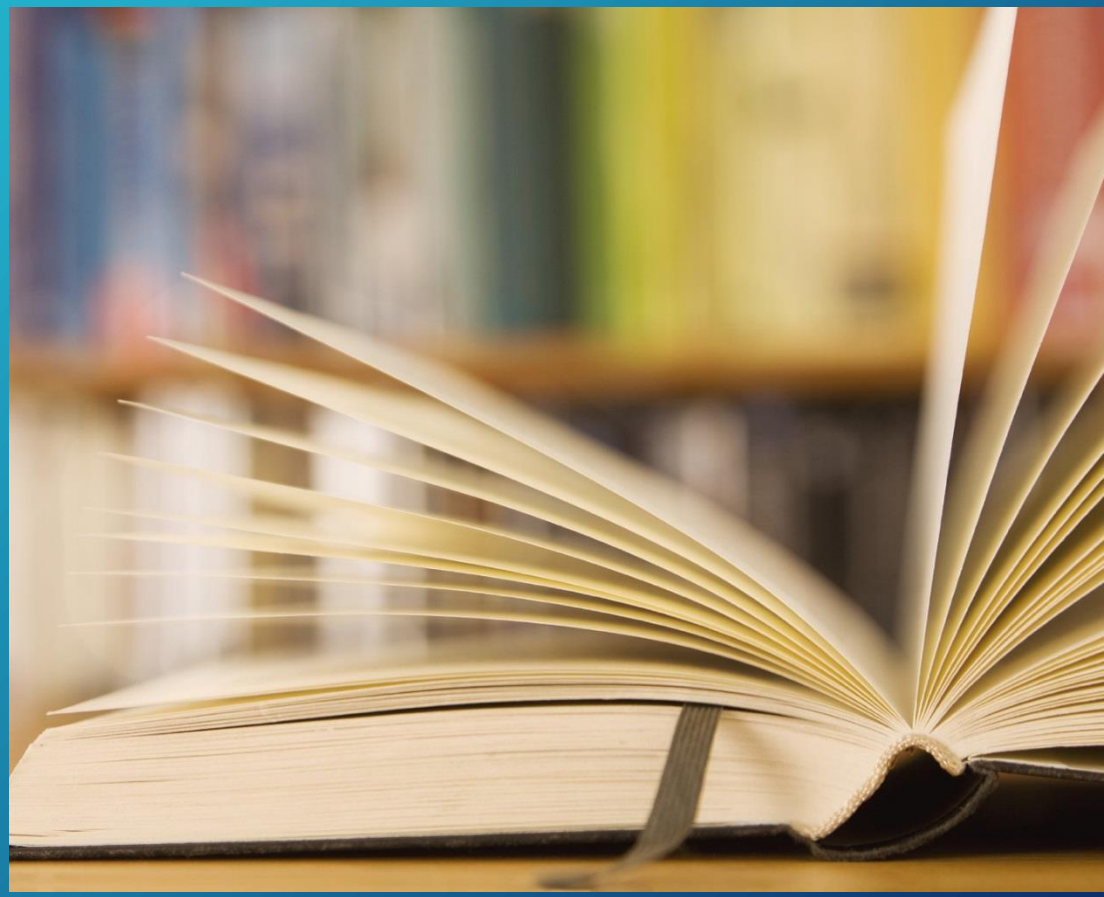
SEKOLAH TINGGI TEKNOLOGI
TERPADU NURUL FIKRI
CHARACTER BUILDING CAMPUS
STT - NF

PENGANTAR KEAMANAN KOMPUTER

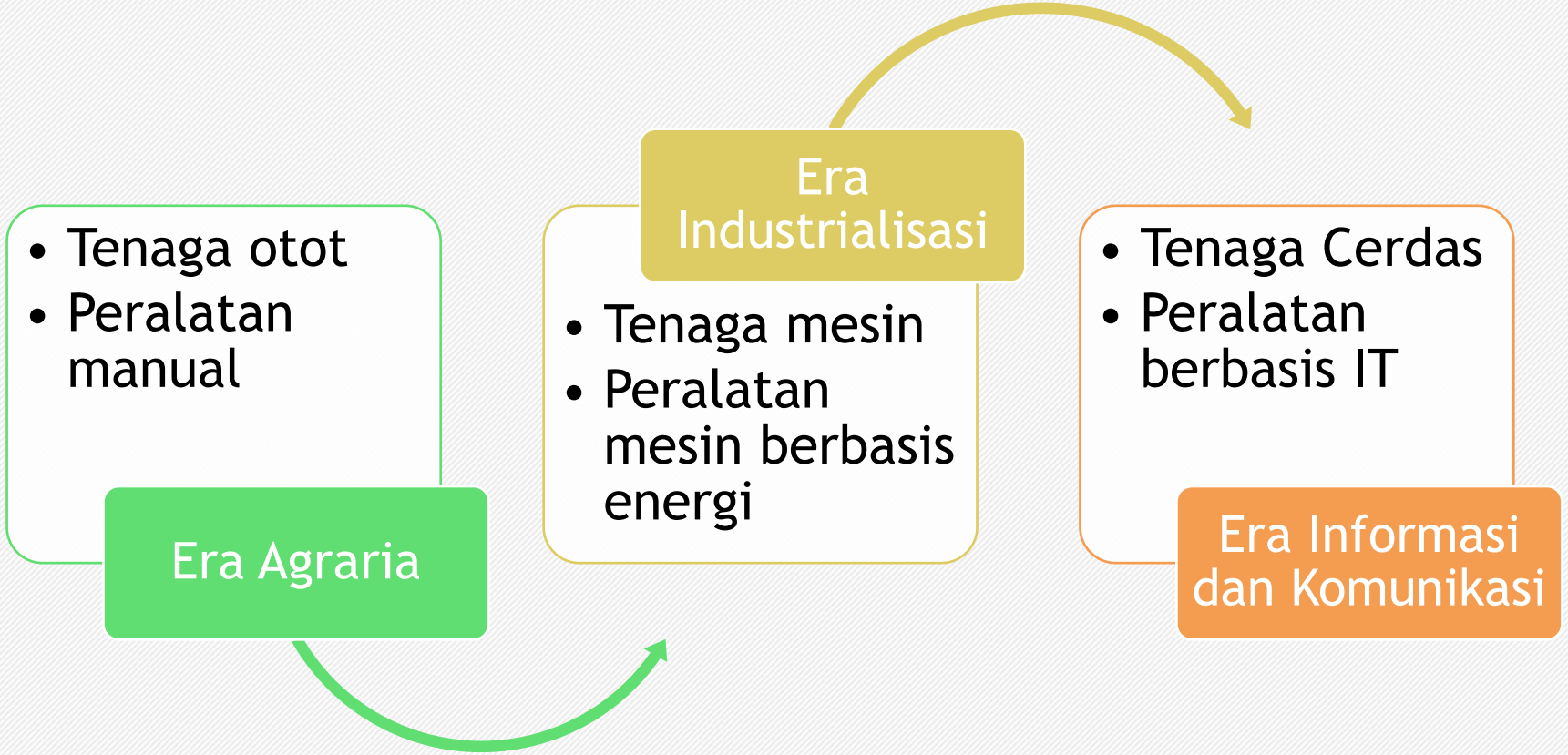
Keamanan Sistem Informasi – Aditya Putra, ST., MT.



