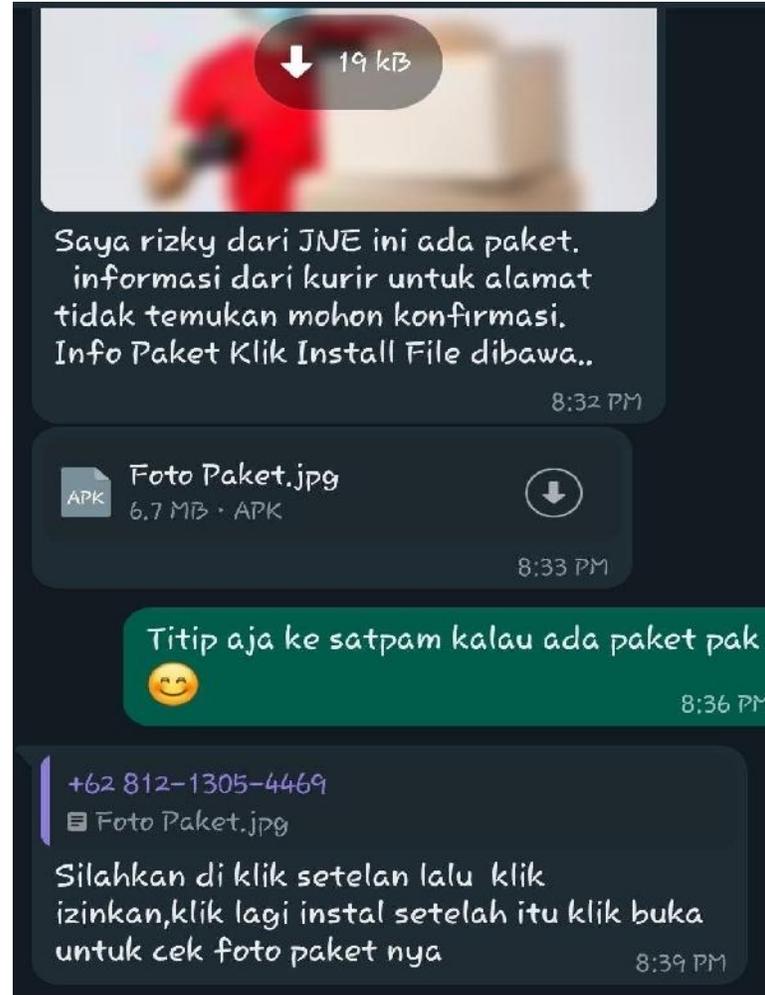
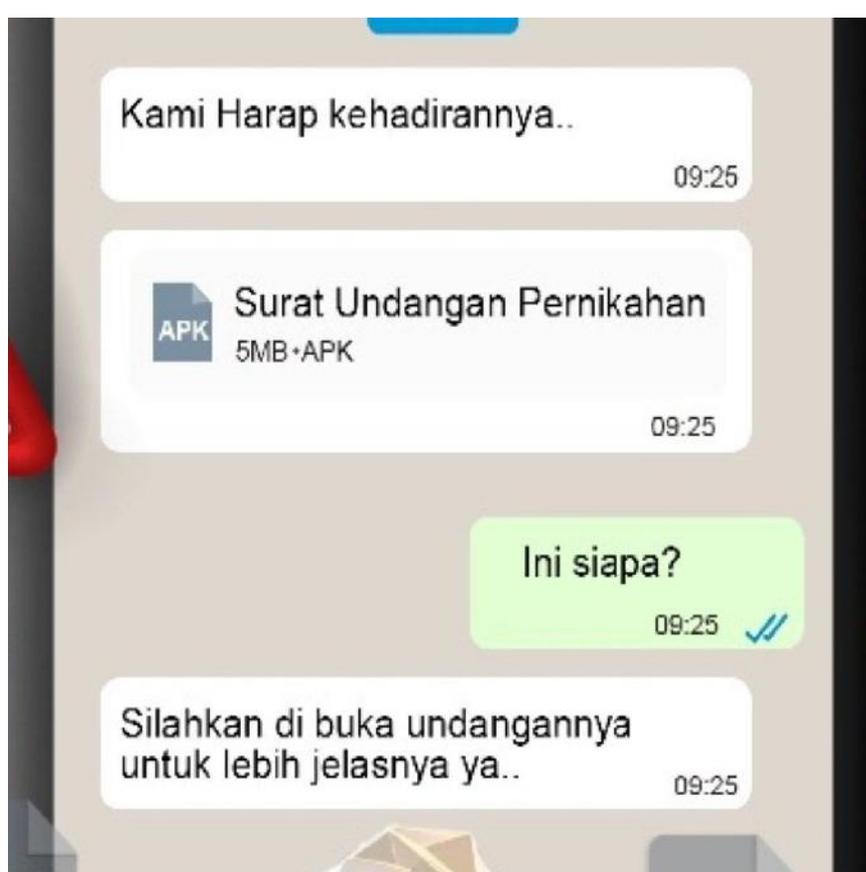
SMS/MMS



