Keamanan Siber & Potensi Ancaman Eminen Kedepan

Ardi Sutedja K.
Ketua & Pendiri
Indonesia Cyber Security Forum (ICSF)
chairman@icsf.or.id
+62817835876

Indonesia Cyber Security Forum (ICSF), adalah Badan Hukum Perkumpulan Profesi yang didirikan berdasarkan Akta Notaris RA Mahyasari A. Notonagoro, SH, pada tanggal 16 November 2017 , dan dengan **Nomor Akta # 21**. Dan mendapatkan pengesahan berdasarkan **Keputusan Menteri Hukum & Hak Asasi Manusia RI No. # AHU-0017778.AH.01.07.Tahun 2017**

INDONESIA CYBER SECURITY SUMMIT™

Cyber Security Is Everyone's Business

Tentang Ardi Sutedja K.

Ardi Sutedja K.

- ***Ketua & Pendiri, Indonesia Cyber Security Forum (ICSF)***
- ***Ketua & Pendiri, Indonesia Chief Information Officers Forum (id.CIO)***
- ***Ketua & Pendiri Indonesia Biometric Association (IBA)***
- ***Ketua Dewan Penasehat, Asosiasi Forensik Digital Indonesia (AFDI)***
- ***Anggota Dewan Kehormatan & Etika, Asosiasi FinTech Indonesia (AFTECH)***
- ***CEO, PT Indonesia Dirgantara Expo (IDEX)***
- ***CEO, PT Media Solutions International (MSI)***
- ***CEO PT Jasa Siber Indonesia (JSI)***
- ***Komisaris, Mitra Tekno Madani (MTM), anak usaha PNM Group***
- ***Penceramah Tamu, SESKO-AD & SESKO-TNI, UNHAN, BAIS-TNI, BIN, Mabes TNI, RSIS- NTU-Singapore, UNSW-Australia & RSA Conferences.***

Ardi Sutedja K., adalah Direktur Utama dari PT Indonesia Dirgantara Expo (IDEX), sebuah perusahaan Event Organiser (EO) nasional yang fokus pada kegiatan- kegiatan yang terkait dengan tehnologi, antara lain, Tehnologi Informasi dan Komunikasi (TIK) Tehnologi Ke-Dirgantaraan (Aviasi) dan Tehnologi Ke-Maritiman. Selain memimpin IDEX, Ardi juga menjadi salah satu pendiri dan pengurus dari Indonesia Cyber Security Forum (ICSF) dan Indonesia Chief Information Officers Forum (id.CIO), dua organisasi nirlaba yang fokus kepada pembangunan kewaspadaan, pembangunan kapasitas, dan pengembangan tehnologi keamanan dan ketahanan siber. Dan, Ardi juga telah ditunjuk sebagai Ketua Dewan Kehormatan Asosiasi Forensik Digital Indonesia (AFDI) dan Anggota Dewan Kehormatan & Etika Asosiasi FinTech Indonesia (AFTECH).

Pengalaman kerja Ardi selama kurang lebih 30 tahun, meliputi pengalaman baik di militer, pemerintahan maupun swasta, termasuk diantaranya pengalaman merumuskan hal-hal yang terkait dengan, *cybersecurity strategy*, *governance & compliance, IT risk assessment*, ancaman siber, *vulnerability assessment, IT security design & implementation, incident management & data loss protection/privacy services*. Ardi juga kini fokus kepada manajemen resiko serta dampak dari munculnya tehnologi-tehnologi yang bersifat *mobile* dan portable, media-media Sosial, *Cloud Computing,* dan tehnologi-tehnologi lainnya.

Memiliki pendidikan dasar di bidang Ilmu Hukum dari Universitas Indonesia, dan pendidikan Pasca Sarjana di bidang Administrasi Bisnis dari State University of New York (SUNY), serta beberapa *fellowship* dari University of Malta dan George C. Marshall Center for Security Studies (NATO) di Jerman, serta berbagai sertifikasi profesi keahlian khusus di bidang Keamanan & Ketahanan Siber, Intelijen Siber dan *Cyber Behavioral Analysis*, yang diperolehnya dari berbagai lembaga sertifikasi dan pelatihan global, termasuk sertifikat pelatihan ilmu kajian khusus dari beberapa lembaga/institusi pemerintah/militer dari negara- negara mitra kerja, antara lain, Amerika Serikat, Korea Selatan dan Jerman.

Masalah Keamanan Siber Adalah Ancaman KamNas!

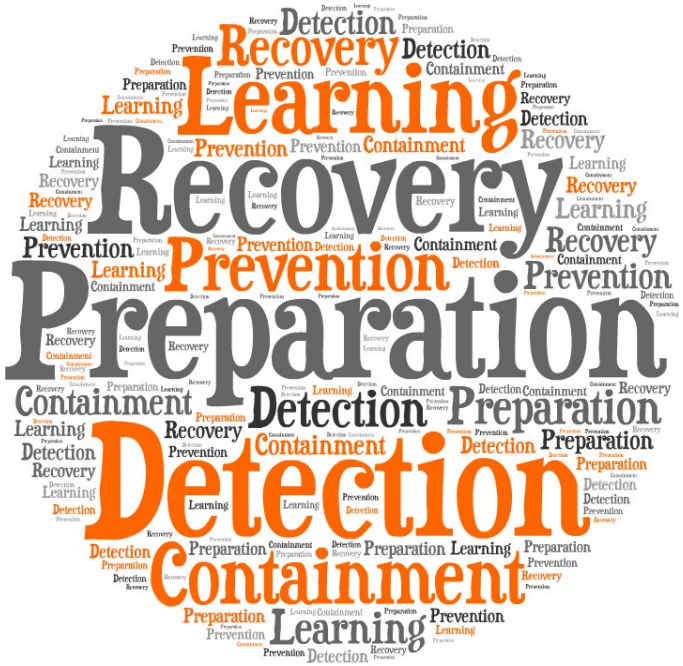
- **"...systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters."** - *USA Patriot Act (P.L. 107-56)*

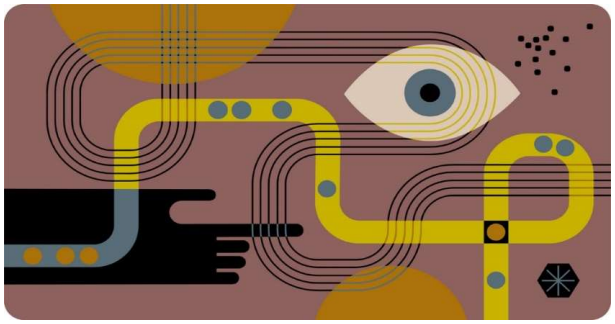
Is ALL about Risks to Human Life & Business Continuity!

Lantas bagaimana kita, memandangnya?

Pandangan Luas Dari Helicopter

Mengenal Dunia Digital Dari Sejarah



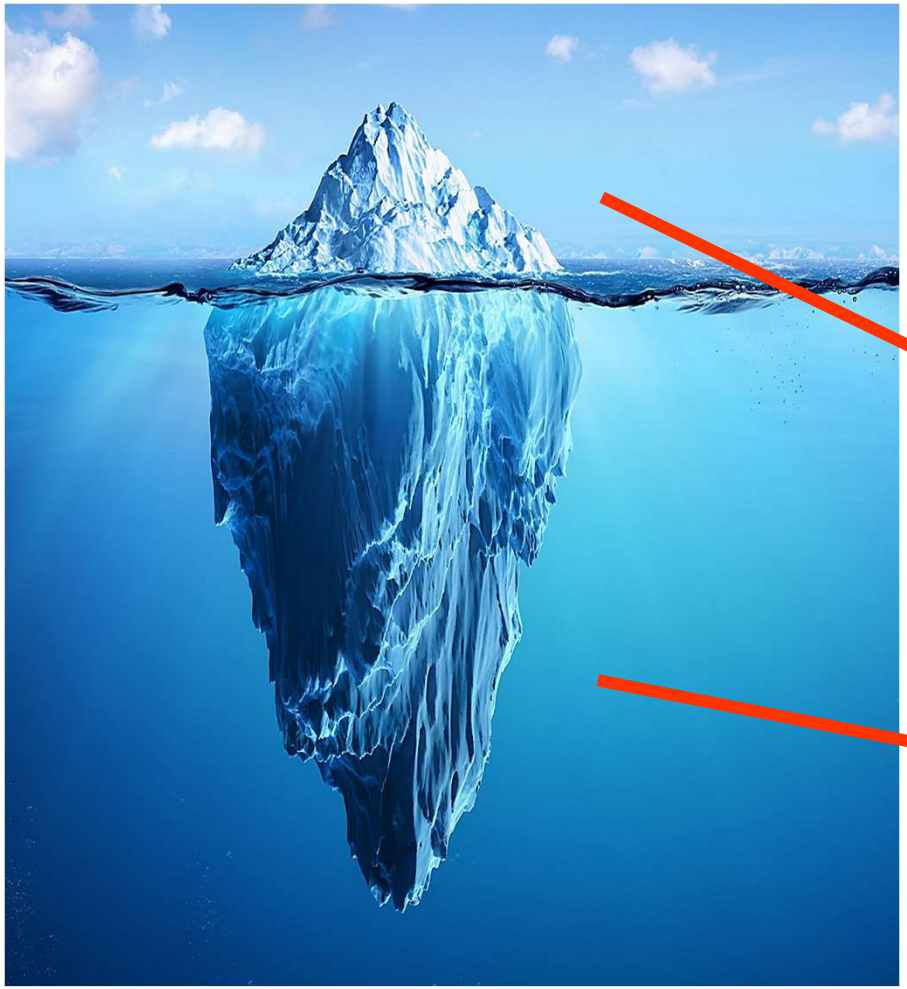


"Membayangkan melalui fakta & sejarah"

INDONESIA CYBER SECURITY SUMMIT™

Cyber Security Is Everyone's Business

▪ Attack Surface: Ilusi Kita Selama Ini



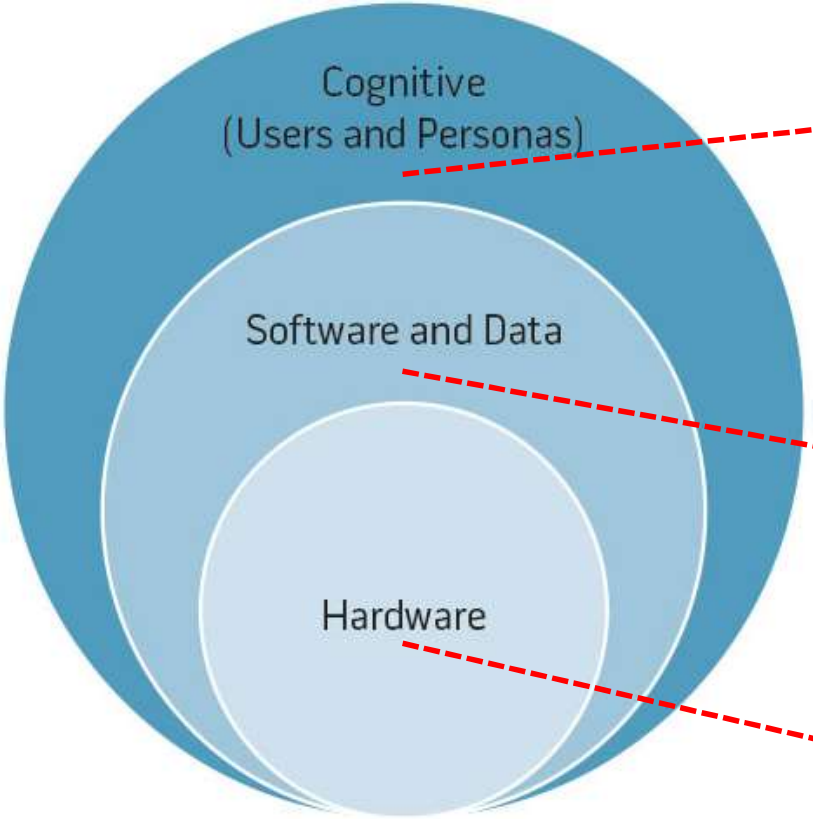
The Software Illusion

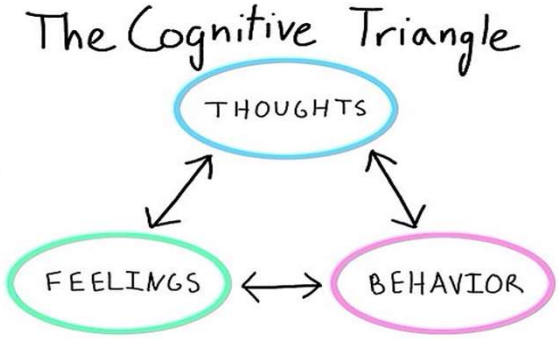
Saat ini hampir semua perusahaan keamanan siber global hanya berpikir bahwa serangan akan terjadi diatas O/S atau di permukaan saja, padahal para peretas juga kini semakin kreatif dan inovatif untuk menyerang apa yang ada dibawah permukaan.

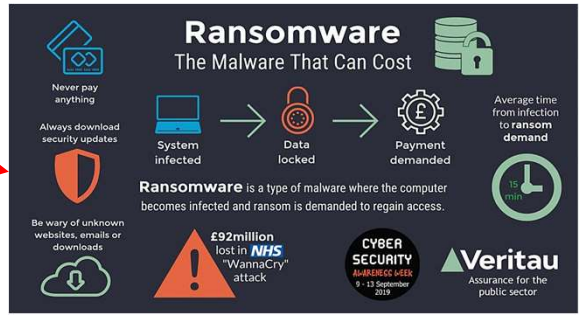
Yang Terlihat Oleh Para Vendor Keamanan Siber