Agenda

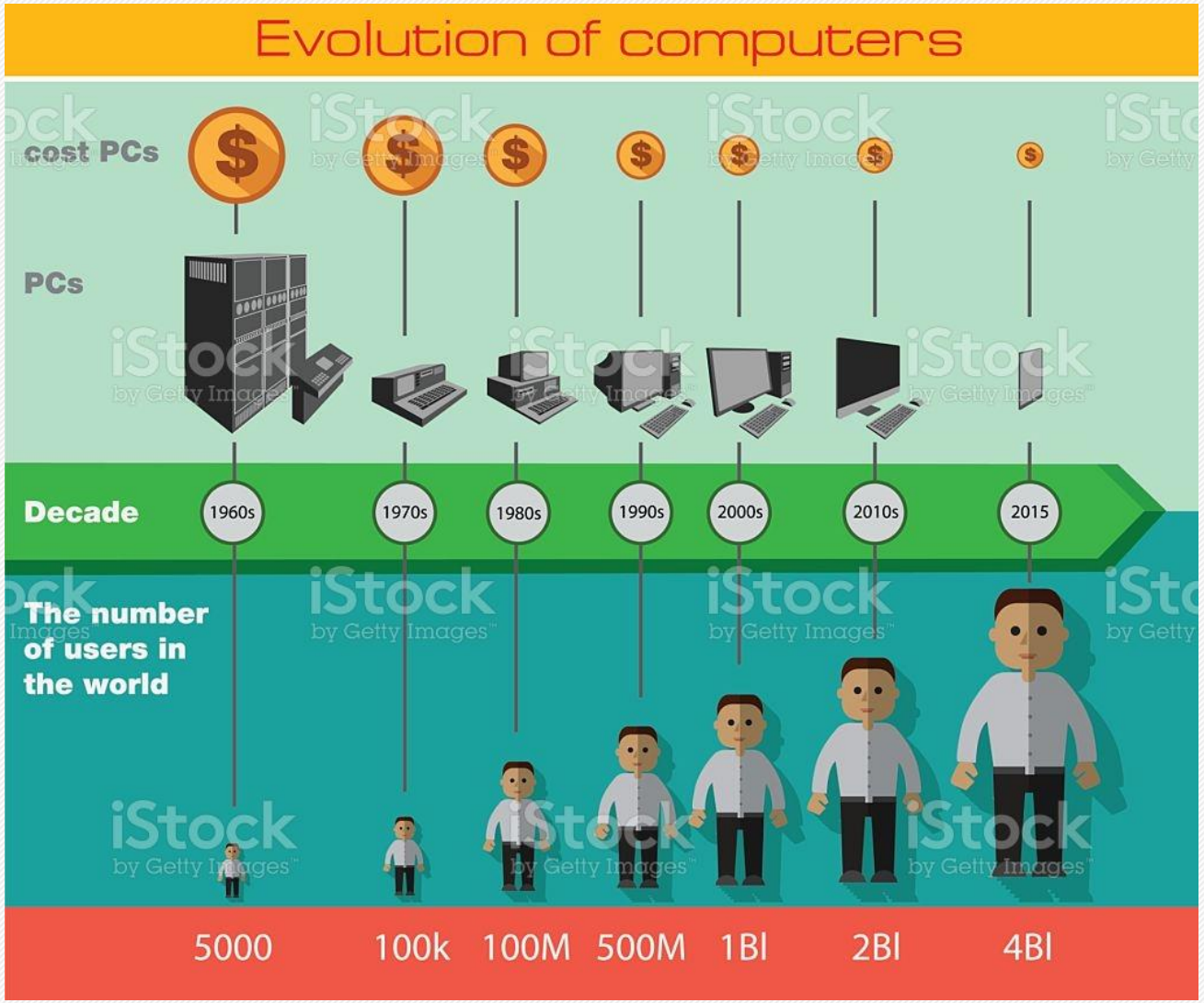
- Pengenalan Keamanan Komputer
- Sejarah Perkembangan Keamanan Komputer
- The Triad: CIA
- The Reverse Triad: DAD
- Pengendalian Keamanan Komputer
- Standar Keamanan Komputer
- ISO 27001