E-mail address

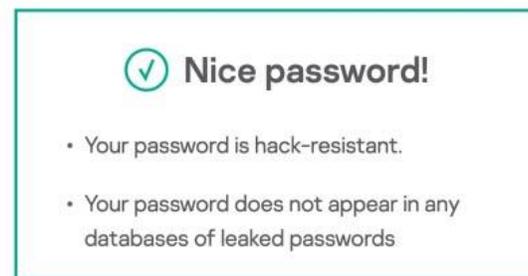
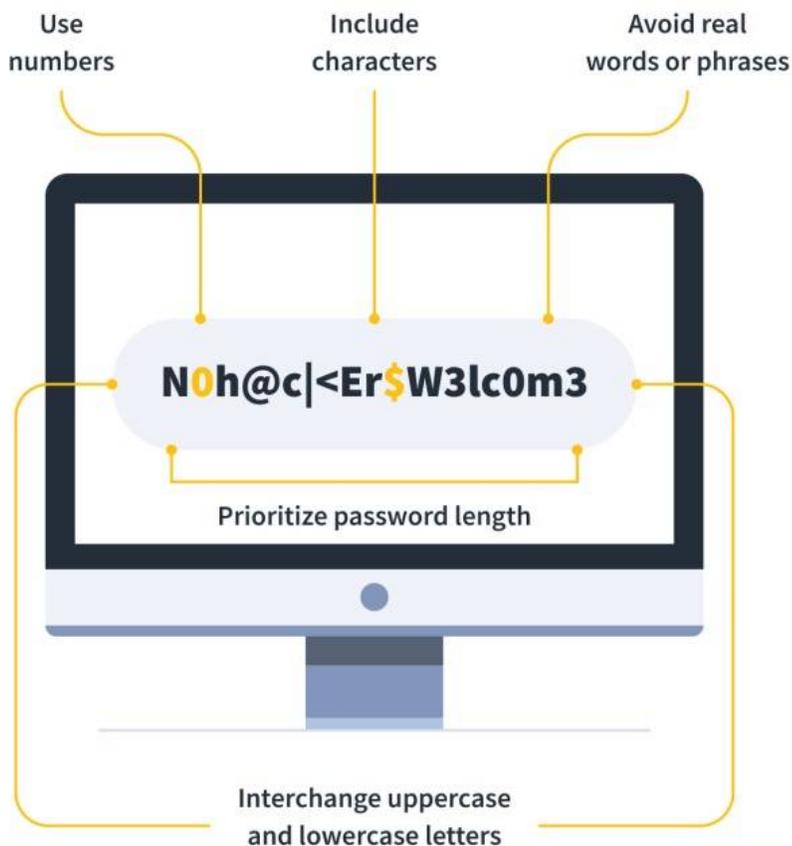
# Contoh 1 Kejahatan Phishing

## 2. Dipadukan dengan teknik Social Engineering



# Pencegahan Phishing

- Menggunakan password unik untuk setiap aplikasi, memenuhi kriteria strong password dan mengupdate password secara berkala



Your password will be bruteforced with an average home computer in approximately...

10 years



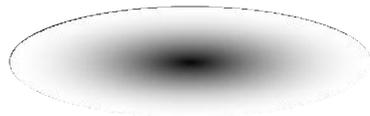
# Pencegahan Phishing

- Menerapkan Multi-FA untuk login pada layanan aplikasi tertentu



# Kebocoran Data

Ilustrasi, Potensi kebocoran informasi dari Ruang Siber atau Platform Media



## What Google Knows

Google compiles enough data to build comprehensive portfolios of most users—who they are, where they go and what they do—and the information is all available at [google.com/dashboard](http://google.com/dashboard). Here are just a few things WSJ reporter Tom Gara found out about himself.

### GOOGLE SEARCH 64,019

Google thinks Tom performs most of his searches around 8 a.m. ET, but this is probably skewed by years spent outside the U.S.

### ANDROID DEVICES 3

Google knows all of Tom's synched Android phones, including the old Nexus S phone that he gave to his mom.

### WALLET 3

Credit cards (two expired) saved in Google Wallet, plus two shipping addresses and 13 itemized purchases since June 2009.

### DOCS 855

Documents Tom has created, plus the 115 he has opened that belong to other people.

Graphic by Alberto Cervantes/  
The Wall Street Journal

### GMAIL 134,966

All of Tom's emails since he first got a Gmail account in 2004. Google also stores his 6,147 chats.