Yang Sekarang Dilihat & Di Sasar Para Peretas Canggih

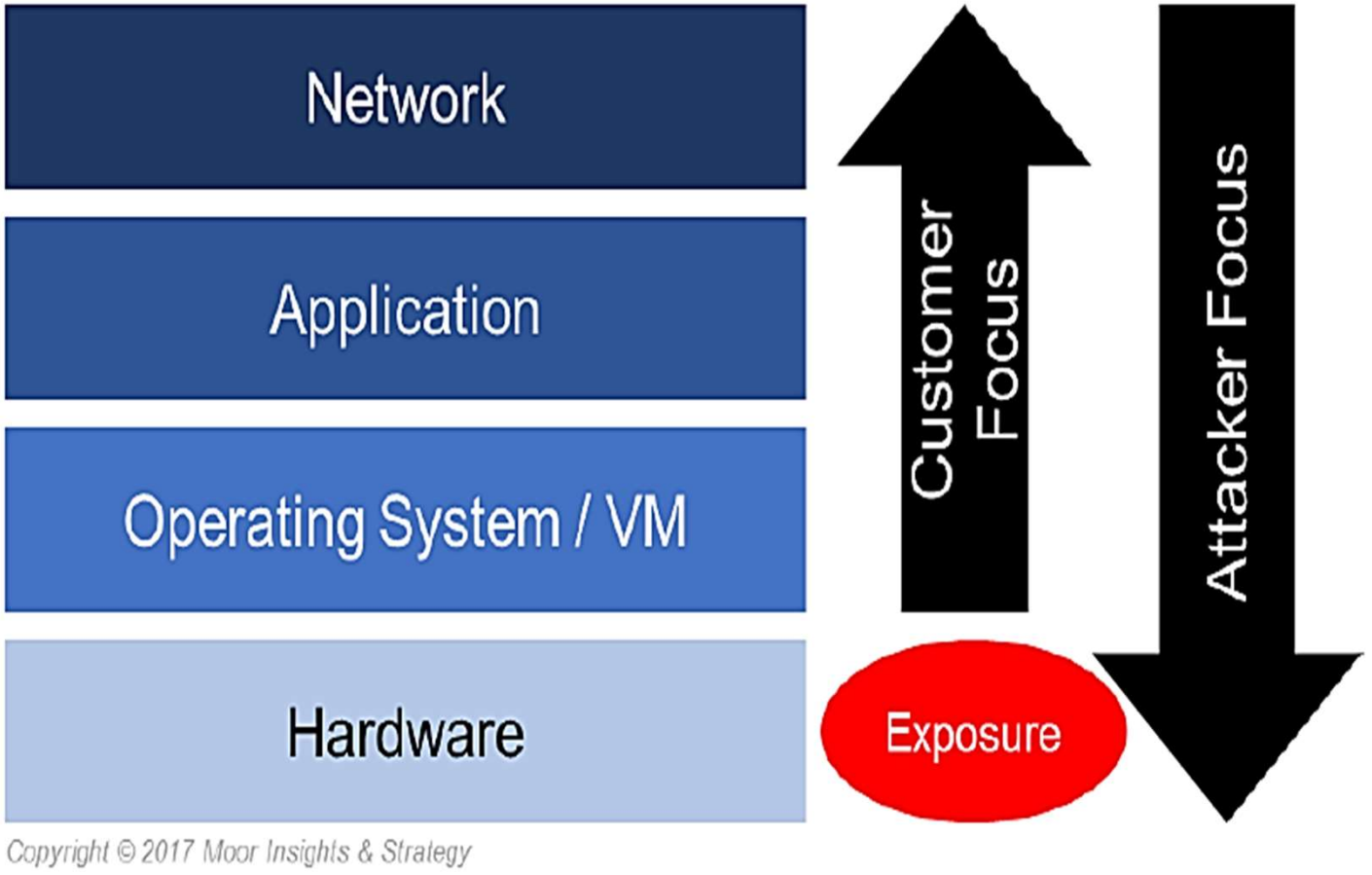
3 Hal Pokok Yang Menjadi Sasaran



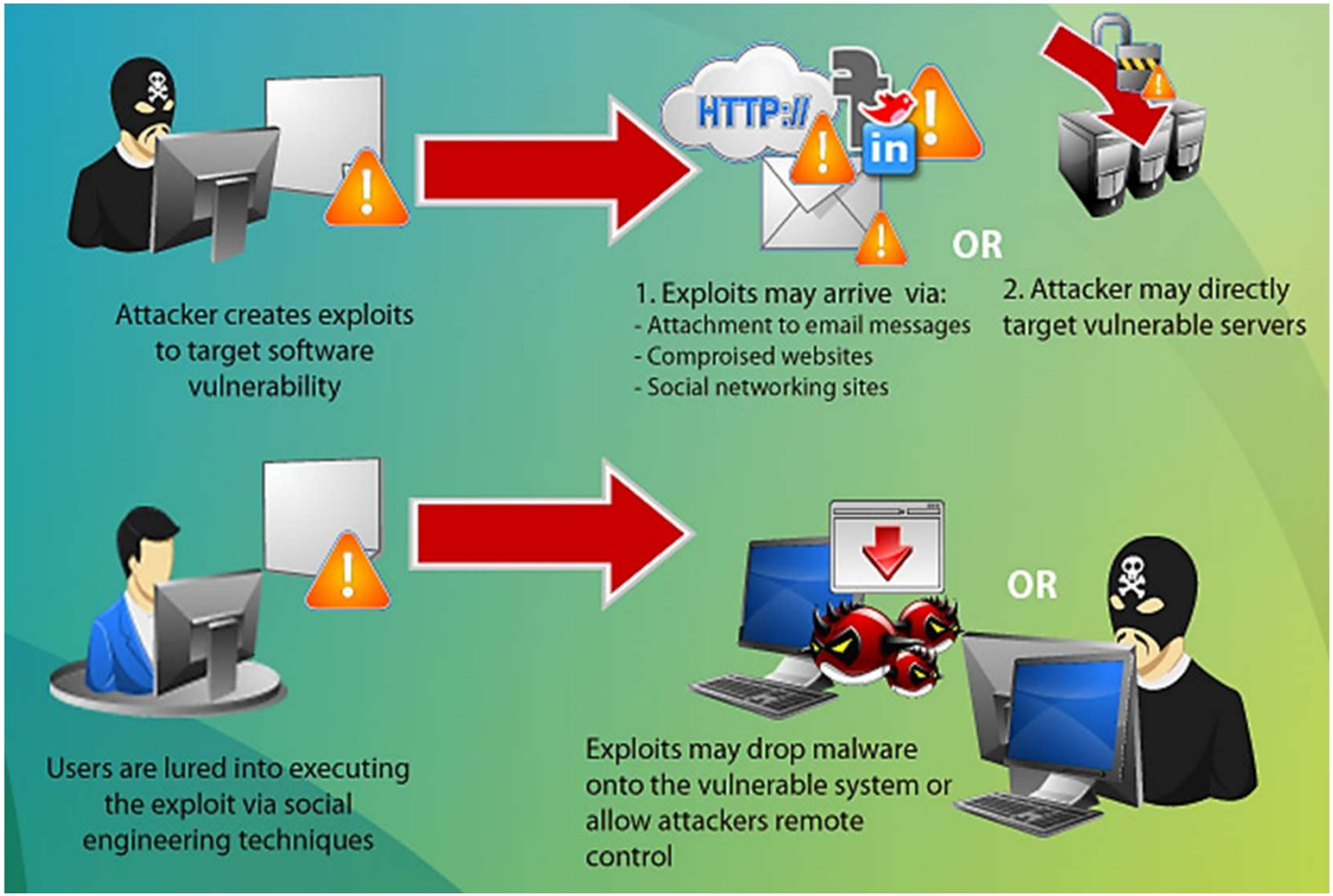




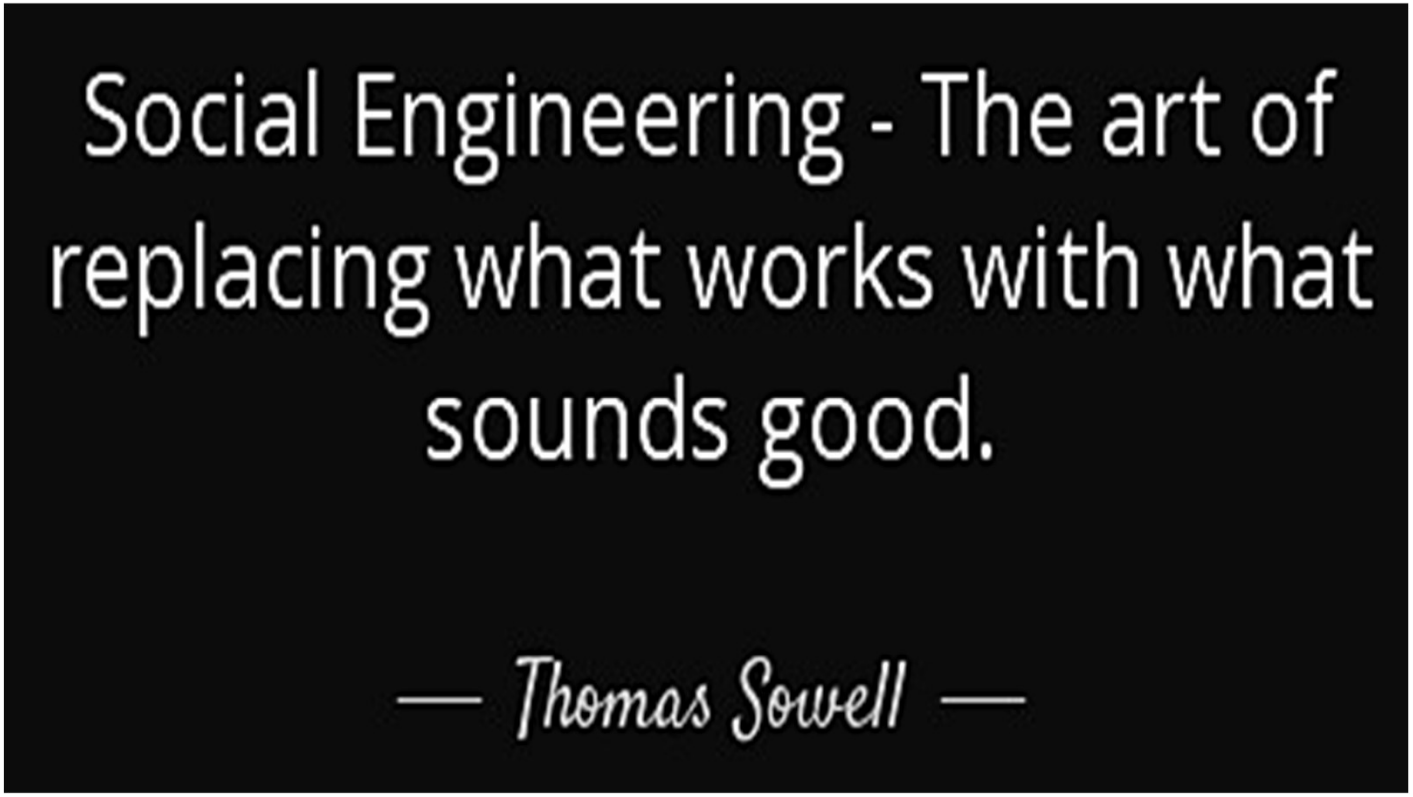
1. Serangan Terhadap Hardware



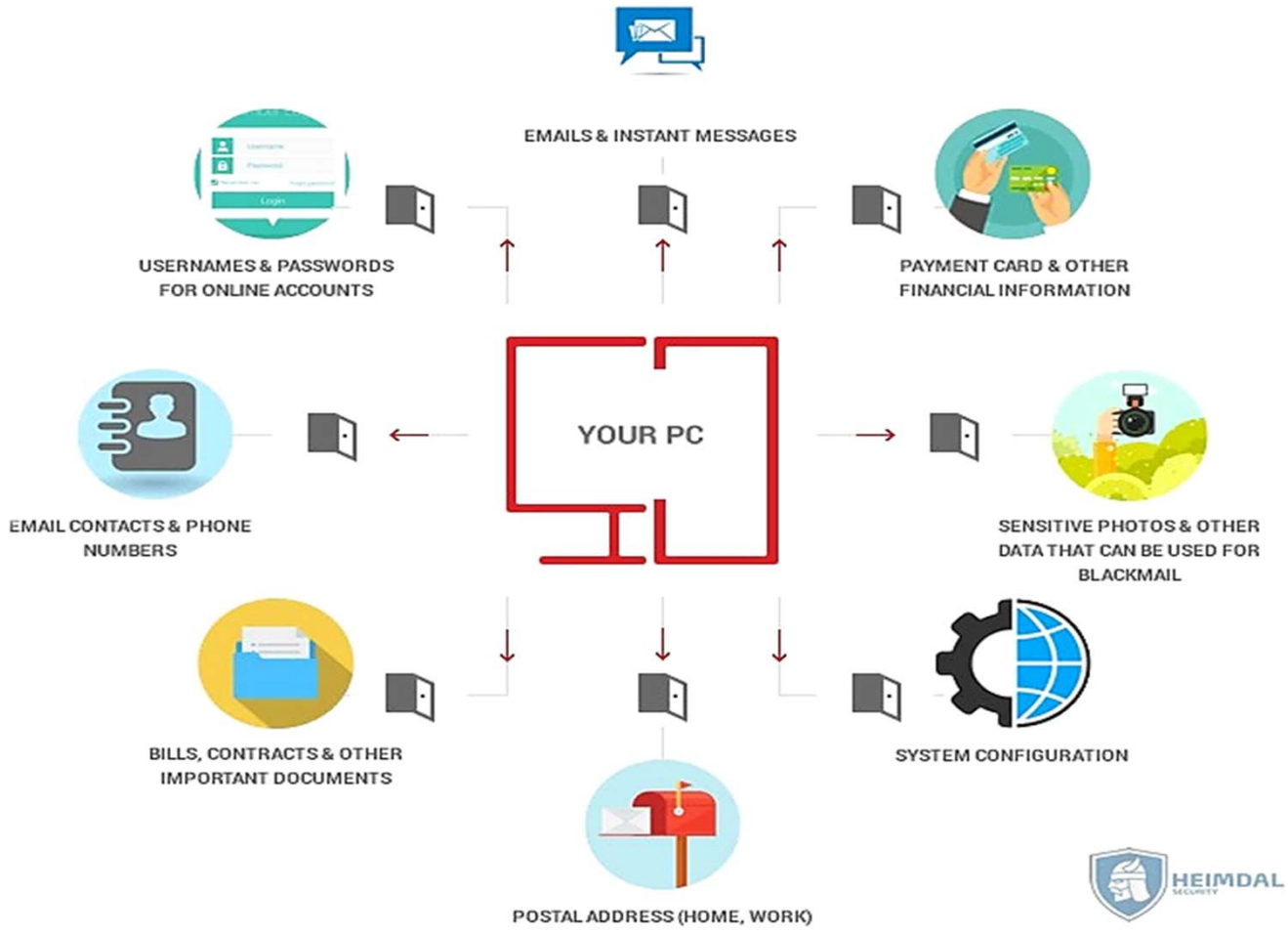
2. Serangan Atas Software & Data



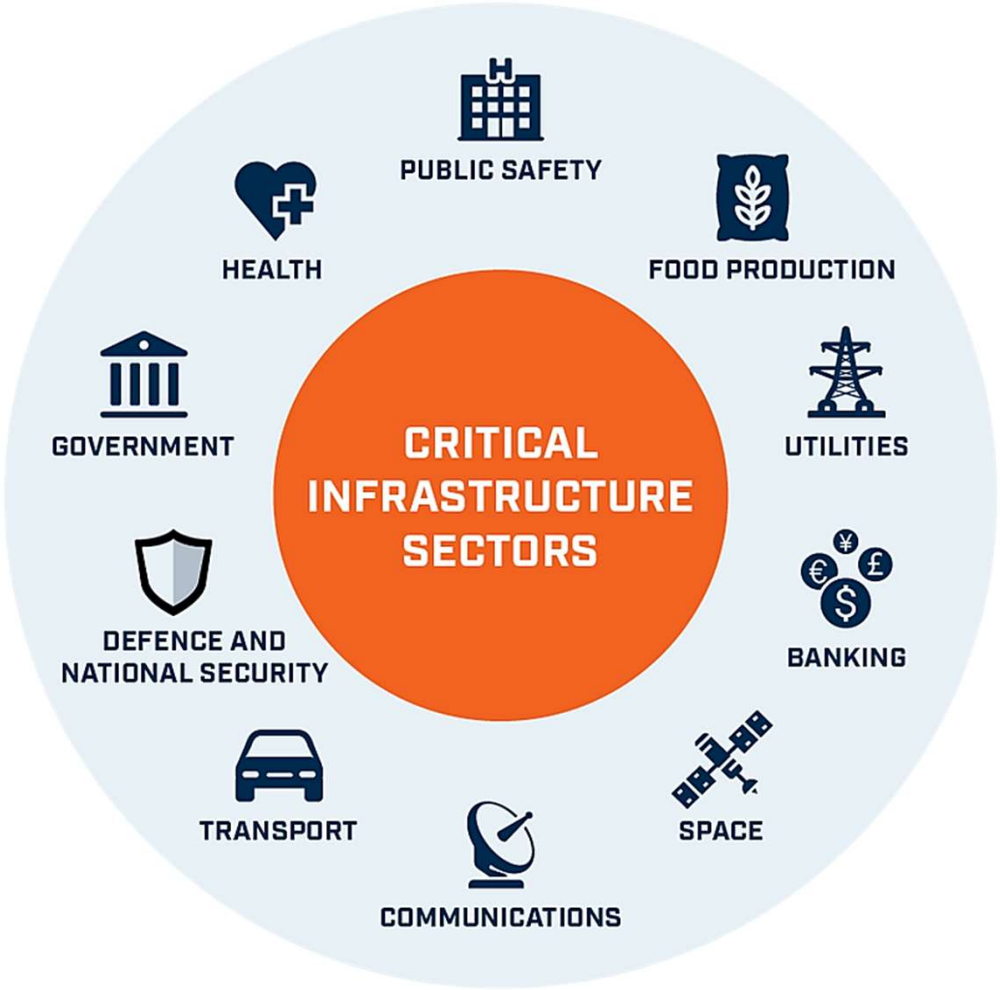
3. Serangan Kognitif: SOCENG



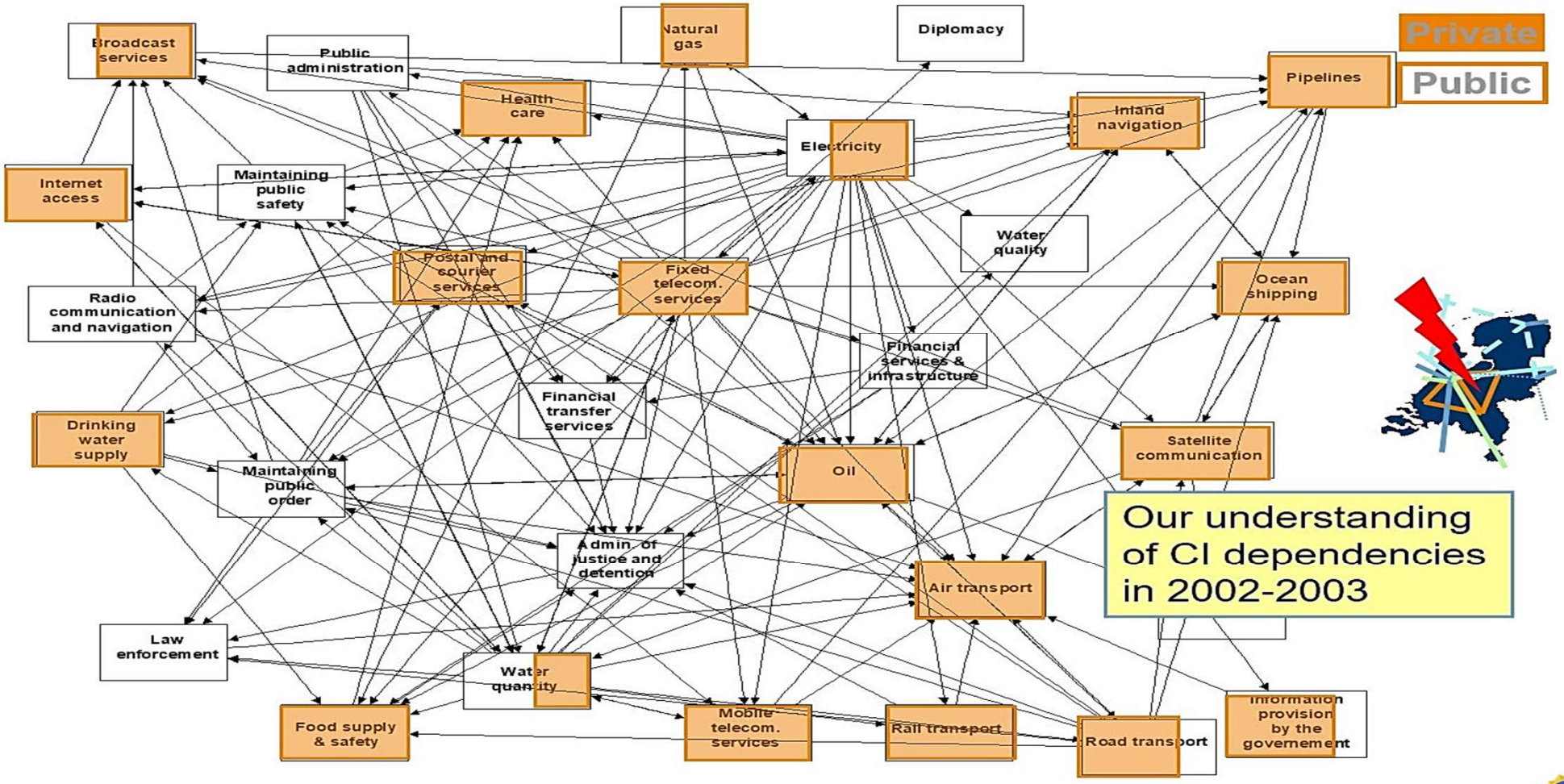
Aset Strategis Sebagai Sasaran & Pintu Masuk



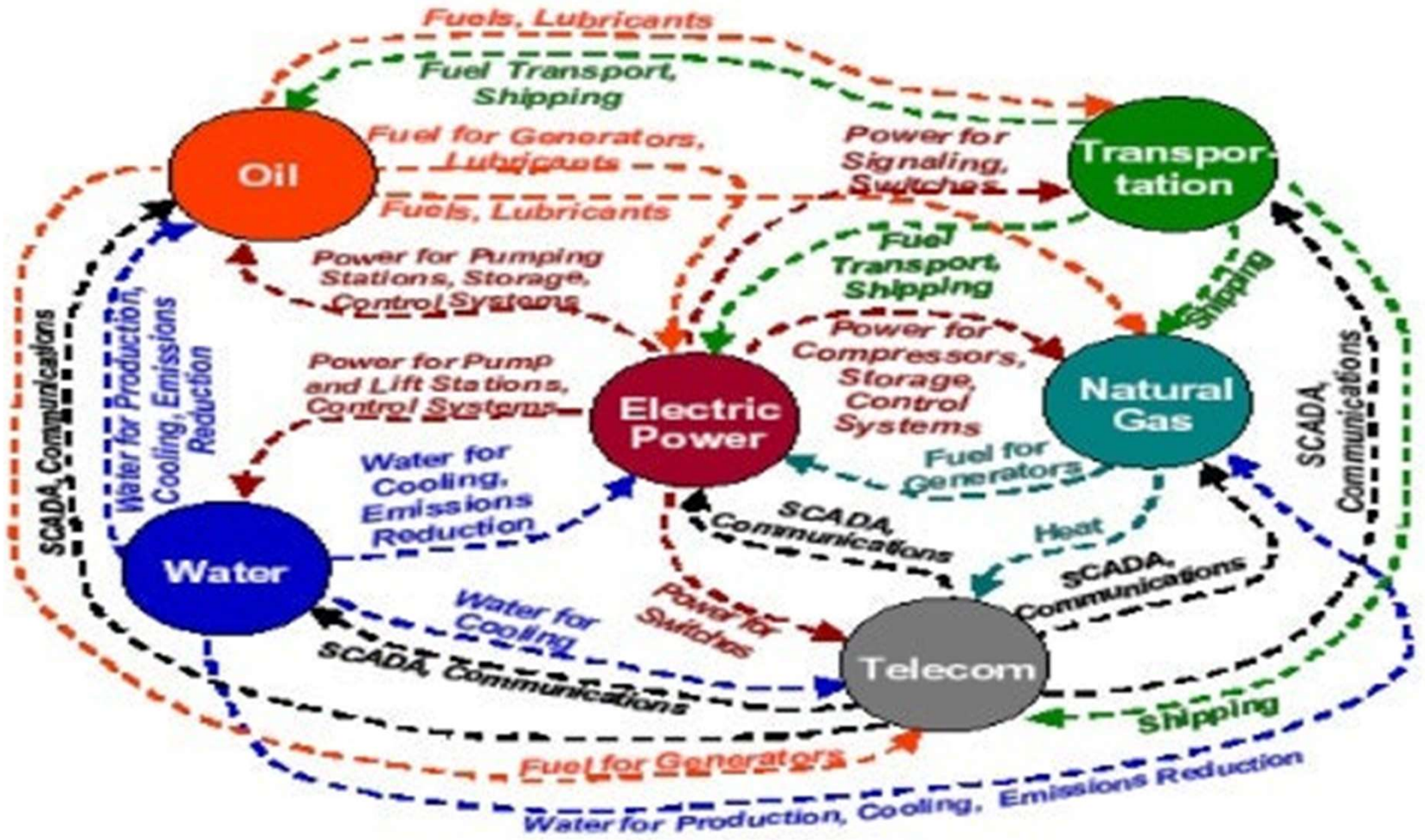
Sektor Infrastruktur Kritis



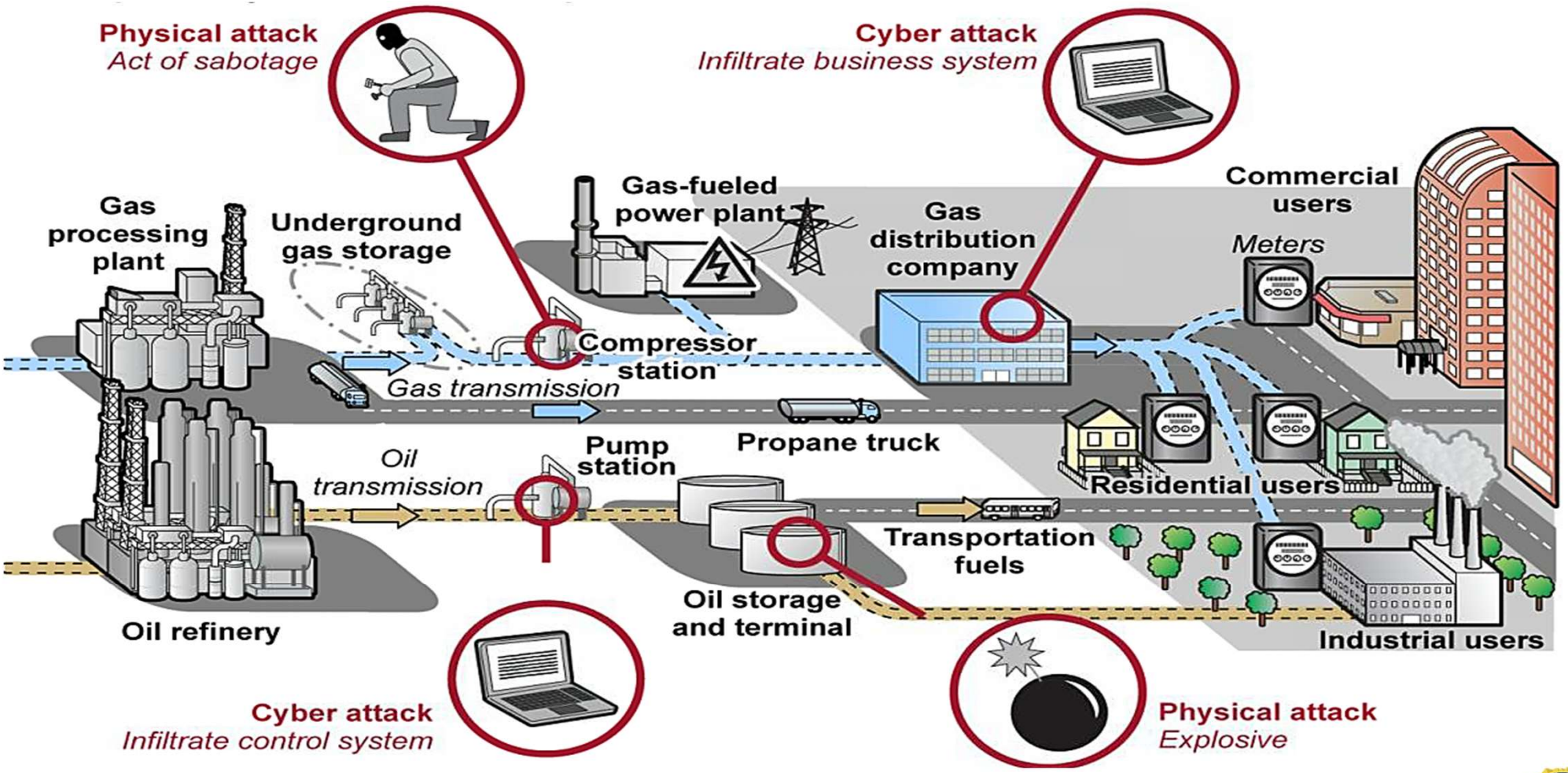
Kompleks, Saling Bergantung & 75% Swasta



Seperti Apa Kompleksitasnya?



Melihat Dari Helicopter: Komponen Dasar Kerentanan



Kompleksitas Lainnya : TRANSFORMASI DIGITAL

Transformasi Digital adalah merupakan suatu keharusan yang tidak terelakkan semenjak 2-3 tahun terakhir, dan sangat dirasakan pada saat pandemi Covid 19 dimana telah memaksa kita semua untuk, merubah berbagai kebiasaan kita dalam kehidupan termasuk pada pelayanan publik. Tidak bisa dipungkiri bahwa proses Transformasi Digital ini juga telah melahirkan berbagai tantangan, kesempatan dan manfaat, serta resiko-resiko yang jarang ada yang mau membicarakannya.

Semuanya Ini BUKAN Ilmu Sulap!

Fakta – Fakta Tentang Indonesia

Fakta – Fakta Terbaru Di Indonesia 2022

10 Kementerian dan Lembaga Negara Indonesia Diduga Diretas Hacker China

Fakta – Fakta Terbaru Lainnya Di Indonesia 2022

Ancaman Siber Kian Besar

Selama pandemi Covid-19, serangan siber semakin tinggi. Sepanjang Januari–Agustus 2021, ditemukan lebih dari 888,7 juta serangan siber, termasuk peretasan pada lembaga pemerintah.

JAKARTA, KOMPAS — Ancaman keamanan siber di Tanah Air semakin besar seiring dengan kian tingginya penggunaan teknologi informasi dan komunikasi digital. Maraknya peretasan belakangan ini semestinya dijadikan peringatan untuk mempersiapkan diri terhadap segala potensi serangan siber. Selain menyiapkan manajemen krisis, strategi keamanan siber juga perlu segera dibangun.

Data yang dihimpun Badan Siber dan Sandi Negara (BSSN) menunjukkan, sepanjang Januari-Agustus 2021 ditemukan lebih dari 888,7 juta serangan siber. Sebagian besar serangan berbentuk *malware*, *denial of service* atau mengganggu ketersediaan layanan, serta aktivitas *trojan*.

Ransomware atau *malware* yang meminta tebusan dan kebocoran data menjadi tren serangan siber belakangan ini. Kebocoran data akibat *malware* pencuri informasi paling banyak ditemukan di sektor pemerintah, yakni 45,5 persen, diikuti sektor keuangan 21,8 persen, telekomunikasi 10,4 persen, penegakan hukum 10,1 persen, transportasi 10,1 persen, dan BUMN lain 2,1 persen.

Kepala BSSN Hinsa Siburian di sela-sela pembukaan Digital Leadership Academy Kementerian Komunikasi dan Informatika, Senin (13/9/2021), mengungkapkan, semakin tinggi pemanfaatan teknologi informasi dan komunikasi digital, semakin tinggi pula risiko dan ancaman keamanan siber. Apalagi, di tengah pandemi Covid-19, sebagian besar aktivitas beralih ke ruang siber. Artinya, kerentanan dan kerawanan akan serangan juga relatif besar.