Pengenalan Keamanan Komputer



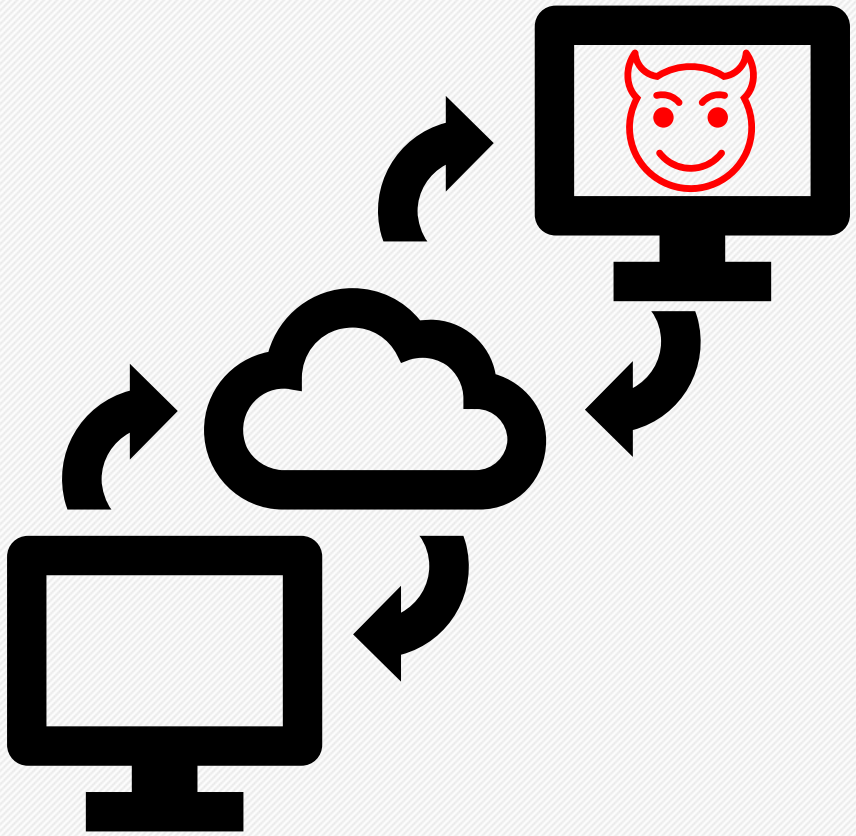
*Alvin Toffler dalam bukunya, **The Third Wave**

Pengenalan Keamanan Komputer



- Ukuran Komputer semakin kecil
- Harga computer semakin terjangkau
- Jumlah pengguna computer semakin tinggi
- Aktivitas yang dilakukan menggunakan computer semakin banyak karena perkembangan teknologi menuntut fitur yang banyak

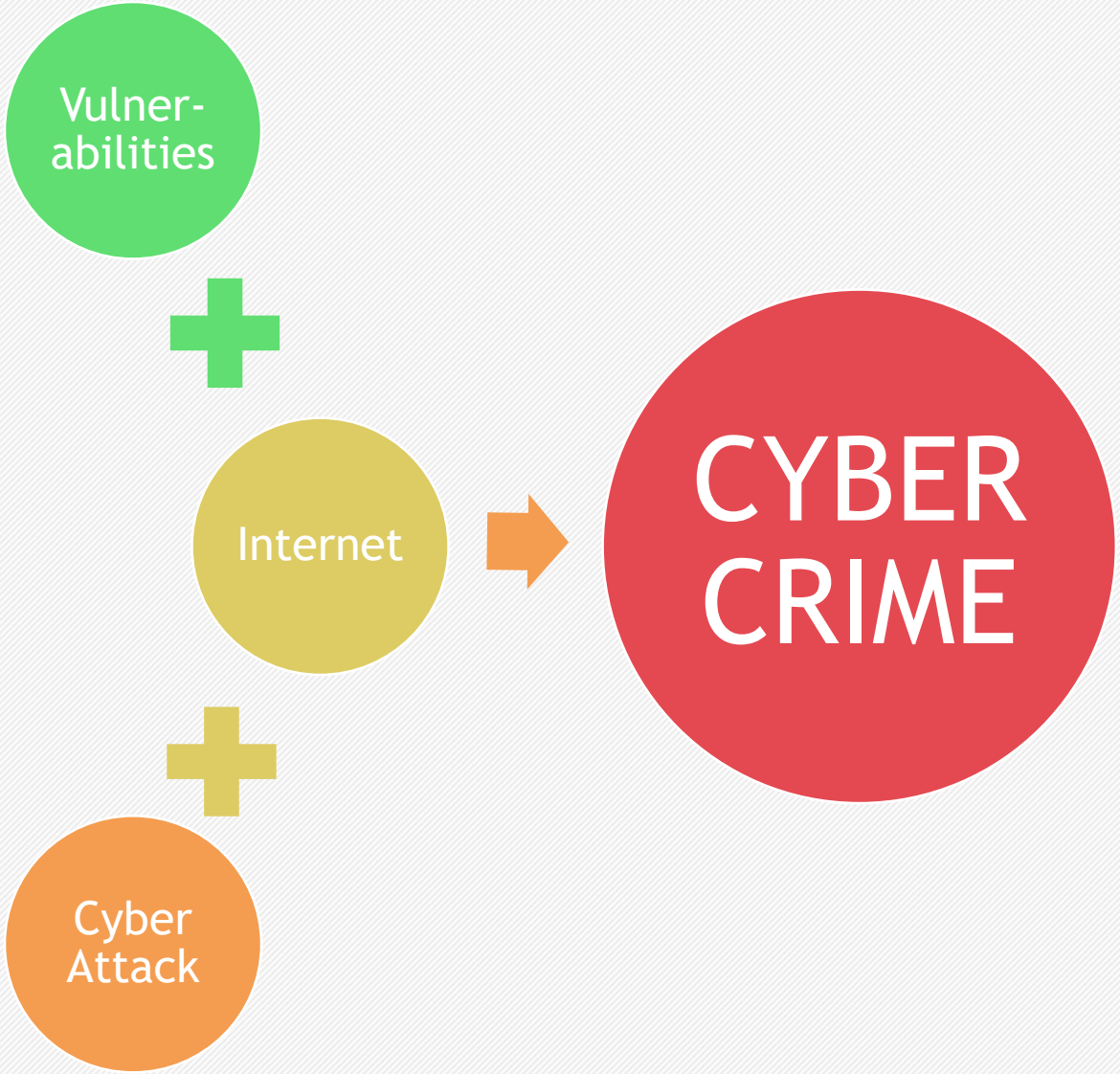
Pengenalan Keamanan Komputer



- Internet muncul dan digunakan oleh computer untuk transaksi data jarak jauh
- Transaksi data yang terjadi di internet semakin tinggi