### CONTACTS 2,702

Google knows the people that Tom emails the most. At the top is a friend in Egypt.

### YOUTUBE 9,220

Videos Tom has watched, listed in chronological order, including a series viewed in June about canoes.

### GOOGLE PLAY 117

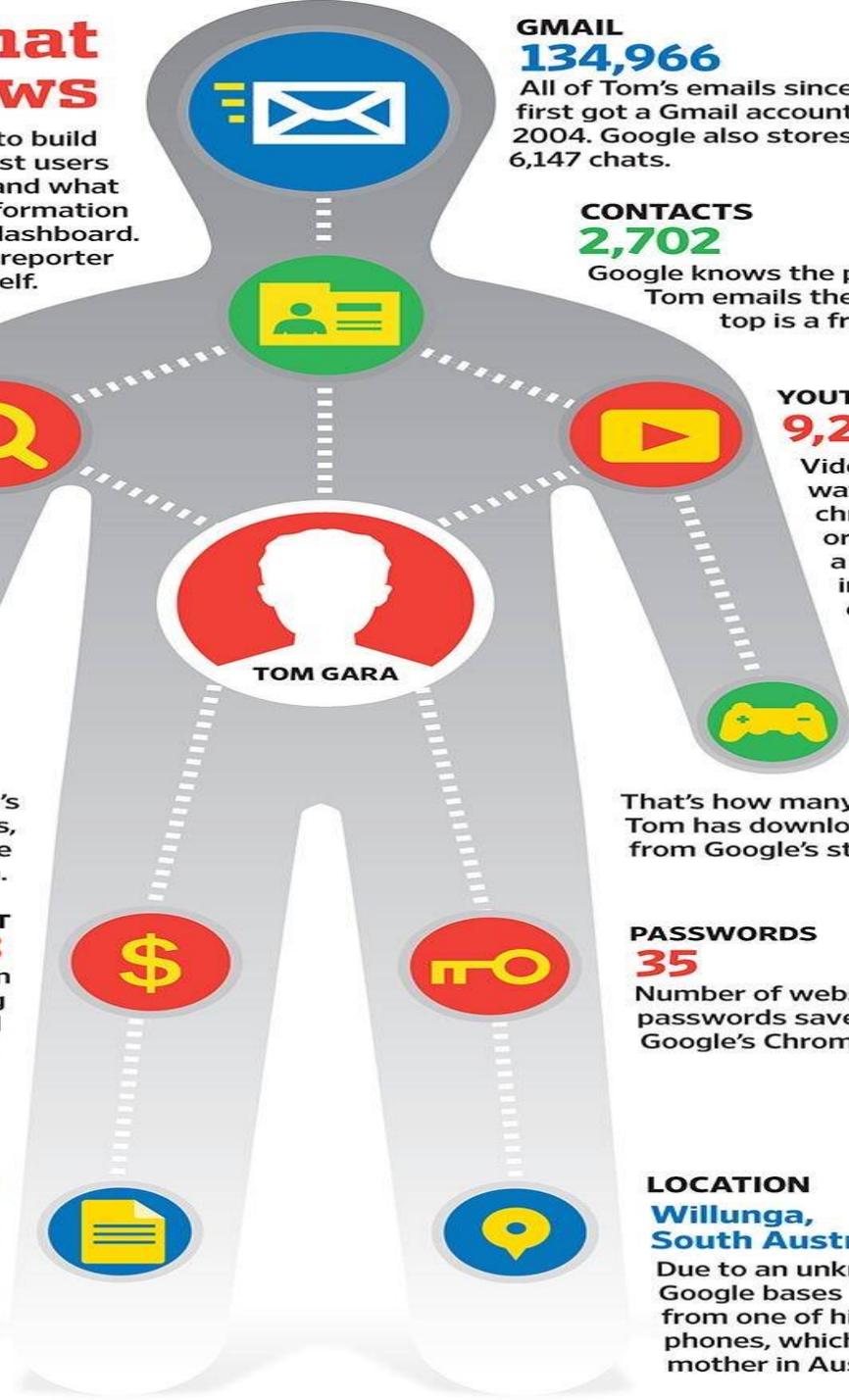
That's how many apps Tom has downloaded from Google's store.

### PASSWORDS 35

Number of website passwords saved in Google's Chrome browser.