"Manfaat atau kemudahan yang kita dapat (dari penggunaan teknologi informasi) itu sebenarnya berbanding lurus dengan risiko dan ancaman keamanan siber. Kalau kita tidak siap untuk itu (serangan siber), ya, memang agak repot," ujar Hinsa.

Selama pandemi, peretasan kian marak terjadi. Terakhir pada Jumat pekan lalu, jaringan internal 10 kementerian/lembaga, termasuk Badan Intelijen Negara (BIN), diduga diretas. Berdasarkan informasi The Record, peretasan ditemukan Insikt Group, divisi riset ancaman siber dari Recorded Future. Peretasan ini dikaitkan dengan Mustang Panda, sekelompok peretas dari China yang dikenal dengan berbagai aksi spionase dan menargetkan negara-negara di kawasan Asia Tenggara.

Hinsa menegaskan, semua kalangan perlu waspada di tengah maraknya serangan siber. Lebih dari itu, manajemen krisis juga dibutuhkan karena tidak ada yang bisa memprediksi kapan serangan di ruang siber bakal terjadi. Seperti dugaan peretasan jaringan internal 10 kementerian/lembaga juga terjadi secara tiba-tiba.

"Jadi, memang itu cirinya ruang siber, (serangan) sewaktu-waktu. Apa intinya? Ya, kita memang harus siap, kita harus membangun strategi keamanan siber, kita harus *alert* (waspada) dengan situasi," tuturnya.

Saat ini, BSSN tengah membangun strategi keamanan siber. Selain itu, membangun dan membentuk keamanan nasional untuk keamanan siber. Ini merupakan bagian yang tak terpisahkan dari kepentingan keamanan nasional.

Kemampuan deteksi

Berkaca dari dugaan peretasan di lingkungan pemerintah, Director of Cyber Security BDO Indonesia M Novel Ariyadi mengingatkan agar kementerian/lembaga terus meningkatkan kapabilitas pada area deteksi serangan siber. Peningkatan kemampuan deteksi ini penting karena karakteristik serangan siber berbeda dengan serangan fisik.

"Serangan fisik relatif lebih mudah dideteksi oleh korban. Hal ini berbeda dengan serangan siber. Sering kali yang terjadi, korban tak mampu mendeteksi serangan. Bahkan, mereka baru mengetahui telah menjadi korban dari pihak media atau peneliti eksternal," ujarnya.

Sama seperti pada kasus kebocoran data sebelumnya, kasus dugaan peretasan terhadap jaringan internal 10 kementerian/lembaga ini juga diketahui dari media asing. Hal ini, menurut Novel, menunjukkan tidak adanya kemampuan deteksi (*detection capability*) dalam mengenali dan mendeteksi serangan.

Novel berpandangan pendekatan audit reguler kini sudah harus dilengkapi dengan pendekatan *continuous threat hunting*. Pendekatan ini untuk memperbaiki kemampuan deteksi di mana senantiasa diasumsikan serangan siber telah berhasil dilakukan pihak lawan pada sebuah organisasi sampai dibuktikan tidak terjadi. Pendekatan ini dilakukan terus-menerus dengan frekuensi lebih sering ketimbang audit reguler.

"Perbedaan pendekatan ini dibandingkan dengan audit reguler adalah tidak mengacu pada kepatuhan terhadap sebuah standar tertentu, tetapi mengacu pada profil risiko bagi sebuah organisasi. Khususnya terkait profil penyerang atau *threat actor* yang patut diduga memiliki *intention* dan *capability* untuk melakukan serangan siber," katanya.

Selain itu, BIN perlu pula meningkatkan koordinasi dengan BSSN untuk mengembangkan analisis korelasi antara intelijen fisik dan intelijen siber. Selanjutnya, hasil analisis itu didiseminasi kepada semua kementerian/lembaga yang rawan menjadi target serangan siber.