- Ada gula ada semut
- Nilai data meningkat dan massif → mengundang orang yang tidak bertanggung jawab untuk berkeliaran di internet

Pengenalan Keamanan Komputer

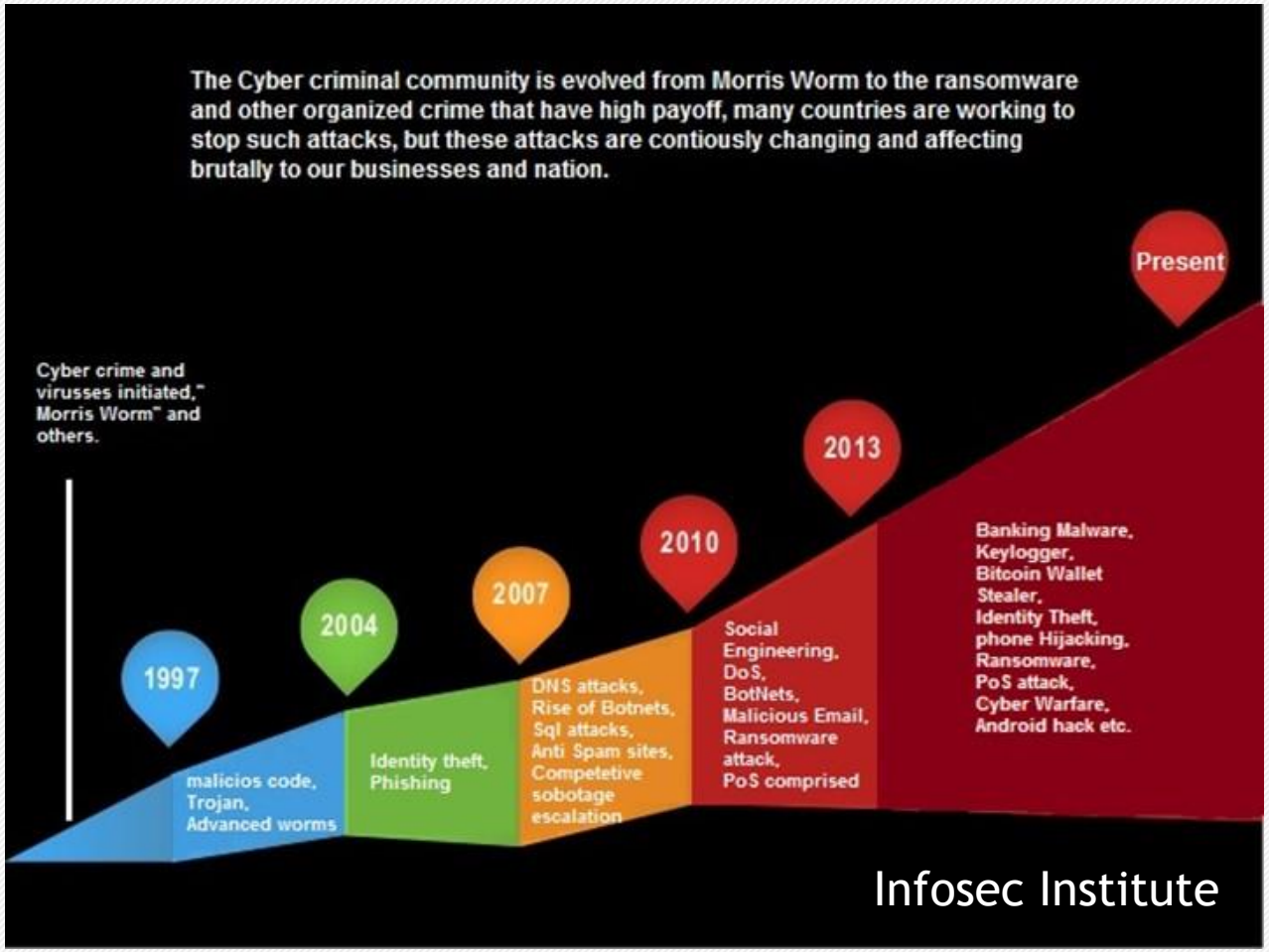


Cyber Crime (Kejahatan Siber) adalah akumulasi dari:

- Vulnerabilities (kerentanan) yang tercipta pada aplikasi
- Internet yang memungkinkan computer terhubung dengan jaringan computer lain
- Cyber Attack (Serangan Siber) yang dilakukan pihak luar pada suatu target computer

Vulnerability yang berpotensi dieksploitasi oleh hacker di internet adalah ancaman pada komputer