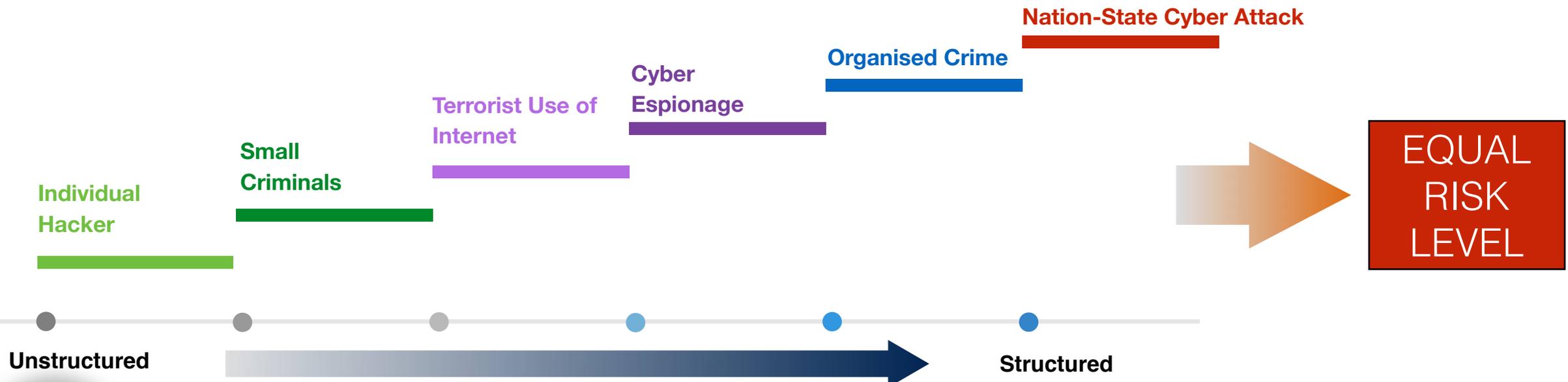
### LOCATION Willunga, South Australia

Due to an unknown glitch, Google bases Tom's location from one of his old Android phones, which he gave to his mother in Australia.



# Internet has Unlocked The Nation Threat Spectrum

Teknologi Internet memberikan kemudahan bagi siapapun dalam memperoleh informasi termasuk informasi terkait metode eksploitasi terhadap sistem informasi. Kondisi ini dapat memperbesar peluang munculnya serangan terhadap suatu negara yang tidak hanya berasal dari **Nation-State Actor** namun juga berasal dari **Perusahaan, Grup bahkan Individual (All Spectrum)** dengan potensi **tingkat resiko yang sama**



# Keamanan Bukan Produk, tetapi Proses

## Teknologi

Tidak ada Teknologi yang 100 % aman

## Risiko

Era digitalisasi menyebabkan Risiko keamanan semakin meningkat



## Hacker

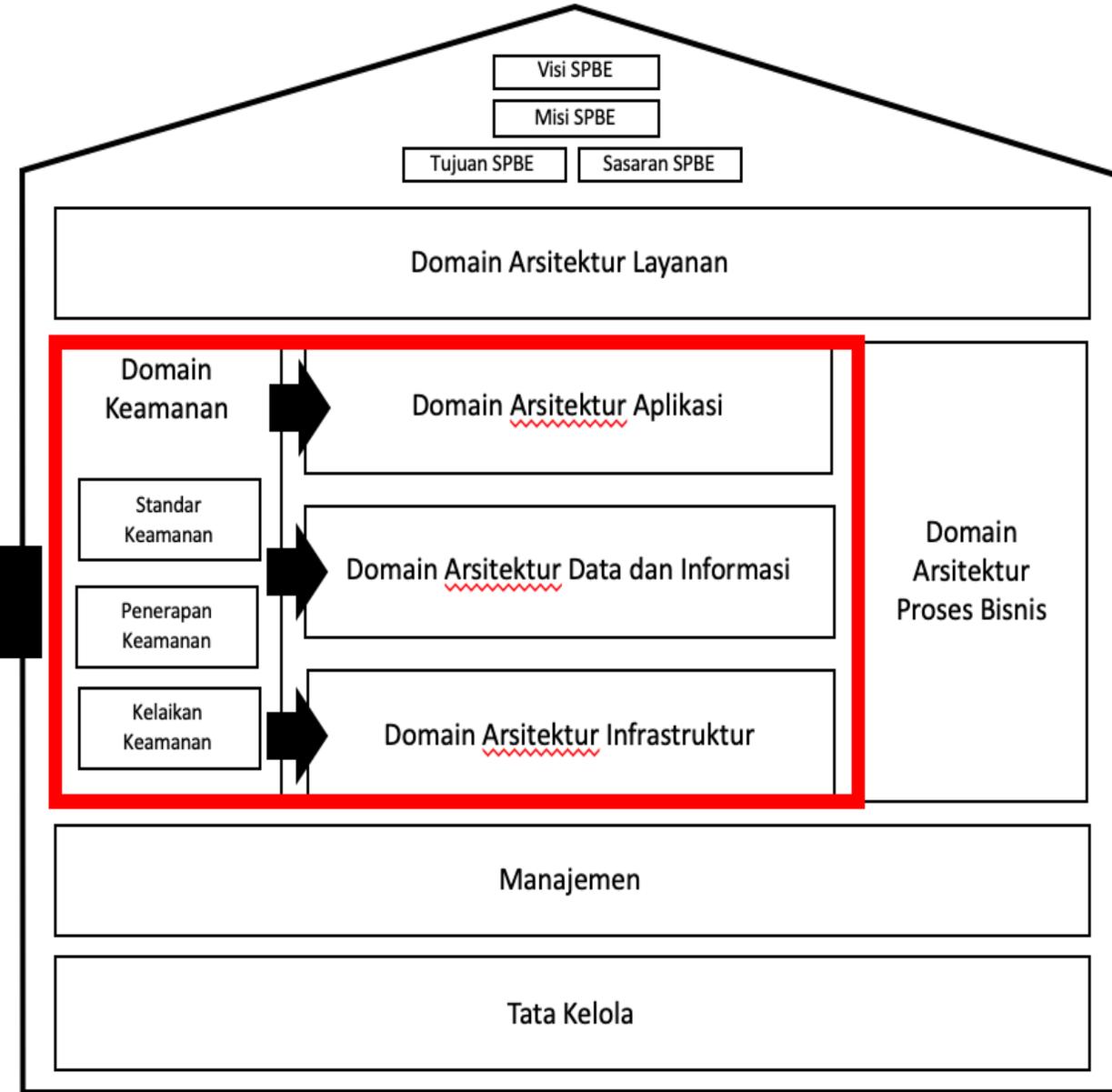
Selalu mencari Kerentanan yang bisa di eksploitasi