Secara terpisah, Kepala Departemen Hukum Telekomunikasi, Informasi, Komunikasi, dan Kekayaan Intelektual Universitas Padjadjaran Sinta Dewi Rosadi mengatakan, solusi terbaik yang dibutuhkan adalah membenahi sistem keamanan siber di internal pemerintah. Instansi pemerintahan harus menggandeng para ahli keamanan siber untuk memeriksa kekurangan atau celah yang ada dalam sistem dan jaringannya.

Selain itu, harus ada pula ketentuan yang mewajibkan audit eksternal. Artinya, sistem keamanan itu diaudit oleh pihak ketiga untuk menguji apakah semua sistem yang ada aman atau tidak.

"Itu akan menguji apakah memang terjadi kebocoran atau tidak. Jadi, harus secara komprehensif penanganannya. Apalagi sekarang tambah banyak serangan seperti ini," tuturnya.

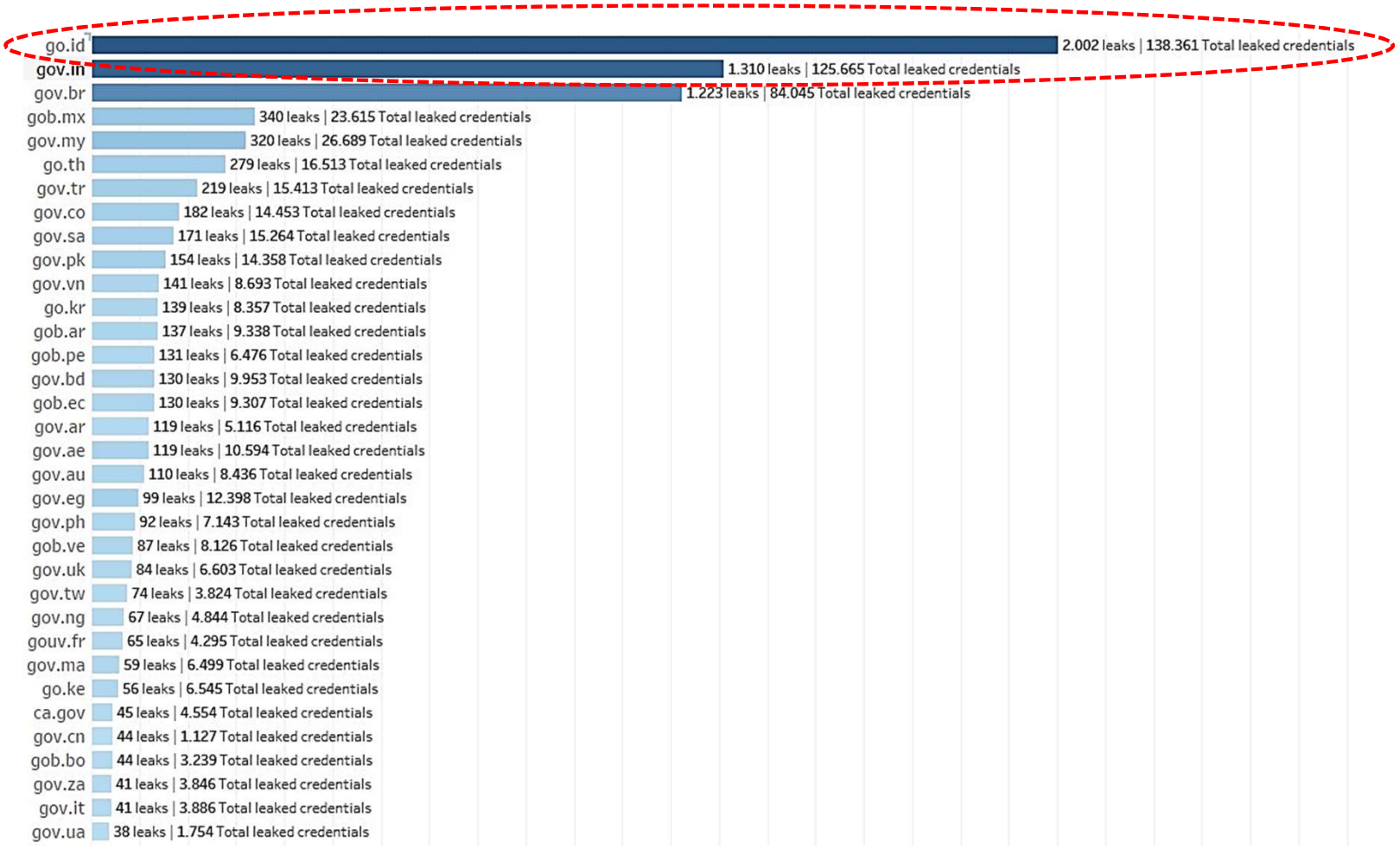
Sinta pun mengingatkan, tantangan ke depan semakin kompleks, terutama saat Indonesia menerapkan kebijakan satu data. Tingkat kerawanan akan serangan diperkirakan semakin tinggi sehingga pemerintah perlu mempersiapkan regulasi, organisasi, dan juga sistem keamanan siber.

Baik Novel maupun Sinta mendorong BSSN segera melakukan investigasi dugaan peretasan yang menyasar jaringan internal 10 kementerian/lembaga di Indonesia. Investigasi ini dibutuhkan untuk mengungkap pelaku peretasan dan menjaga kepercayaan publik terhadap reputasi pemerintah di ruang siber. Laporan dari The Record dapat menjadi data awal untuk menginvestigasinya secara lebih mendalam. (BOW)

▶ klik.kompas.id/polhuk

Baca artikel lainnya seputar Politik dan Hukum di Kompas.id dengan memindai QR Code.

Fakta – Fakta Terbaru Di Indonesia 2022



https://docs.google.com/spreadsheets/d/1KC615oNu1GJN4hymAR1Hxe1M46WG_FW4UMmHWbD3y3s/edit#gid=793840740

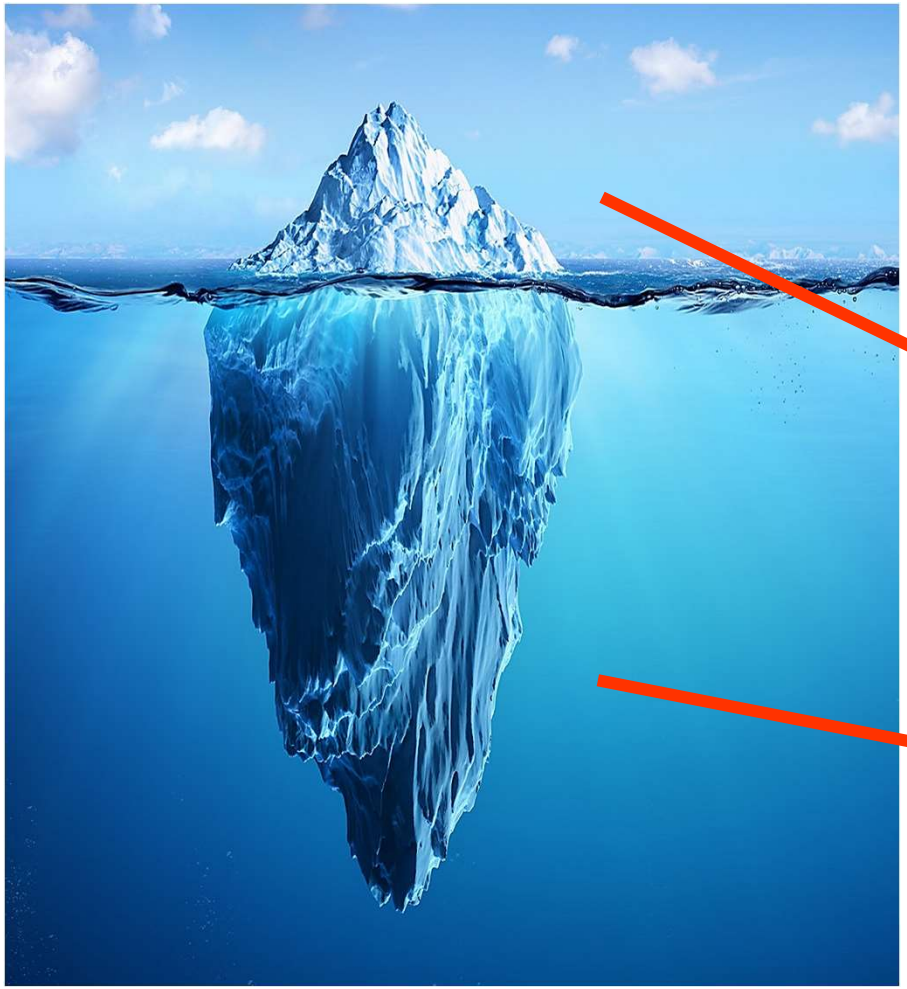
Taxonomi Ancaman Siber

Cyber Threat	Motive	Targets of Opportunity	Methodologies	Capabilities
Nation States ~ Peace Time	Economic, Military, Political	Commercial Enterprises, Intelligence, National Defense, Governments, National Infrastructure	Military & Intel specific cyber doctrine, hacktivists	Asymmetric use of the cyber domain short of kinetic
Nation States ~ War Time	Economic, Military, Political	Commercial Enterprises, Intelligence, National Defense, Governments, National Infrastructure	Military & Intel specific cyber doctrine, hacktivists	Asymmetric use of the cyber domain including kinetic
Cyber Terrorists & Insurgents	Political	Infrastructure, Extortion and Political Processes	Combination of advanced persistent threats (APT)	Developing – will be a concern in 2012
Cyber Criminals – Grey & Black Markets	Financial	Intellectual Property Theft, Fraud, Theft, Scams, Hijacked Network & Computer Resources, Cyber Crime for Hire	Exploits, Malware Botnets, Worms & Trojans	Cell-based structure as an APT
Criminal Organizations – RBS	Financial		Use of above with distinct planning	Highly professional, dangerous
Rogue Organizations – Anonymous, LulzSec	Financial	Intellectual Property Theft, Direct & Indirect pressure on OGA Resources	Organic hacking capabilities unsurpassed	Organized yet de-centralized

Resiko HTAG Siber Adalah ANCAMAN NYATA

It's not a matter of if, but when?

▪ Attack Surface: Ilusi Kita Selama Ini



The Software Illusion

Saat ini hampir semua perusahaan keamanan siber global hanya berpikir bahwa serangan akan terjadi diatas O/S atau di permukaan saja, padahal para peretas juga kini semakin kreatif dan inovatif untuk menyerang apa yang ada dibawah permukaan.

Yang Terlihat Oleh Para Vendor Keamanan Siber

Yang Sekarang Dilihat & Di Sasar Para Peretas Canggih

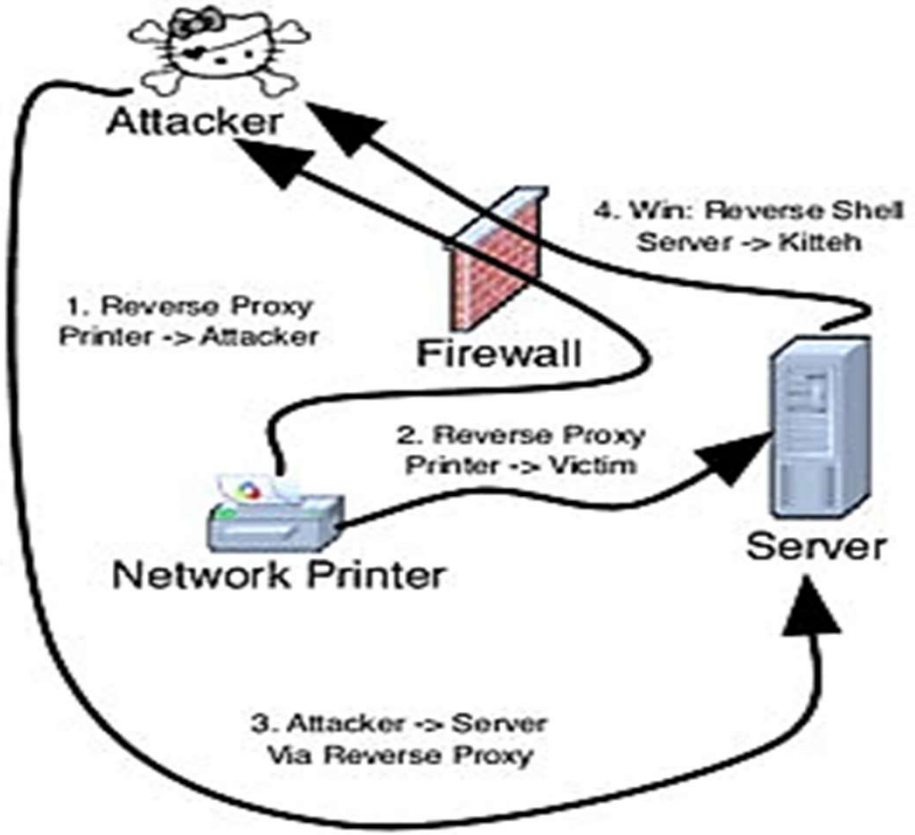
▪ Firmware Attack (Jarang Dibicarakan!)

Attacks against the hardware and firmware of a device stand as some of the highest impact threats facing modern organizations. Firmware retains the highest privileges, allows attackers to bypass traditional controls, and grants a higher level of persistence. The firmware layer has also quickly become one of the most active areas of cybersecurity with attackers increasingly setting their sights on the area of the enterprise where vulnerabilities are plentiful and defenses are often weakest.

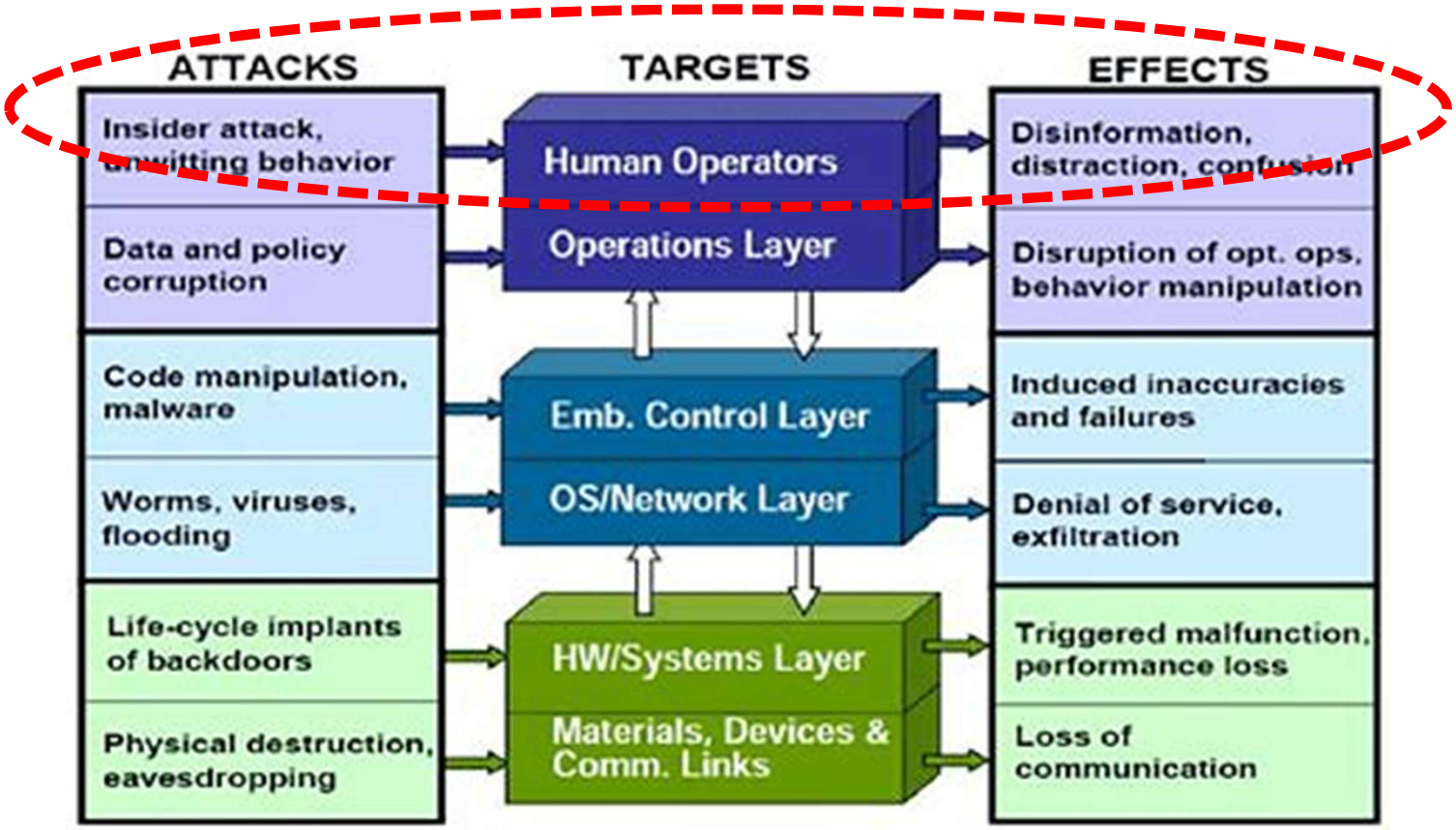
Firmware and hardware attacks are also significantly different from traditional malware and network threats. Security teams must be prepared to defend against a new set of attacker strategies, vectors, and understand how the wide variety of firmware components can be used as part of a persistent attack.