Sejarah dan Perkembangan Keamanan Komputer

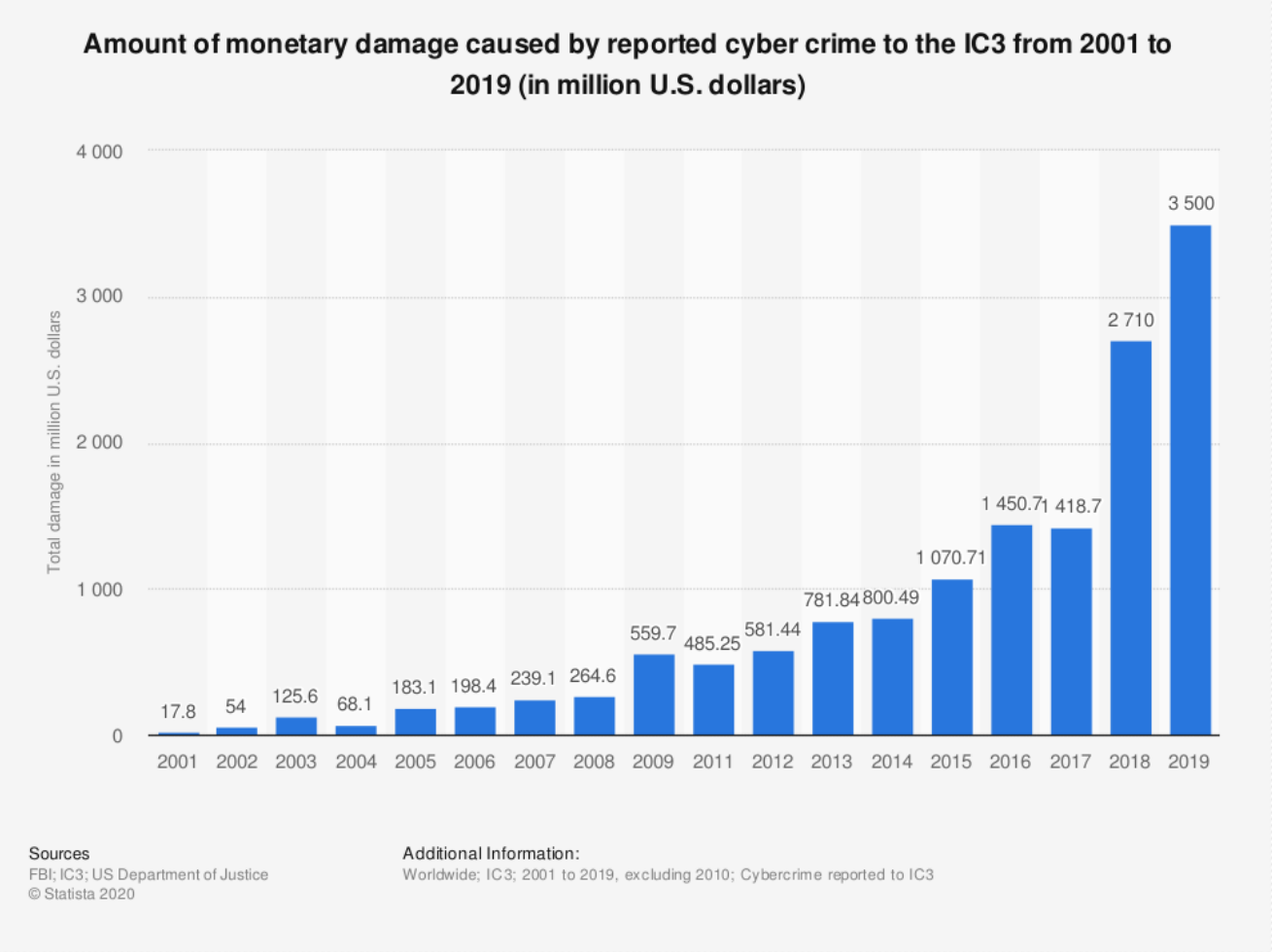


Cyber Attack (Serangan Siber) terus berevolusi mulai dari:

- Malicious code, trojan/worm/virus
- Identity theft, phising
- DNS, SQL Attack
- Social Engineering, DoS, Botnets, Ransomware
- Banking Malware, Bitcoin Waller Stealer, Android Hack

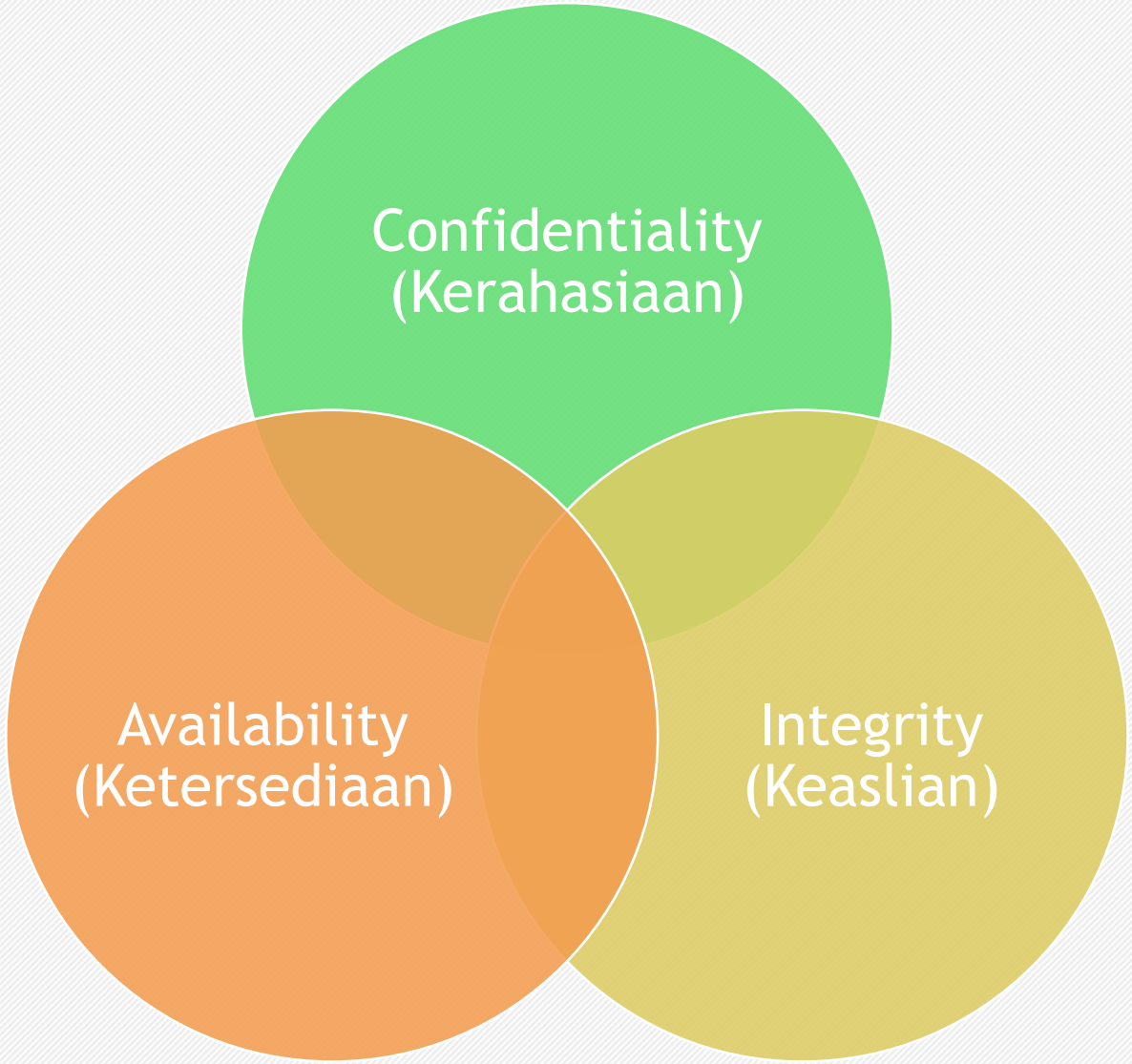
Cyber Attack akan terus berevolusi seiring evolusi dari perkembangan teknologi itu sendiri