## Manusia

Kewaspadaan semua pihak menjadi faktor utama

# DOMAIN KEAMANAN SPBE

OBJEK/PRIORITAS YANG HARUS DIAMANKAN



# PRINSIP KEAMANAN SPBE

## PASAL 41 PERPRES NO.95 TAHUN 2018



### **PENJAMINAN KERAHASIAAN**

*Penetapan klasifikasi keamanan, pembatasan akses, dan pengendalian keamanan/enkripsi dan kriptografi.*

### **KEUTUHAN**

*Pendeteksian modifikasi dan tanda tangan elektronik tersertifikasi.*

### **KETERSEDIAAN**

*Penyediaan cadangan, perencanaan untuk menjamin data dan informasi dapat selalu diakses, dan pemulihan.*

### **KEASLIAN**

*Penyediaan mekanisme verifikasi, validasi dan hush function.*

### **KENIRSANGKALAN (NON-REPUDIATION)**

*Penerapan tanda tangan digital dan jaminan pihak ketiga terpercaya melalui penggunaan sertifikat digital.*



# TANTANGAN DAN URGENSI IMPLEMENTASI KEAMANAN TRANSFORMASI DIGITAL TERKAIT LAYANAN SPBE

## TANTANGAN

***Integrity dan Authentication***

Layanan SPBE membutuhkan keutuhan dan keaslian data yang tinggi. Tantangannya adalah menghadapi kerawanan/serangan modifikasi dan perubahan data.

***Data Privacy/ Confidentiality***

Sebagian besar layanan SPBE mengelola data/informasi yang **berklasifikasi rahasia/terbatas**, selain itu kondisi saat ini terdapat banyak aplikasi yang dimiliki oleh Instansi Pemerintah sehingga terjadinya duplikasi data. Tantangannya adalah **memastikan tidak terjadi insiden kebocoran data dalam aplikasi SPBE** dengan kondisi banyak data yang tersebar pada setiap aplikasi dan Infrastruktur SPBE.

***Availability***

Layanan SPBE menuntut **kebutuhan sistem** dapat selalu di akses kapanpun, dimanapun dan dalam kondisi apapun (ketersediaan). Tantangannya adalah **memastikan tidak terjadi kehilangan dan kerusakan data** meskipun jika terjadi insiden.