**Source: Anatomy of a Firmware Attack by Eclypsium*

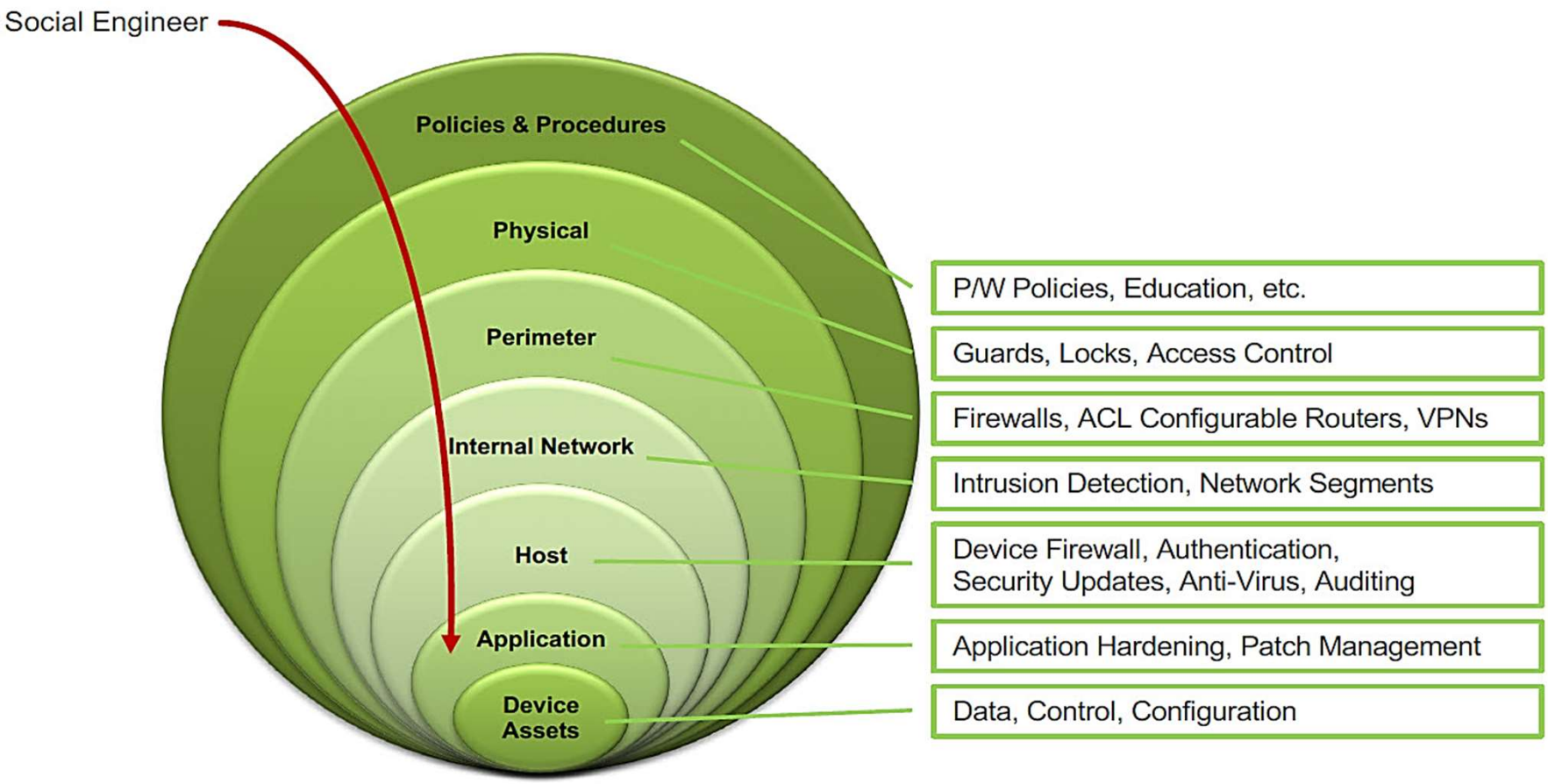
▪ Firmware Attack : Dampaknya



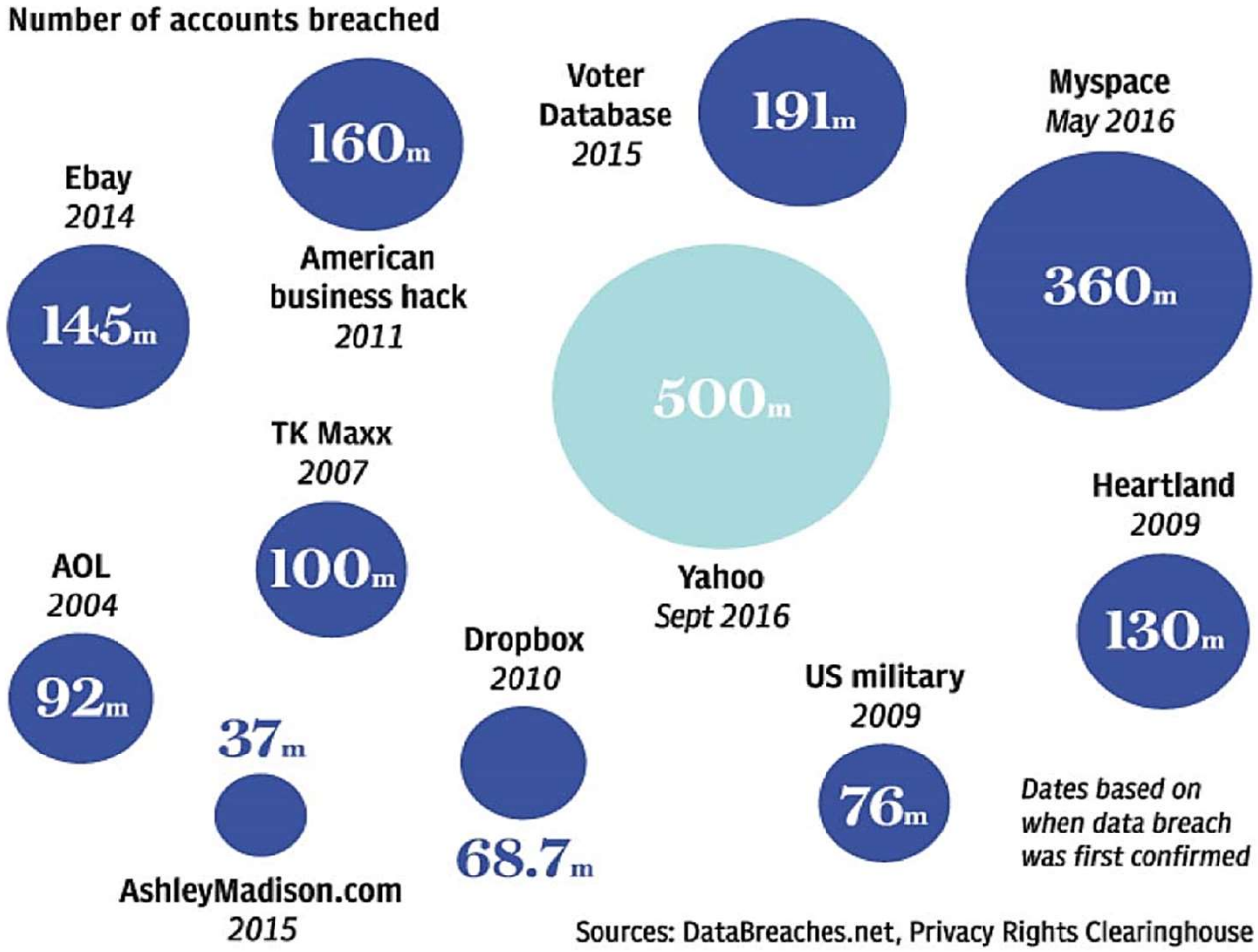
Yang Diserang : The Weakest Link!



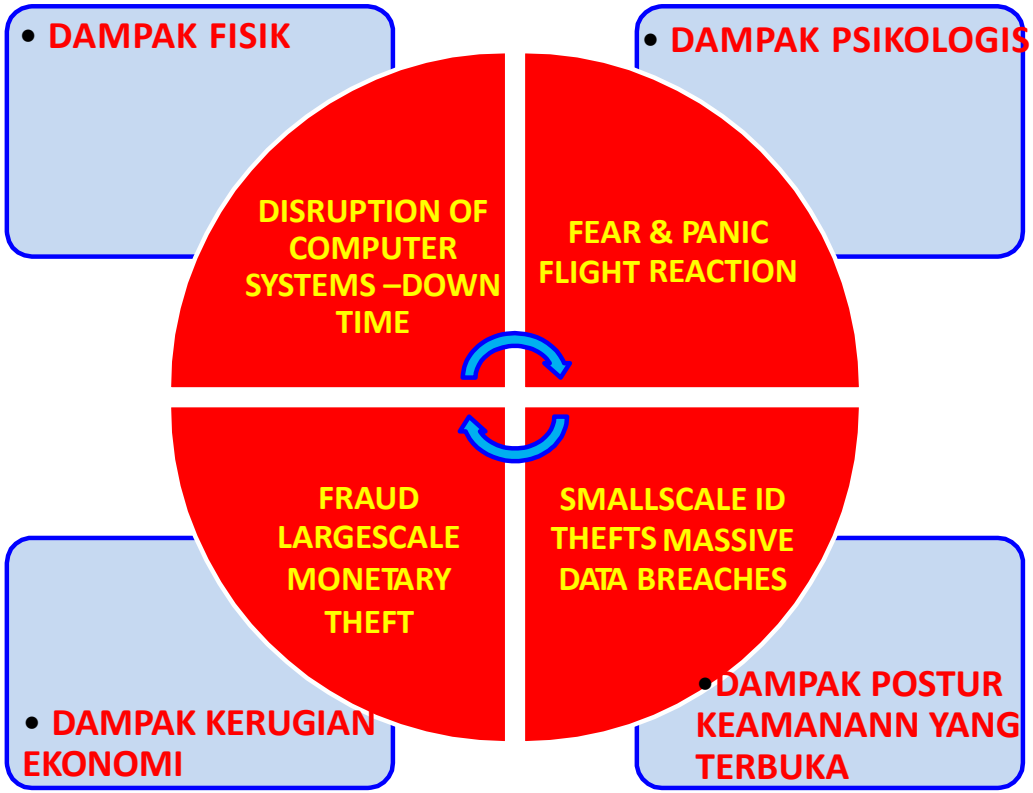
SOCENG Sudah Merambah Ke Dalam Tehnologi