Sejarah dan Perkembangan Keamanan Komputer



- Evolusi Serangan dan Kejahatan Siber berbanding lurus dengan nilai kerugian yang dialami
- Uang adalah salah satu motivasi terbesar dalam cyber crime

The Triad: CIA

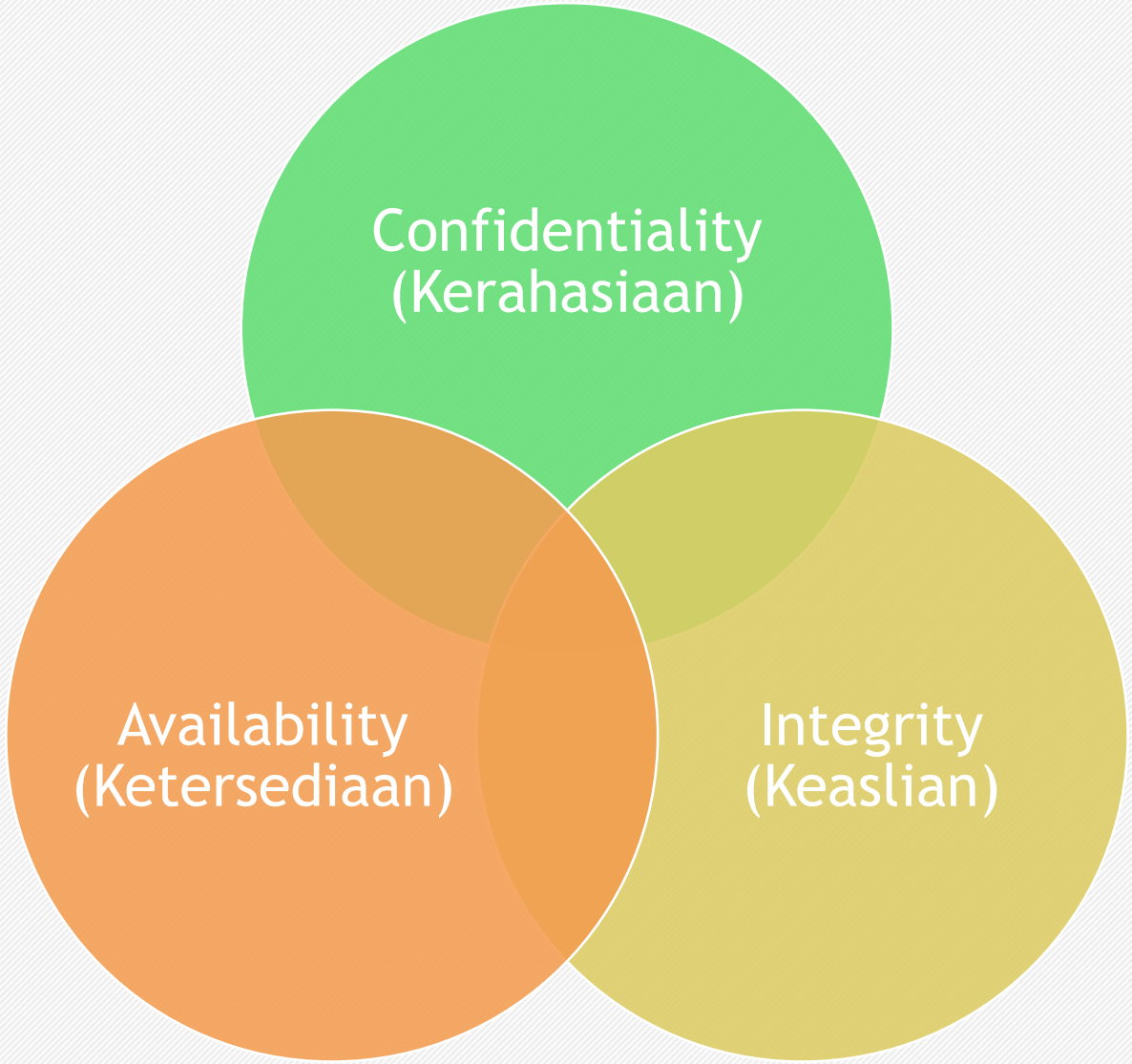


CIA adalah Tiga konsep utama dalam Keamanan Informasi

CIA terdiri dari Confidentiality (Kerahasiaan), Integrity (Keaslian), dan Availability (Ketersediaan

Pemodelan ini sangat membantu dalam memahami konsep dari Keamanan Informasi

The Triad: CIA



Confidentiality (Kerahasiaan) adalah prinsip dalam menjaga suatu data agar tidak bisa dibaca/dilihat oleh orang yang tidak seharusnya