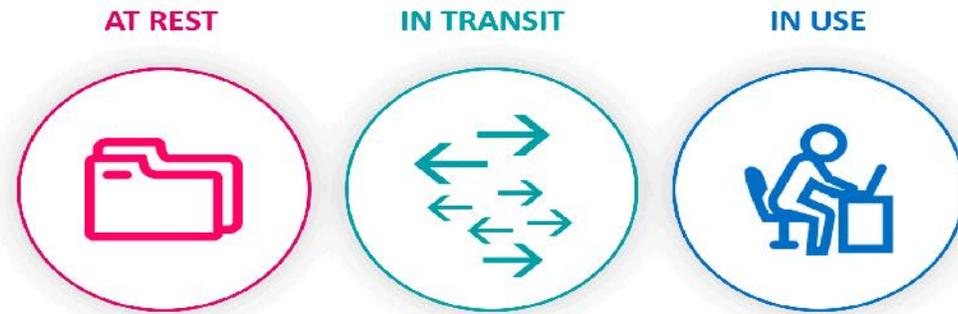
## URGENSI IMPLEMENTASI

**PEMENUHAN SERTIFIKAT ELEKTRONIK**

**PEMENUHAN LAYANAN KRIPTOGRAFI**

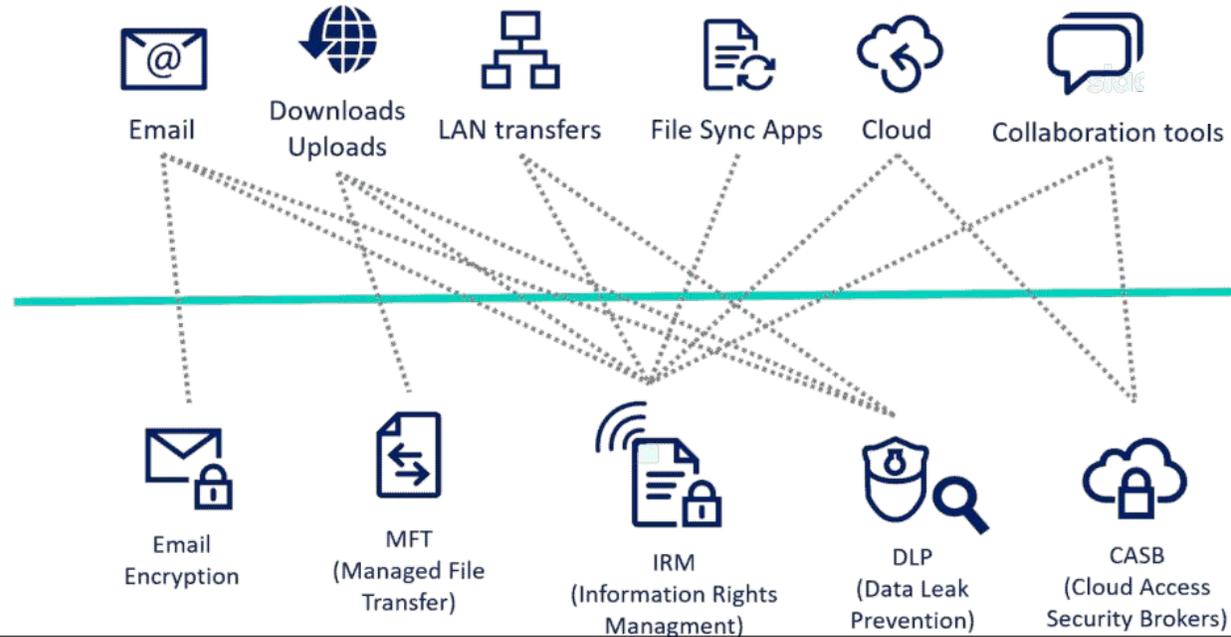
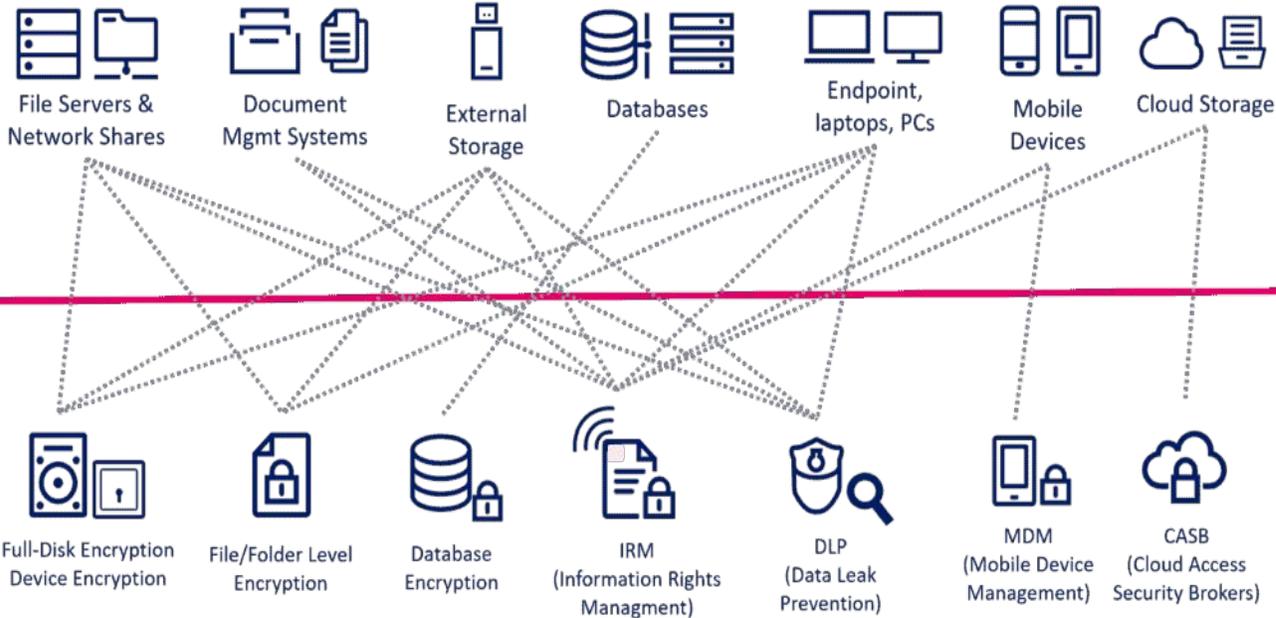
**MANAJEMEN KRISIS SIBER DAN SISTEM KEAMANAN DATA REKAM CADANG**