Perusahaan Besar Sudah Mengalami SOCENG

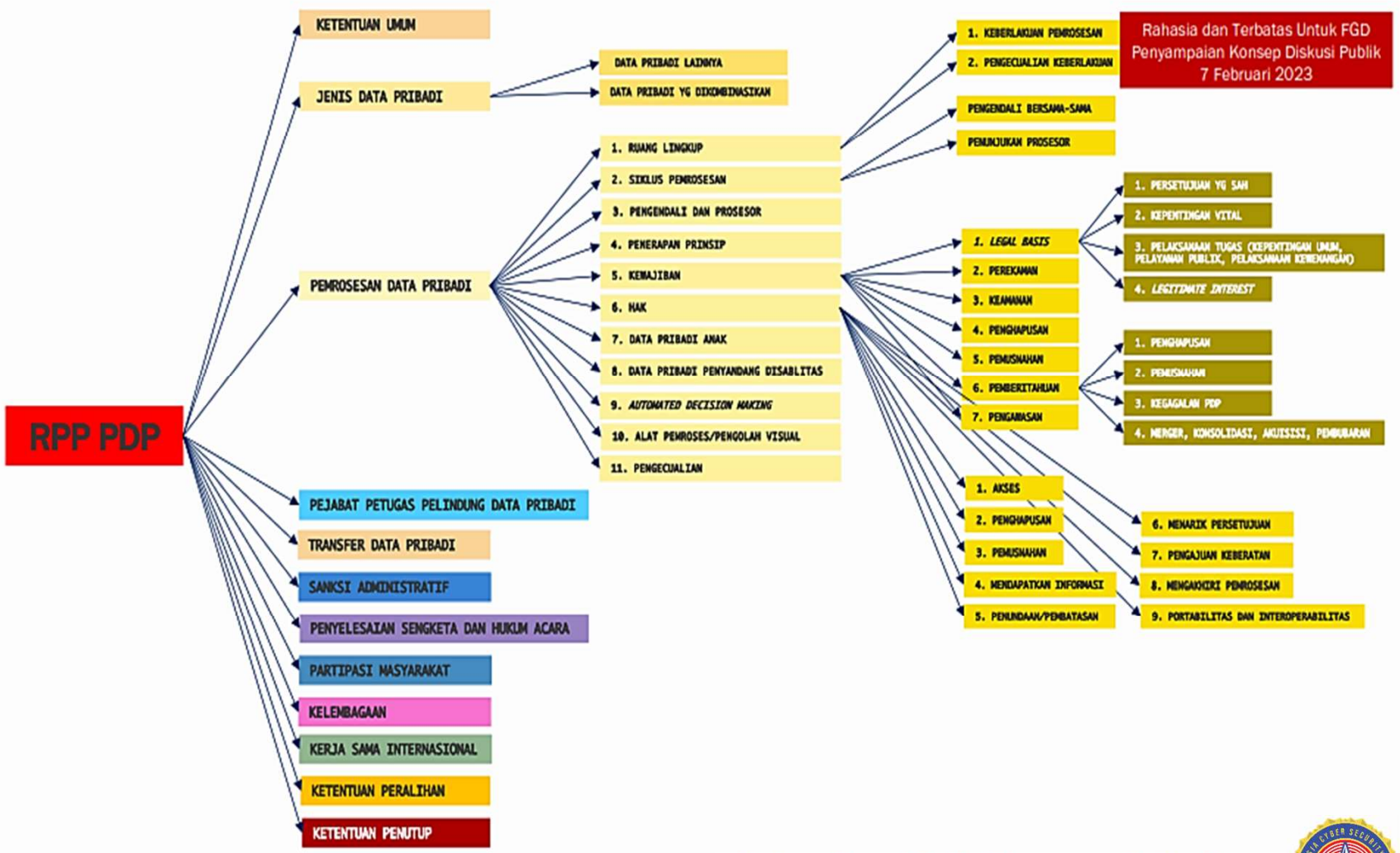


Dampak Dari HTAG Siber



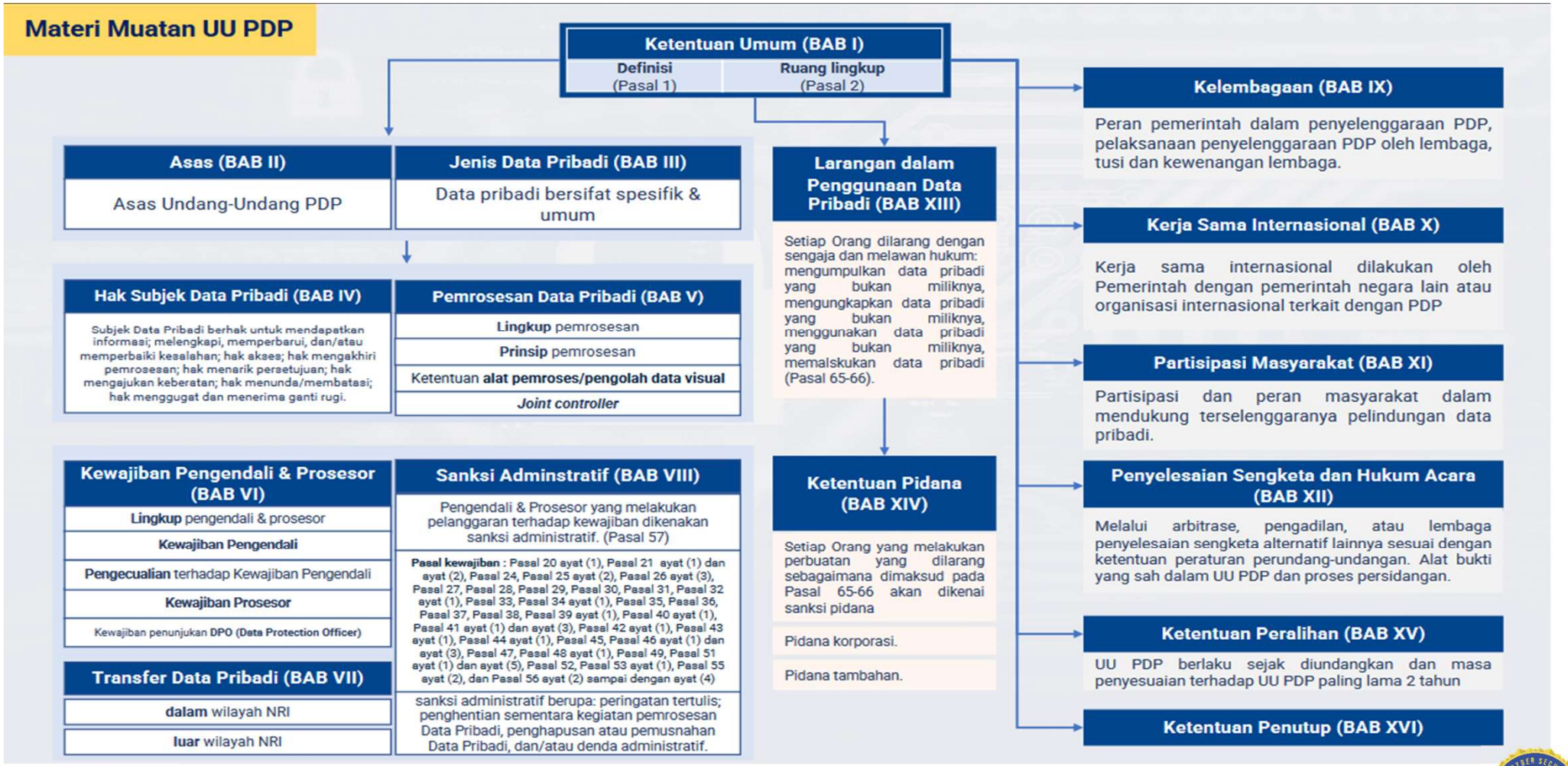
Bagan Tubuh UU No. 27 Tahun 2022

UU 27/2022
PELINDUNGAN DATA PRIBADI



Rahasia dan Terbatas Untuk FGD
Penyampaian Konsep Diskusi Publik
7 Februari 2023

Materi Muatan UU No. 27 Tahun 2022



Amanat Pelindungan Data Pribadi

UU 27/2022
PELINDUNGAN DATA PRIBADI

Rancangan Peraturan Pemerintah

10 + Amanat Baru
UU No. 27/2022

1. Pengajuan Keberatan atas Pemrosesan Secara Otomatis (*Pasal 10*)
2. Pelanggaran Pemrosesan Data Pribadi dan Tata Cara Pengenaan Ganti Rugi (*Pasal 12*)
3. Hak Portabilitas dan Interoperabilitas (*Pasal 13*)
4. Pelaksanaan Pemrosesan Data Pribadi (*Pasal 16*)
5. Penilaian Dampak Pelindungan Data Pribadi (*Pasal 34*)
6. Tata Cara Pemberitahuan Dalam Hal Penggabungan, Pemisahan, Pengambilalihan, Peleburan, atau
7. Pembubaran Badan Hukum (*Pasal 48*)
8. Pejabat atau Petugas yang Melaksanakan Fungsi Pelindungan Data Pribadi (*Pasal 54*)
9. Transfer Data Pribadi ke Luar Wilayah Hukum Negara Republik Indonesia (*Pasal 56*)
10. Tata Cara Pengenaan Sanksi Administratif (*Pasal 57*)
11. Tata Cara Pelaksanaan Wewenang Lembaga (*Pasal 61*)

Fakta – Fakta Terbaru Global : KERUGIAN!

Global Cybercrime Damage Costs:

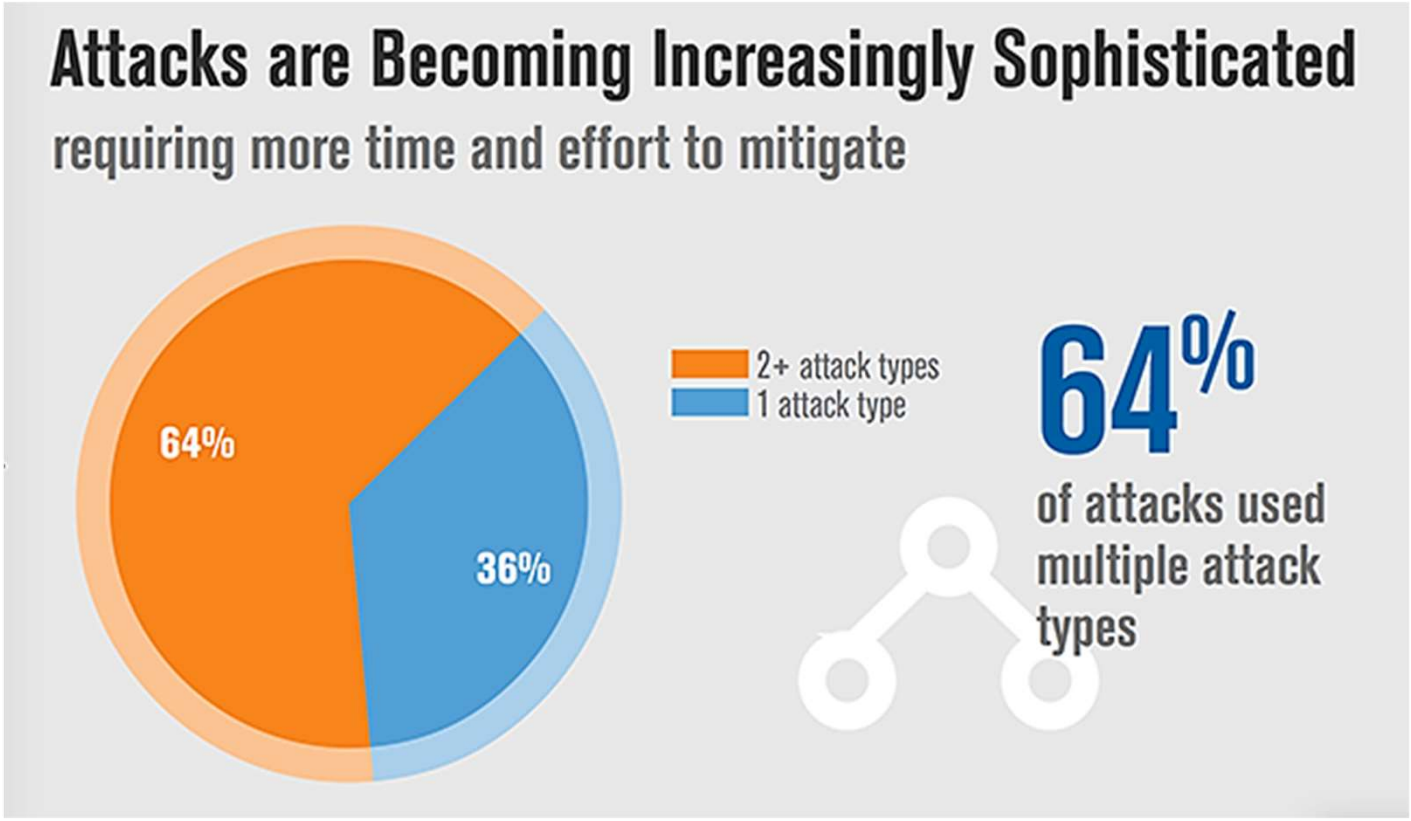
- $6 Trillion USD a Year. *
- $500 Billion a Month.
- $115.4 Billion a Week.
- $16.4 Billion a Day.
- $684.9 Million an Hour.
- $11.4 Million a Minute.
- $190,000 a Second.

ALL FIGURES ARE PREDICTED BY 2021

CYBERSECURITY VENTURES

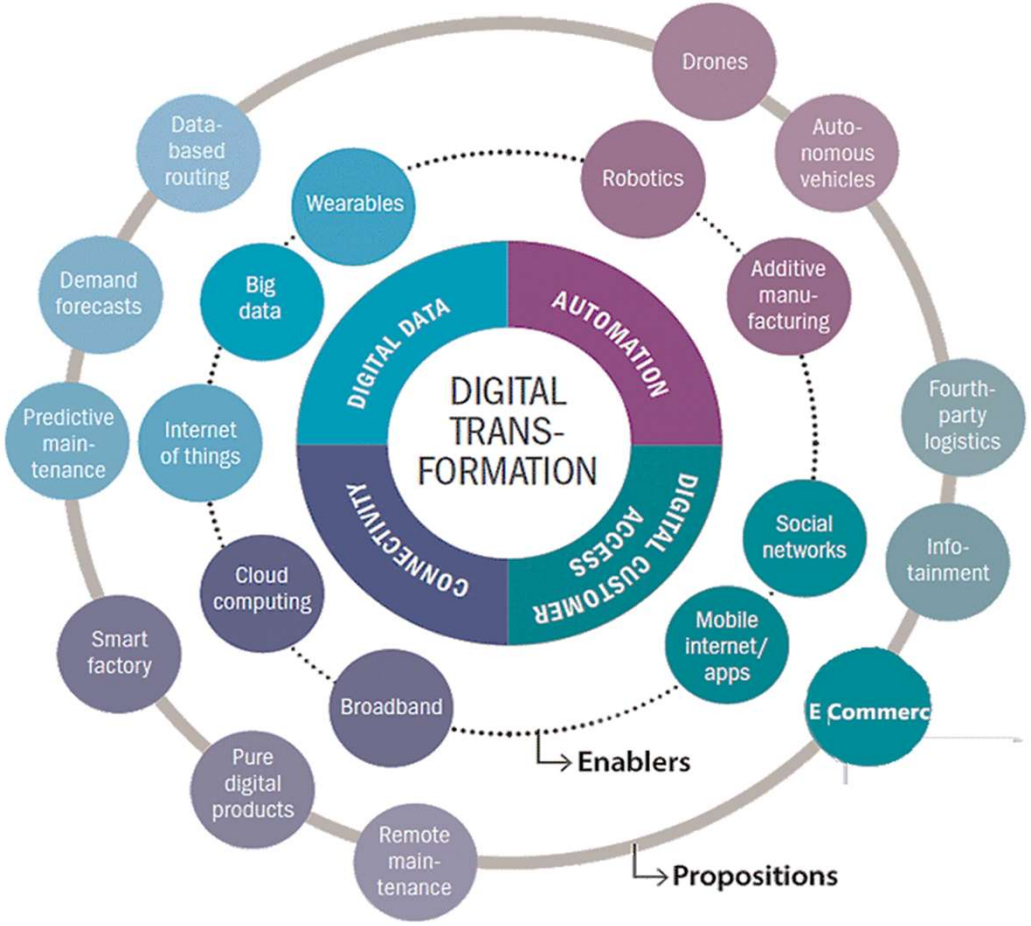
* SOURCE: CYBERSECURITY VENTURES

INGAT : Ancaman Siber Tidak Pernah Tunggal!



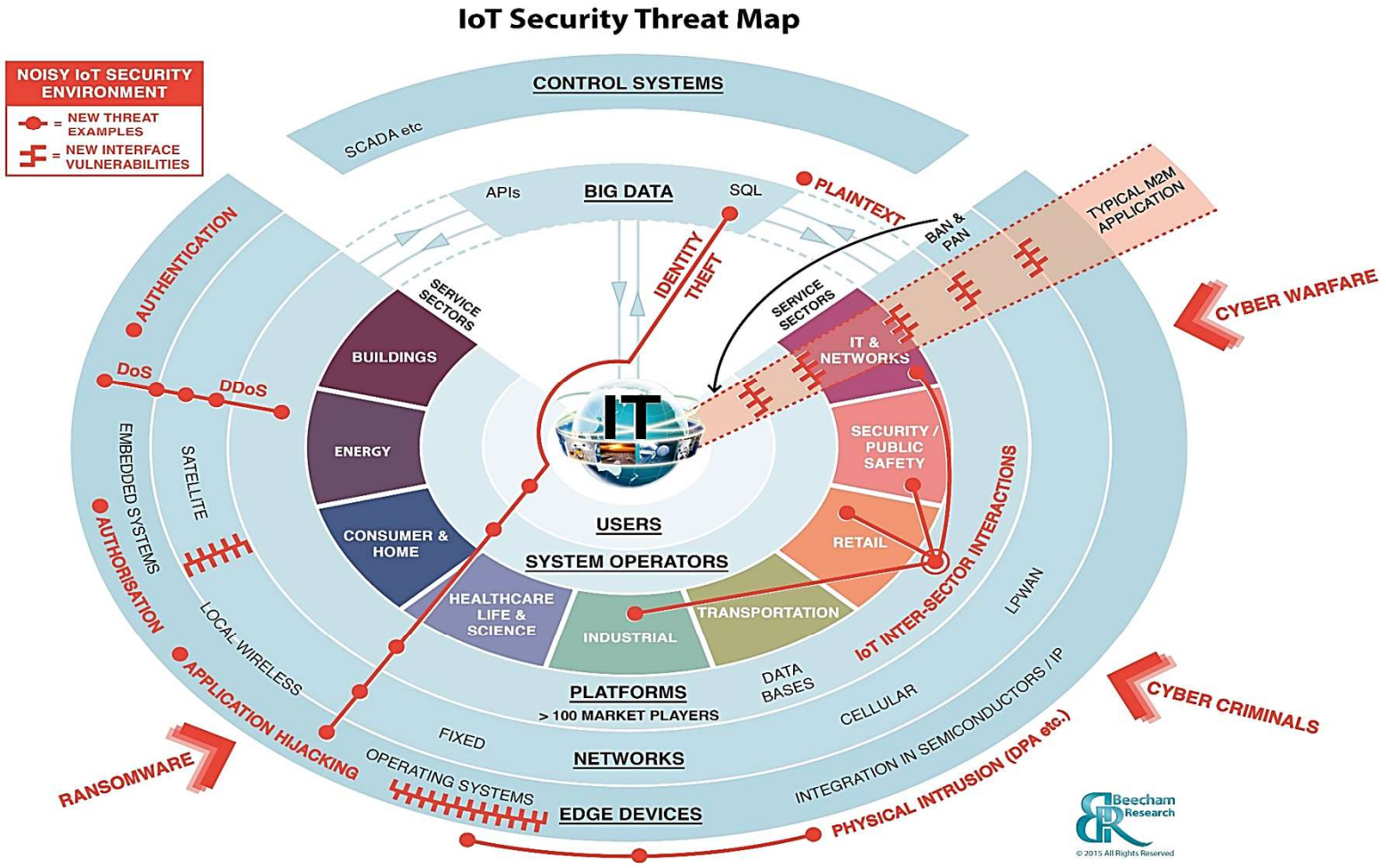
*Source : Verisign Q2 2016 DDoS Trends: Layer 7 DDoS Attacks a Growing Trend