Integrity (Keaslian) adalah kemampuan untuk mencegah suatu data agar tidak diubah oleh orang yang tidak bertanggungjawab

Availability (Ketersediaan) adalah kemampuan untuk mengakses data Ketika diperlukan

The Triad: CIA - Contoh Kasus

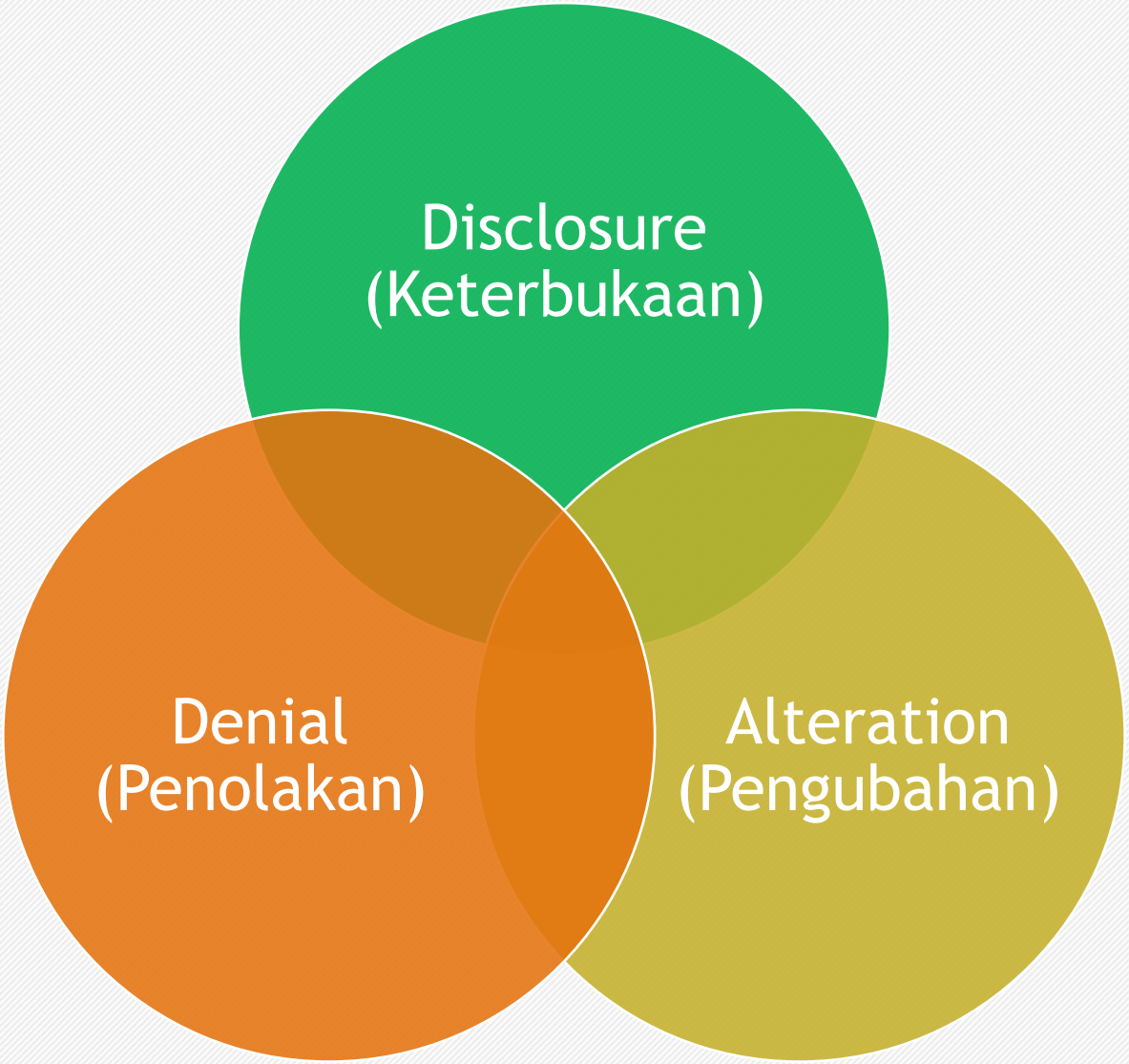
Salah satu contoh Keamanan Informasi yang paling mudah dan dimiliki semua orang adalah Rekening Bank. Mari lihat bagaimana penerapan konsep CIA dalam menjaga keamanan Rekening Bank

Confidentiality (Kerahasiaan), Rekening Bank harus terjaga kerahasiaannya. Hanya pemilik rekening yang boleh mengakses, melihat, dan melakukan transaksi atas rekening tersebut

Integrity (Keaslian) Nilai dari rekening bank harus sesuai dan tidak boleh berubah kecuali ada transaksi valid yang terjadi. Perubahan 1 digit saja akan berdampak serius

Availability (Ketersediaan) Rekening bank harus bisa diakses oleh pemilik rekening kapanpun pemilik menginginkannya

The Reverse Triad: DAD



Lawan dari CIA adalah DAD yaitu Disclosure (Keterbukaan), Alteration (Pengubahan), dan Denial (Penolakan)

Jika ketiga factor ini terjadi dalam sebuah upaya keamanan informasi, bisa dipastikan kualitas keamanannya rendah