# AREA KEAMANAN DATA/INFORMASI



## PROTECTING DATA AT REST

## PROTECTING DATA IN TRANSIT





PERATURAN BADAN SIBER DAN SANDI NEGARA  
NOMOR 4 TAHUN 2021  
TENTANG

PEDOMAN MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN  
BERBASIS ELEKTRONIK DAN STANDAR TEKNIS DAN PROSEDUR KEAMANAN  
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA  
KEPALA BADAN SIBER DAN SANDI NEGARA,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 41 ayat (4) dan  
Pasal 48 ayat (5) Peraturan Presiden Nomor 95 Tahun 2018  
tentang Sistem Pemerintahan Berbasis Elektronik, perlu  
menetapkan Peraturan Badan Siber dan Sandi Negara tentang  
Pedoman Manajemen Keamanan Informasi Sistem  
Pemerintahan Berbasis Elektronik dan Standar Teknis dan  
Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik;

## BAB II. MANAJEMEN KEAMANAN INFORMASI KEAMANAN SPBE



# REGULASI ACUAN PEMBINAAN KEAMANAN SPBE PERBAN BSSN No. 4/2021

- Perban ini Terdiri dari 36 Pasal yang meliputi kebijakan Manajemen Keamanan Informasi dan Standar Teknis Prosedur Keamanan SPBE dengan ketentuan sebagai berikut :
- BAB I : Ketentuan UMUM (Pasal 1)
- BAB II : Manajemen Keamanan Informasi SPBE ( Pasal 2 – 16 )
- BAB III : Standar Teknis dan Prosedur Keamanan SPBE (Pasal 16-35)
- BAB IV : Penutup (Pasal 36)

## BAB III. STANDAR TEKNIS DAN PROSEDUR KEAMANAN SPBE



# AREA KEAMANAN APLIKASI DAN INFRASTRUKTUR SPBE

## UPAYA KEAMANAN HARUS DDILAKUKAN PEMDA

## CAPAIAN PRINSIP KEAMANAN

### 1. PENERAPAN STANDAR KEAMANAN

*Penerapan standar keamanan dilakukan pada saat pembangunan atau pengembangan aplikasi dan Infrastruktur SPBE.*

### 2. KELAIKAN KEAMANAN DAN PENINGKATAN KEAMANAN

*Kelaikan keamanan dapat dilakukan melalui Security Assessment secara berkala untuk menilai kondisi suatu aplikasi/infra (aspek keamanan). Maupun selanjutnya dilakukan reviu terkait security control berdasarkan standar yang telah ditetapkan. Hasil Assessment harus ditindaklanjuti oleh untuk dilakukan peningkatan atau perbaikan keamanan.*

### 3. AUDIT KEAMANAN SPBE

*Tahap selanjutnya Audit untuk memastikan kepatuhan terhadap kriteria kebijakan keamanan yang telah ditetapkan atau tidak adanya pelanggaran/temuan keamanan terhadap aplikasi dan infrastruktur SPBE.*

### PENJAMINAN KERAHASIAAN (CONFIDENTIALITY)

*penerapan enkripsi (implementasi algoritma kriptografi) dan pengendalian keamanan lainnya (Penetapan klasifikasi keamanan, pembatasan akses dll).*

### KEUTUHAN (INTEGRITY)

*Pendeteksian modifikasi dan penerapan sertifikat elektronik atau penerapan tanda tangan elektronik tersertifikasi.*

### KETERSEDIAAN (AVAILABILITY)

*Penyediaan cadangan dan sistem recovery data, perencanaan untuk menjamin sistem dapat selalu diakses, dan mekanisme pemulihan.*

### KEASLIAN (AUTHENTICITY)

*Penyediaan mekanisme verifikasi, validasi dan hush function.*

### KENIRSANGKALAN (NON-REPUDIATION)

*Penerapan tanda tangan elektronik tersertifikasi dan jaminan pihak ketiga terpercaya melalui penggunaan sertifikat elektronik.*