Tehnologi Baru Memperbesar Resiko HTAG

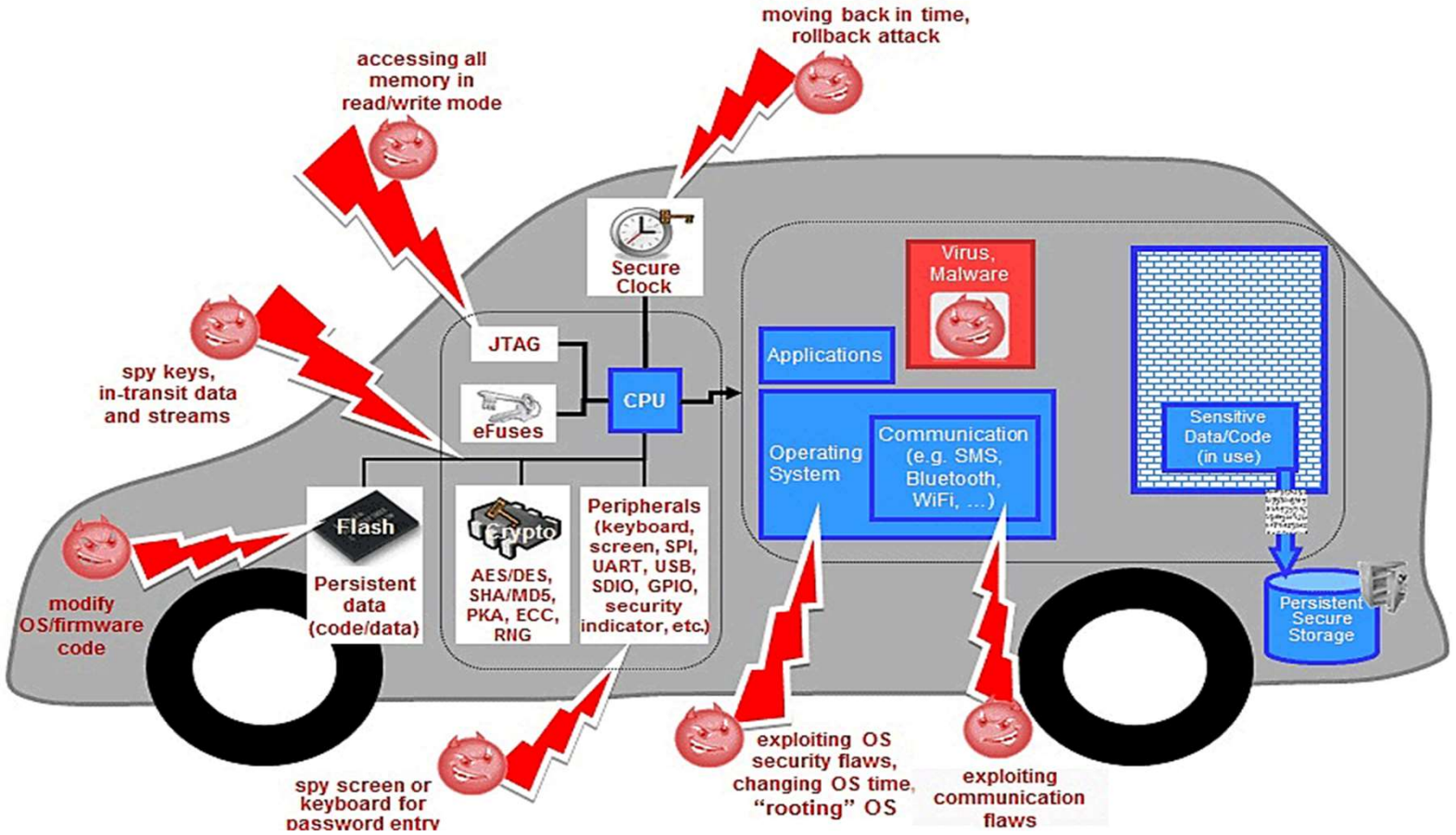


Digital Transformation

Kerentanan Tehnologi Baru: IoT & Potensi Resiko-resikonya



Kerentanan Tehnologi Baru: Kendaraan Listrik

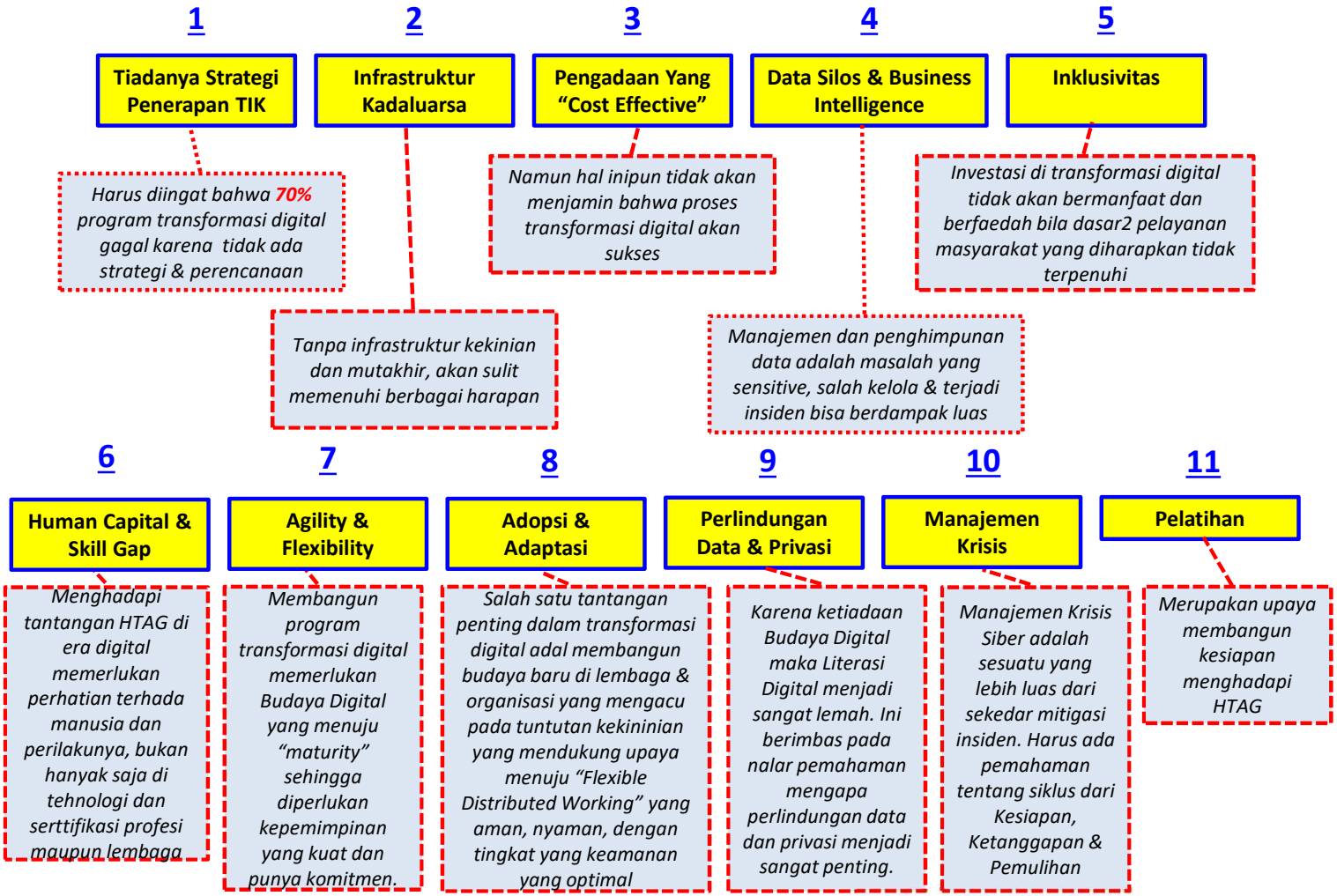


Tantangan Transformasi Digital Yang Dilupakan

1. Proses dan membangun Transformsi Digital bukan sekedar hanya melihat dari sisi pengadaan tehnologi belaka, namun harus mengedepan pemahaman bagaimana kita mampu menyiasati tantangan dalam konsep membangun kesiapan ***"PEOPLE – PROCESS-TECHNOLOGY" (PPT)***
2. Program Transformasi Digital tidak bisa instan dan seketika karena diperlukan perencanaan strategis yang dimulai dari :

   - RISET
   - PERENCANAAN
   - MOTIVASI
   - KEPEMIMPINAN (Leadership That Understand)
3. Mengembangkan program Transformasi Digital PASTI akan menghadapi kendala, terutama dalam hal **ANGGARAN, PERANGKAT & INFRASTRUKTUR YANG KADALUARSA** dan **SUMBER DAYA LAINNYA**.
4. Hambatan, Tantangan, Ancaman & Gangguan Siber **(Ancaman Siber)**
5. Diperlukan strategi pengembangan program **Tranformasi Digital** yang menyeluruh yang **berkelanjutan**, **berkesinambungan** dan memiliki **akuntabilitas publik.**

11 Parameter Penentu Transformasi Digital



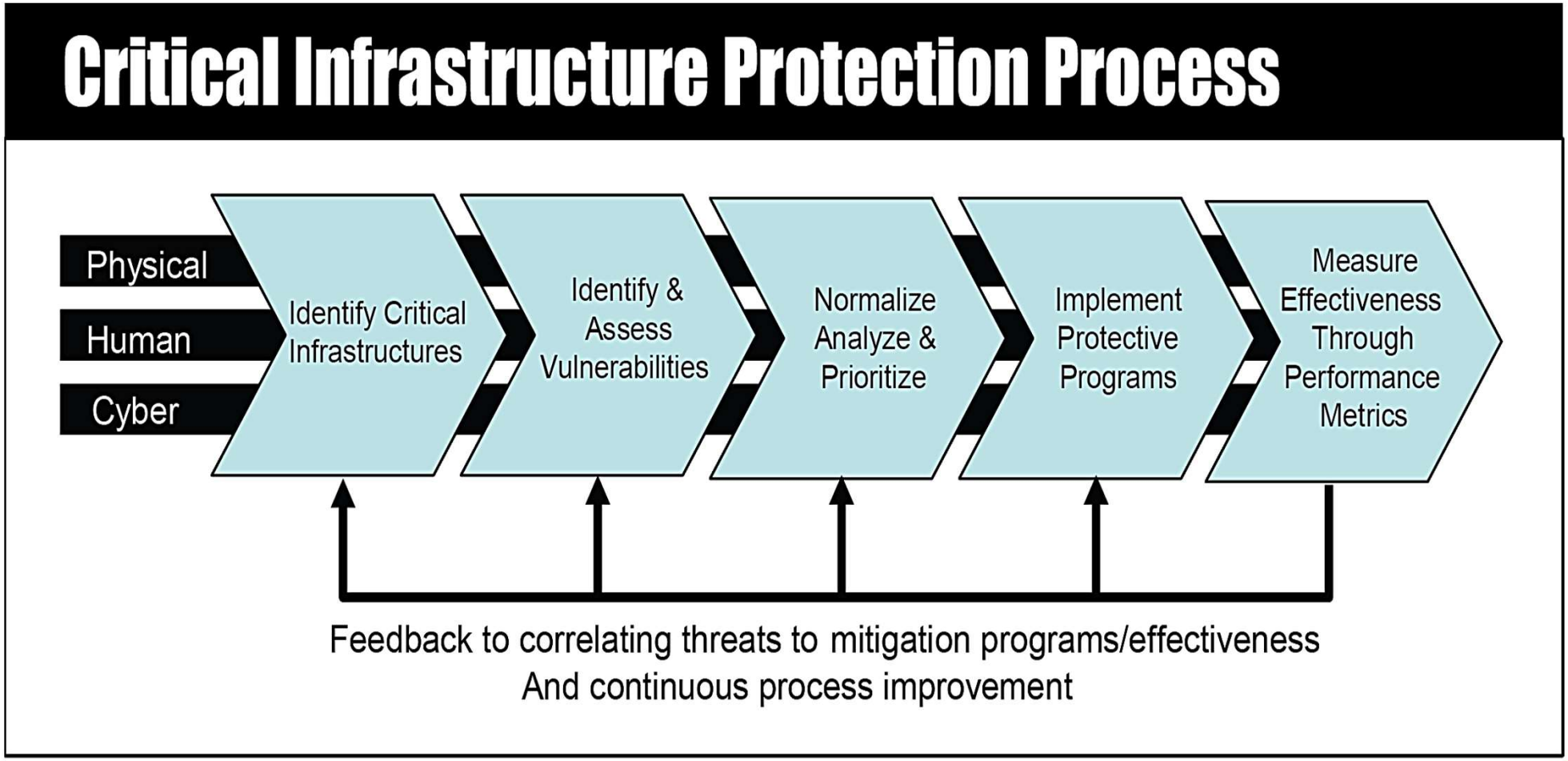
Manajemen Kepemimpinan Berdasarkan Resiko

Hambatan Lainnya : Masalah Budaya Digital

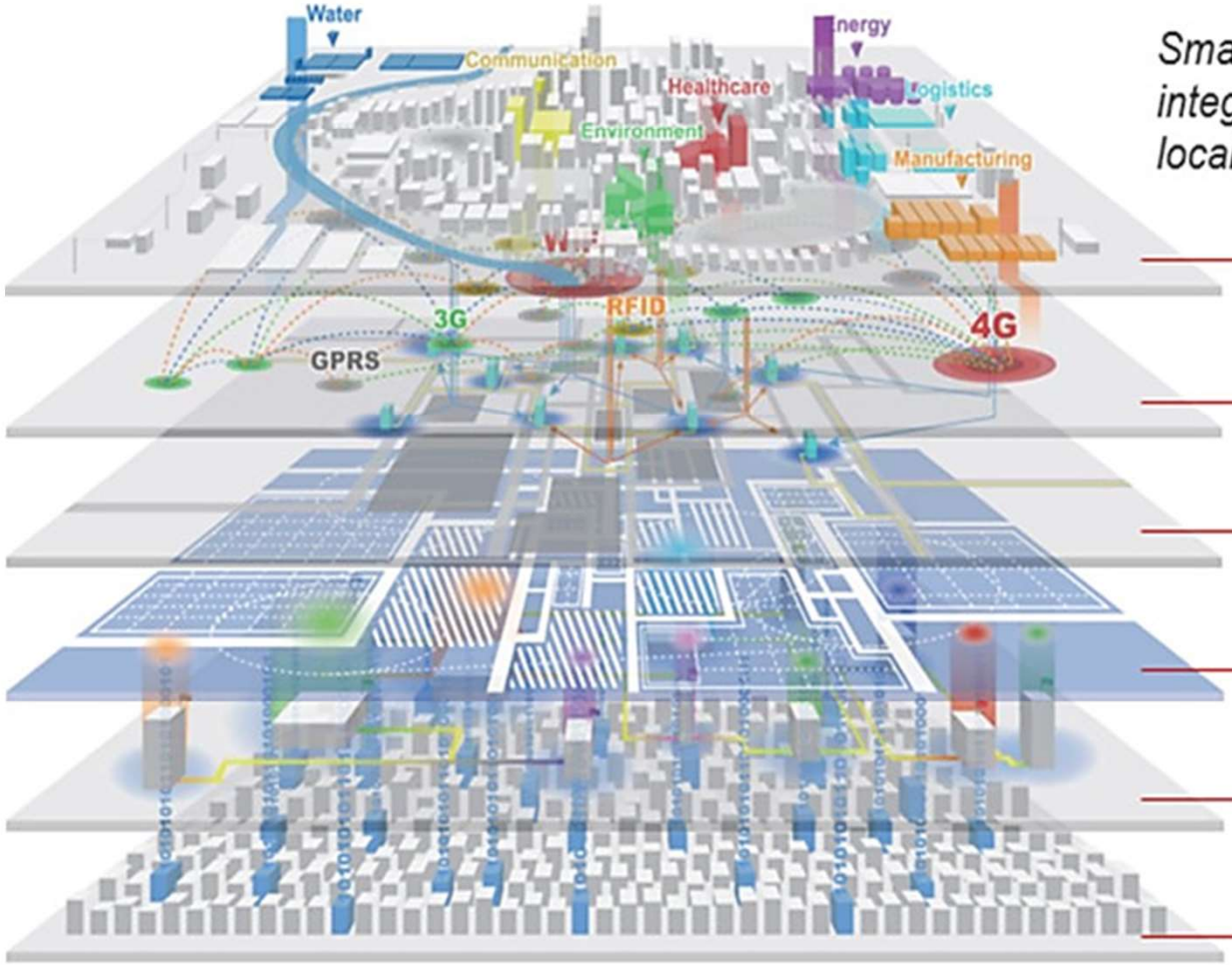
"Menuju Pembangunan Akal Sehat Di Era Digital"

Lantas Bagaimana Kita Bisa Mengatasinya?

Perlu Pemahaman Konsep: PEOPLE-PROCESS-TECHNOLOGY



Gambaran Besar: REALITA



Smart Cities are complex organisms that integrate solutions and infrastructure to meet local goals.