Pengendalian Keamanan Komputer

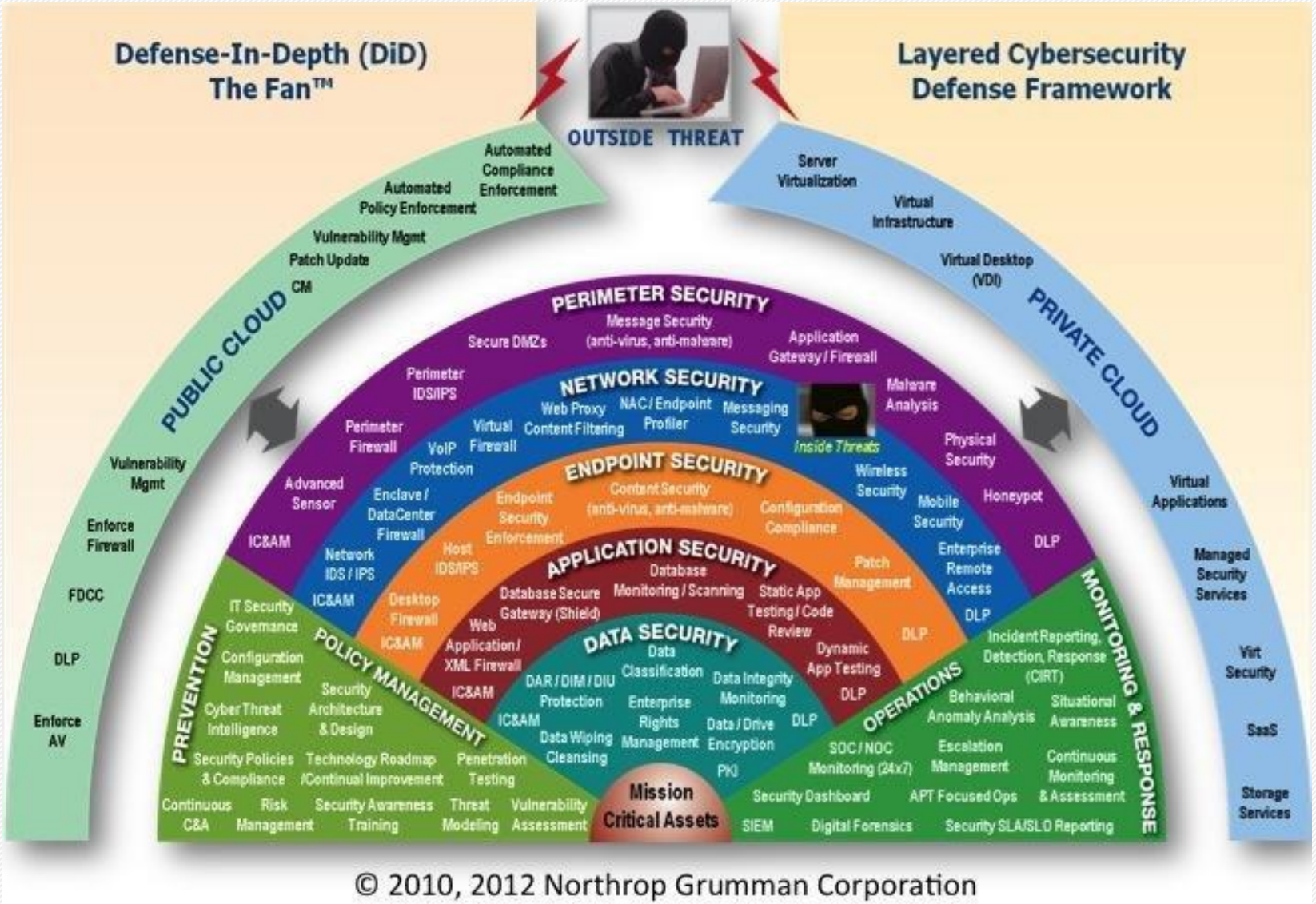
NO SYSTEM IS SAFE !

Tidak ada sistem yang benar-benar aman

Karenanya perlu mengimplementasikan berbagai macam tipe kendali keamanan (access control) untuk membuat suatu sistem aman. Pendekatan ini disebut dengan Defense-in-Depth

Defense in Depth adalah pendekatan untuk melindungi suatu asset di setiap layer security yang ada

Pengendalian Keamanan Komputer



Standar Keamanan Komputer

Standar Keamanan Komputer adalah Kumpulan parameter yang harus dipenuhi untuk mencapai suatu tingkat keamanan tertentu.

Berikut contoh Standar Keamanan yang popular digunakan dalam berbagai sector:

- ISO 27001:2013 → standar paling umun yang digunakan pada sebuah Sistem Manajemen Keamanan Informasi (ISMS)
- PCI DSS (Payment Card Industry Data Security Standard) → standar keamanan yang digunakan bagi para pihak yang ingin menggunakan teknologi kartu elektronik pada organisasinya
- HIPAA (Health Insurance Portability and Accountability Act) → standar keamanan yang menuntut rumah sakit untuk menjaga data pasiennya aman dan tidak bocor
- FINRA (Financial Industry Regulatory Authority) → standar keamanan yang mengatur organisasi keuangan untuk mengatur dana dan transaksi keuangannya terkait keamanan data dan perlindungan data pengguna
- GDPR (General Data Protection Regulation) → dibuat oleh pemerintah negara-negara eropa untuk menjamin perlindungan data pengguna agar aman dan tidak bisa diakses kecuali oleh tanpa otorisasi yang valid

ISO/IEC 27001:2013

ISO 27001 adalah standar keamanan yang telah digunakan secara internasional dan merupakan *best practice* untuk Sistem Manajemen Keamanan Informasi (ISMS)

Terdapat total 114 Kontrol Annex A yang dibagi menjadi 14 Kategori

- A.5 – Information Security Policies (2 Control)
- A.6 – Organisation of Information Security (7 Controls)
- A.7 - Human resource security (6 controls)
- A.8 - Asset management (10 controls)
- A.9 – Access control (14 controls)
- A.10 – Cryptography (2 controls)
- A.11 – Physical and environmental security (15 controls)

ISO/IEC 27001:2013

Terdapat total 114 Kontrol Annex A yang dibagi menjadi 14 Kategori (lanjutan)

- A.12 - Operations security (14 controls)
- A.13 – Communications security (7 controls)
- A.14 – System acquisition, development and maintenance (13 controls)
- A.15 – Supplier relationships (5 controls)
- A.16 - Information security incident management (7 controls)
- A.17 – Information security aspects of business continuity management (4 controls)
- A.18 - Compliance (8 controls)