# Cyber Threat On Election.



- *“Trend cyber threat in election yang terjadi pada sistem Non-E-Voting adalah bukan melakukan hack pada sistem election nya, tapi bagaimana memanfaatkan platform social media yang ada dalam menggiring atau bahkan memanipulasi opini publik melalui“ Disinformation, propaganda. fake news (hoax)”.*



BADAN SIBER DAN SANDI NEGARA

JL. Harsono RM No. 70, Ragunan, Pasar Minggu, Jakarta Selatan



# QUICK WINS YANG DAPAT DILAKUKAN PEMDA



## PEOPLE

## PROCESS

## TECHNOLOGY

■ *Kontinuitas Peningkatan Kapasitas SDM Keamanan:*

- 1. Pelatihan dan Bimbingan Teknis; dan/atau*
- 2. Sertifikasi Kompetensi.*

■ *Harus adanya kaderisasi untuk membentuk tim keamanan informasi dengan memanfaatkan SDM yang ada atau melakukan penambahan SDM melalui skema Open recruitment atau Kontrak SDM Spesialis Keamanan Informasi/ minimal memiliki background IT.*

■ *Jika adanya kendala moratorium atau anggaran terkait Open recruitment dapat menyelenggarakan program magang (bekerjasama dengan universitas/SMK/Komunitas dll).*



■ *Melaksanakan IT Security Assessment (ITSA) atau minimalnya melakukan vulnerability assessment terhadap Aplikasi dan Infrastruktur SPBE;*

■ *Melakukan Hardening System Keamanan SPBE berdasarkan hasil ITSA/VA sebelumnya;*

■ *Penerapan Standar Teknis dan Prosedur Keamanan SPBE Yang Telah Ditetapkan;*

■ *Monitoring dan Penanganan Insiden Siber melalui CSIRT serta selalu berkolaborasi dan berkoordinasi dengan GOV-CSIRT BSSN;*

■ *Melaksanakan Audit Internal Keamanan SPBE (Kolaborasi Inspektorat dan Diskominfo);*

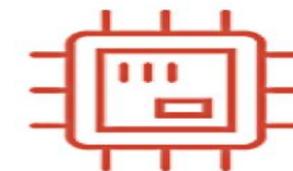


■ *Penerapan Sistem Kriptografi untuk keamanan Aplikasi SPBE khususnya Pengamanan Data/Informasi Elektronik (enkripsi database dll);*

■ *Pemenuhan dan Peningkatan Perangkat IT Security secara periodic (minimal pemenuhan Firewall, IDS/IPS dan anti virus yang proper sesuai dengan risiko yang dimiliki) serta Peningkatan Perangkat Lisensi IT Security;*

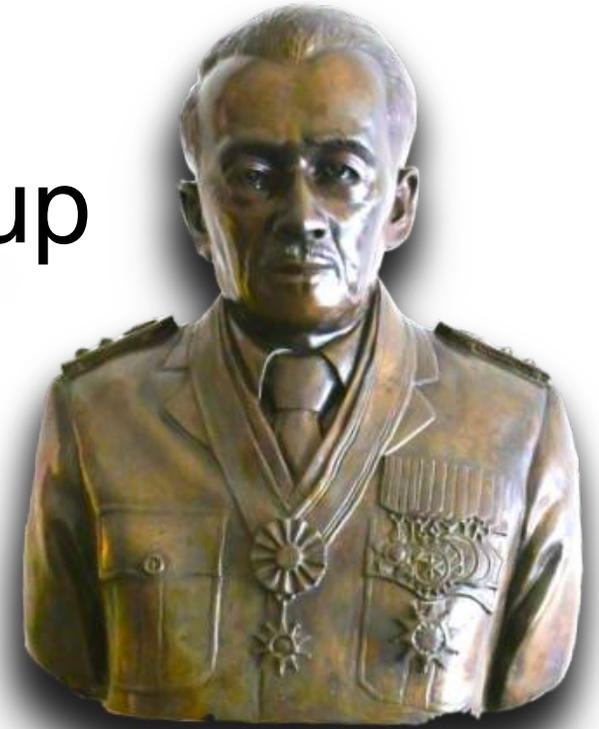
■ *Penerapan Sertifikat Elektronik – BSRE untuk mendukung keamanan dokumen elektronik dll*

■ *Mengoptimalkan Honey-Net Project BSSN dan SIEM-WAZUH;*



# “Kechilafan Satu Orang Sahaja Tjukup Sudah Menjebabkan Keruntuhan Negara”

Mayjen TNI Dr. Roebiono Kertopati  
(1914 - 1984)  
Bapak Persandian Republik Indonesia



BADAN SIBER DAN  
SANDI NEGARA

TERIMA KASIH