Citizens, Business, Organizations

Digital Networks And Services

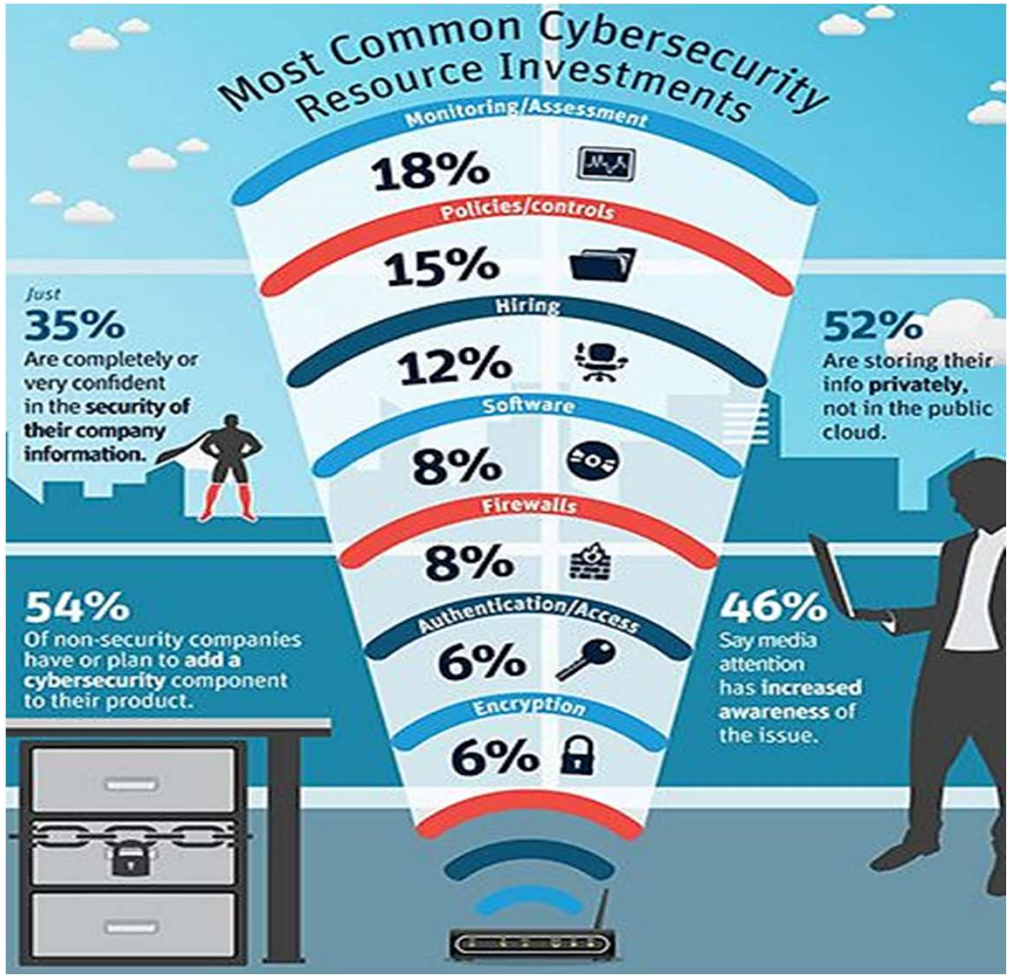
Government Operations And Services

Urban Planning

IT Infrastructure And Operations

Physical Infrastructure

Investasi Sumber Daya



Six Ware Cyber Security Framework

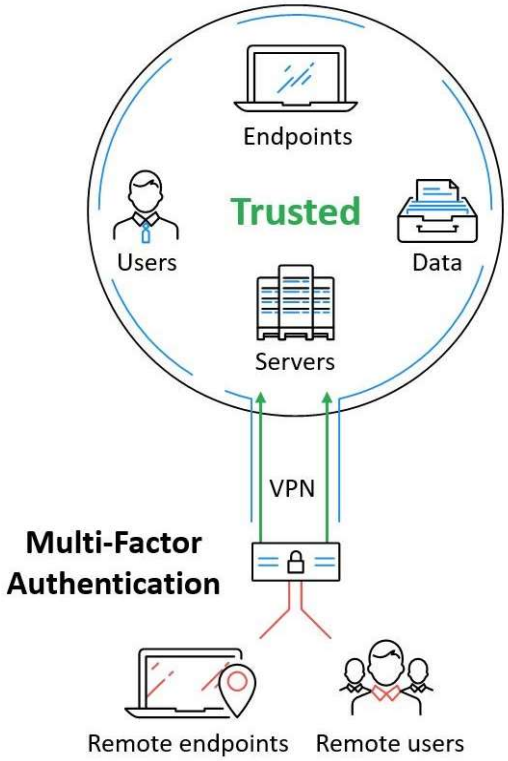
Factors	Variables	Sub-variables	Indicators	Infosec References
Brainware	*CISO, etc.*	*Security training, etc.*	*Security Awareness*	*CISSP, CISA, etc.*
Hardware	*Server Farms*	*USB, etc.*	*No compromises*	*Bench marking, etc.*
Software	*Application*	*MS Office, etc.*	*No pirated Appl. etc.*	*Regular updates,etc*
Infrastructureware	*Network Infrastructure*	*Firewalls.* *IDS.* *DMZ, etc.*	*No network security breaches, etc.*	*Self penetration testing, etc.*
Firmware	*Security hand book*	*Bussiness Continuity Plan*	*Good Bussiness pro- cesses*	*NIST.* *ISO 27001, etc.*
Budgetware	*Sufficient budget*	*Buy software licenses, etc.*	*Licences always updated, etc.*	*Allocated budget policy, etc.*

"ZERO TRUST"

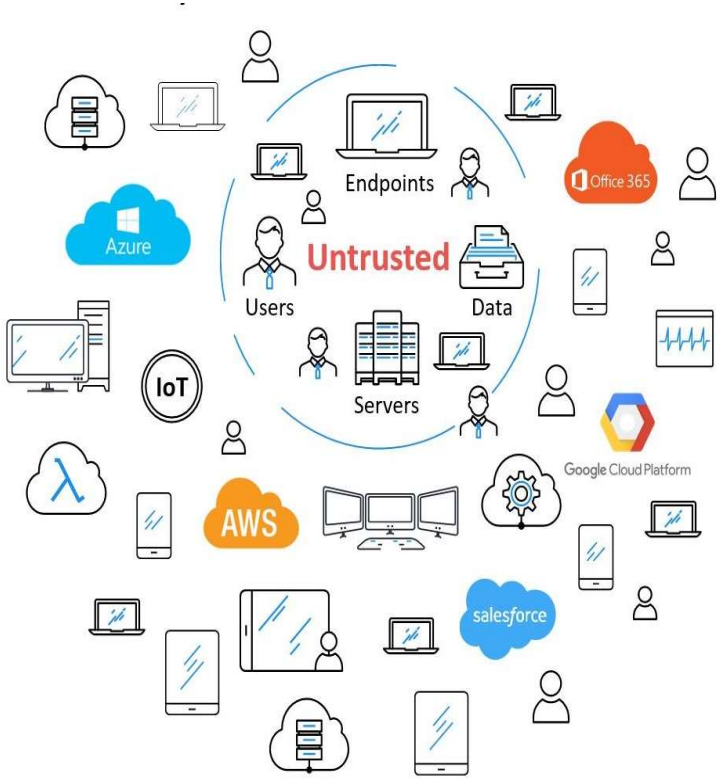
Zero Trust sendiri adalah prinsip serta kerangka kerja keamanan dan ketahanan siber yang mengharuskan semua pengguna, baik di dalam atau di luar jaringan untuk selalu melakukan **otentikasi** dan **meminta ijin** untuk mengakses aplikasi dan data sehingga dapat melindungi aplikasi dan pengguna dari ancaman kejahatan siber.

"ZERO TRUST" – Pola Pikir Yang Dilupakan!

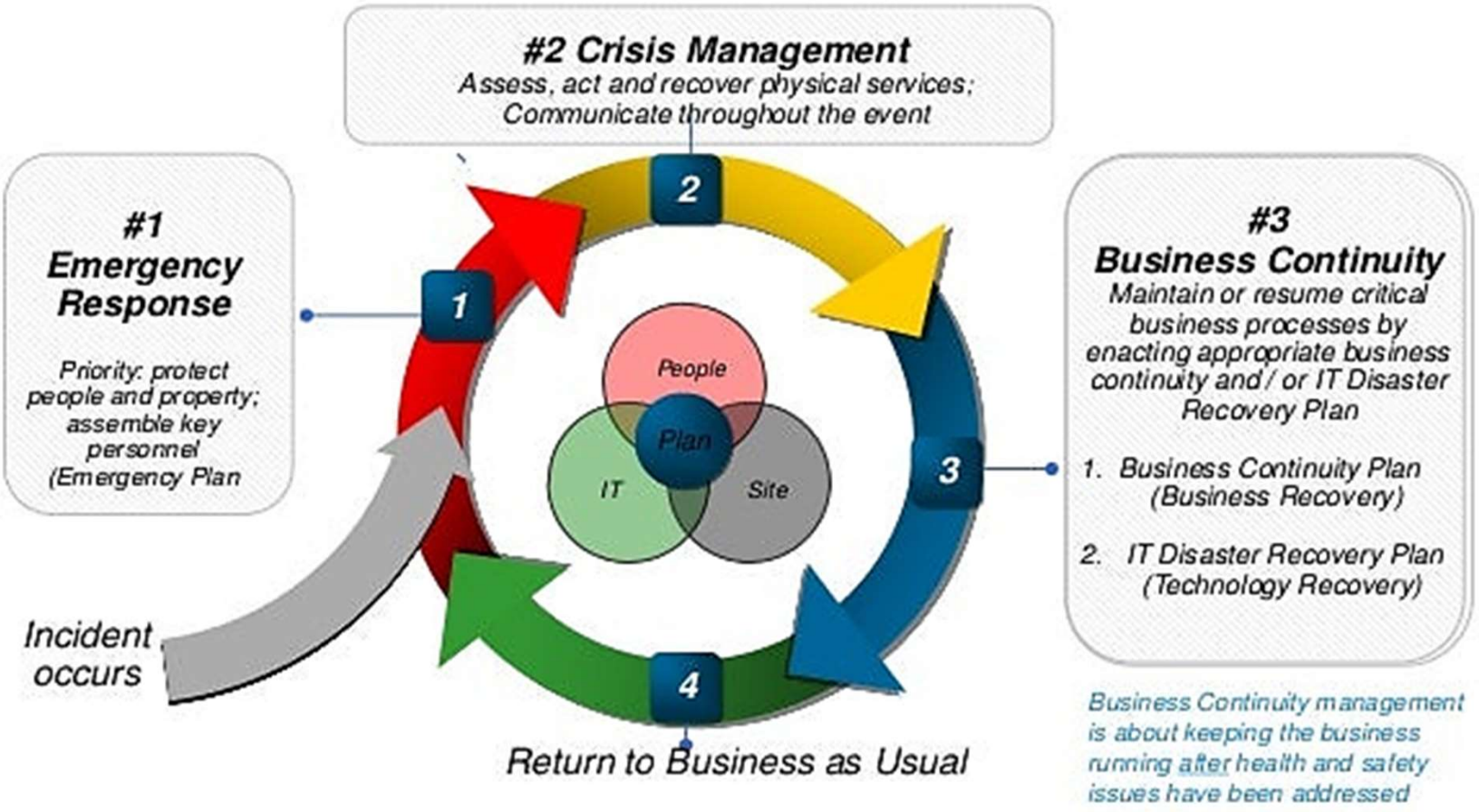
Pola Pikir Lama



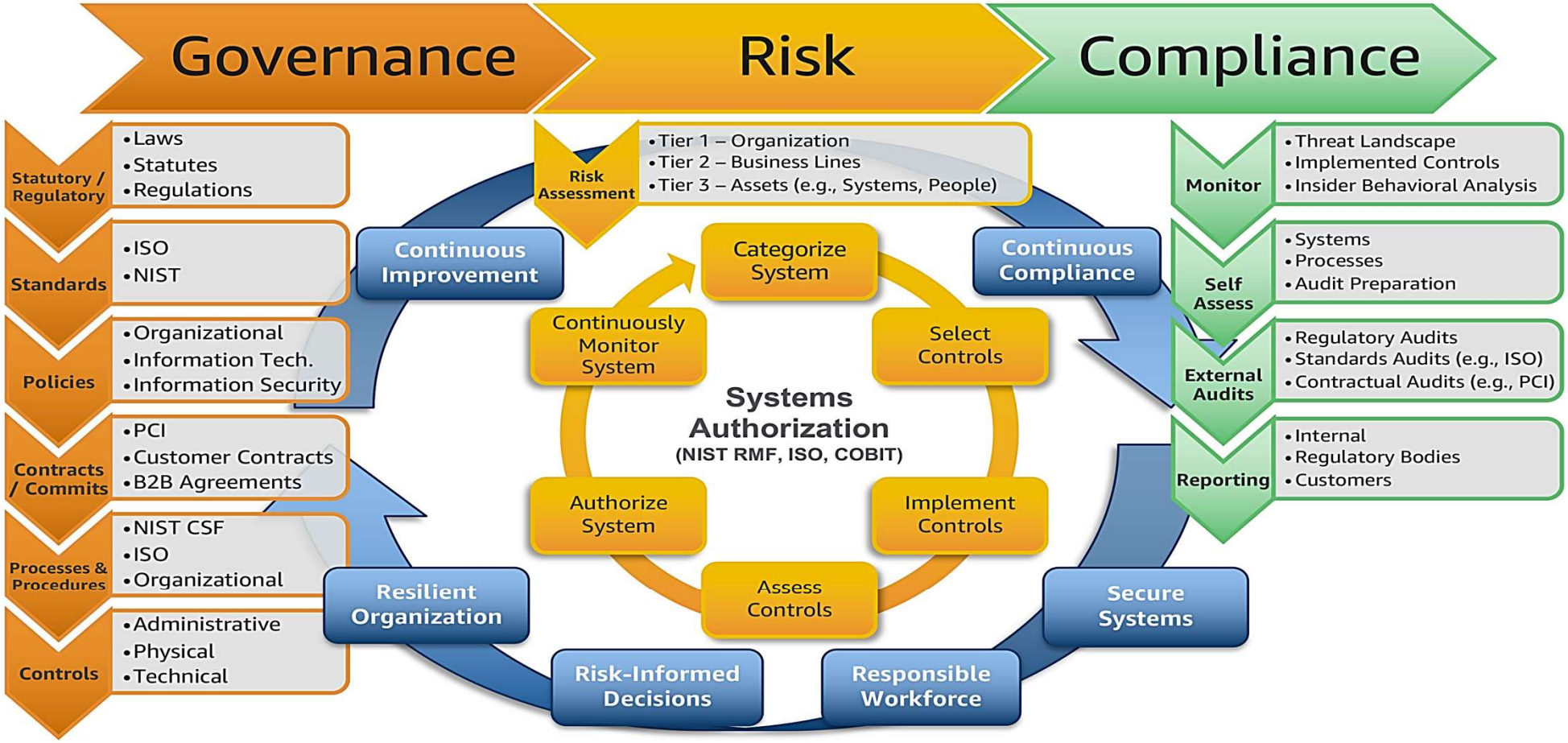
Pola Pikir Baru



Manajemen Krisis: Business Continuity



Pemahaman Standar Kompetensi & Sertifikasi Minimal



Ancaman Siber Kini Semakin Kompleks & Berbahaya!

Setelah menyaksikan dan mengalami situasi dan kondisi tehnologi digital secara global, yang mana tingkat resiko dan keamanannya juga semakin meningkat seiring dengan perkembangan dan pertumbuhan tehnologi digital itu sendiri maka semakin penting bagi kita semua untuk mengenal dan memahami sifat-sifat dan potensi ancaman siber bagi keamanan nasional.

Resiko ancaman siber sekarang sudah bergeser dari pola-pola yang selama ini kita kenal dan pahami. Sekarang mulai banyak muncul beragam bentuk ancaman dan serangan yang dapat mengganggu stabilitas negara, dapat mengganggu dunia usaha, dapat mengganggu perekonimian, dapat mengganggu postur polhukam dan juga dapat mengganggu rantai pasok. Dan ancaman-ancaman tersebut bukan hanya dapat menciptakan berbagai kerugian ekonomi yang tidak ternilai biayanya di berbagai sektor industri, namun juga dapat mengancam kehidupan bernegara dan demokrasi!

Dan, dengan semakin maju dan berkembangnya berbagai tehnologi diatas, resiko ancaman siber juga tidak bisa kita hilangkan dan eliminir, namun dapat kita atasi dan kelola untuk menekan dampak kerusakan dan kerugian yang dapat terjadi. Untuk dapat dan mampu mengelola resiko-resiko tersebut diperlukan upaya dan langkah-langkah untuk membangun budaya digital agar kelak dapat kita pergunakan sebagai sarana peringatan dini bagi ancaman-ancaman siber mendatang.

Dan...Kita Harus Semua Ingat Bahwa :

Dan Sekali Lagi..... Ingat!

"Going forward you won't be judged on whether you had a cyber incident, you will be judged on how you respond to it."

John O'Driscoll, Victorian Government Chief Information Security Officer

Tanggung-Jawab Bersama!

Terima Kasih!

INDONESIA CYBER SECURITY SUMMIT™ Jakarta, Indonesia 2023

Ardi Sutedja K.

Ketua & Pendiri

Indonesia Cyber Security Forum (ICSF)

chairman@icsf.or.id

HP: +62817835876

Indonesia Cyber Security Forum (ICSF), adalah Badan Hukum Perkumpulan Profesi yang didirikan berdasarkan Akta Notaris RA Mahyasari A. Notonagoro, SH, pada tanggal 16 November 2017 , dan dengan **Nomor Akta # 21**. Dan mendapatkan pengesahan berdasarkan **Keputusan Menteri Hukum & Hak Asasi Manusia RI No. # AHU-0017778.AH.01.07.Tahun 2017**

Cyber Security Is Everyone's Business