UNIVERSITAS
GADJAH MADA

Cybersecurity Literacy

Jazi Eko Istiyanto

disampaikan pada “NgabuburIT”

Lab Sistem Komputer dan Jaringan

Departemen Ilmu Komputer dan Elektronika

FMIPA UGM

13-04-2022

UNIVERSITAS
GADJAH MADA

Cybersecurity : IT vs OT

IT/IS : data protection; modif kasi data medik bisa berakibat pasien cacat/meninggal. CIA (*Conf ɨdentiality Integrity Authenticity*). Ransomare menghentikan kegiatan RS, Toyota(?), Colonial Pipeline, dsb

OT(industrial systems) : physical protection. Safety/Security. AIC (*Authenticity Integrity Conf ɨdentiality*) Stuxnet merusak sentrifugal pengayaan uranium Iran, menunda/ menghambat program nuklir Iran. Stuxnet = Weaponised Malware = Cyberweapon.

UNIVERSITAS
GADJAH MADA

Data is the new Oil
Data is the new Uranium

Oil memberikan kesejahteraan, setelah melalui proses seperti Ref nery dsb. Oil harus dijaga agar tidak bocor (oil leak).

Uranium memberikan kesejahteran(eg energy) setelah melalui proses enrichment, dsb. Uranium hrs dijaga agar tidak “bocor” ke luar.

Data hrs dijaga privacy. Tidak boleh ke luar (eg Equifax breach, vulnerability ad di Struts). Data cleansing utk menjaga agar decision benar.

“**Data is the new asbestos...it is a risk, potentially toxic, to the company**”(Christopher Graham, 2016).

Data bisa menjadi Asset, tetapi juga bisa menjadi Liabilitas

UNIVERSITAS
GADJAH MADA

Global Theats

Perusahaan pengangkut container, Maersk, terkena **Notpetya**. Padahal Notpetya adalah “serangan” ke Ukraina sbg negara. Malangnya, Maersk punya kantor di Kiev. Collateral damages!

Stuxnet ternyata tidak hanya mengenai Iran, tetapi seluruh dunia. Semua yg mengoperasikan PLC S7 buatan Siemens.

Solarwinds mengenai banyak institusi pemerintah, bisnis, dan industri USA. *“Poisoning the well”*. Web tempat update/upgrade software yg diinfeksi shg semua updaters/upgraders kena.

UNIVERSITAS
GADJAH MADA

Biaya Security?
Asuransi Security?

"**Rarely is anyone thanked for stopping a disaster that did not happen**"(Mikko Hypponen, F-Secure). **Silent Evidence!**

Security engineers)* hrs menemukan semua lobang dan menutupnya. *Black hat hackers* hanya perlu satu lobang dan mengeksploitasinya.

"**Most software failures and data breaches aren't inevitable. They are the result of neglect and underinvestment in product reliability and security"**(Zeynep Tufecki, U of North Carolina)

Ransomware, Wannacry, mengenai banyak komputer yg sistem operasinya tdk lagi di"support" oleh produsen. *Neglect? Inderinvestment?*

Institusi membayar "premi" ke perusahaan cybersecurity utk jaminan security (security as a "cloud")?

***) Engineers itu profesi. Lulusan FMIPA yg bekerja di industri disebut engineers.**

UNIVERSITAS
GADJAH MADA

Policy Enforcement (Schneier, 2018*)

Best Practices : Tidak perlu mengalami sendiri, belaar dari pengalaman orang lain

Self-Enforcement : krn itu Awareness penting

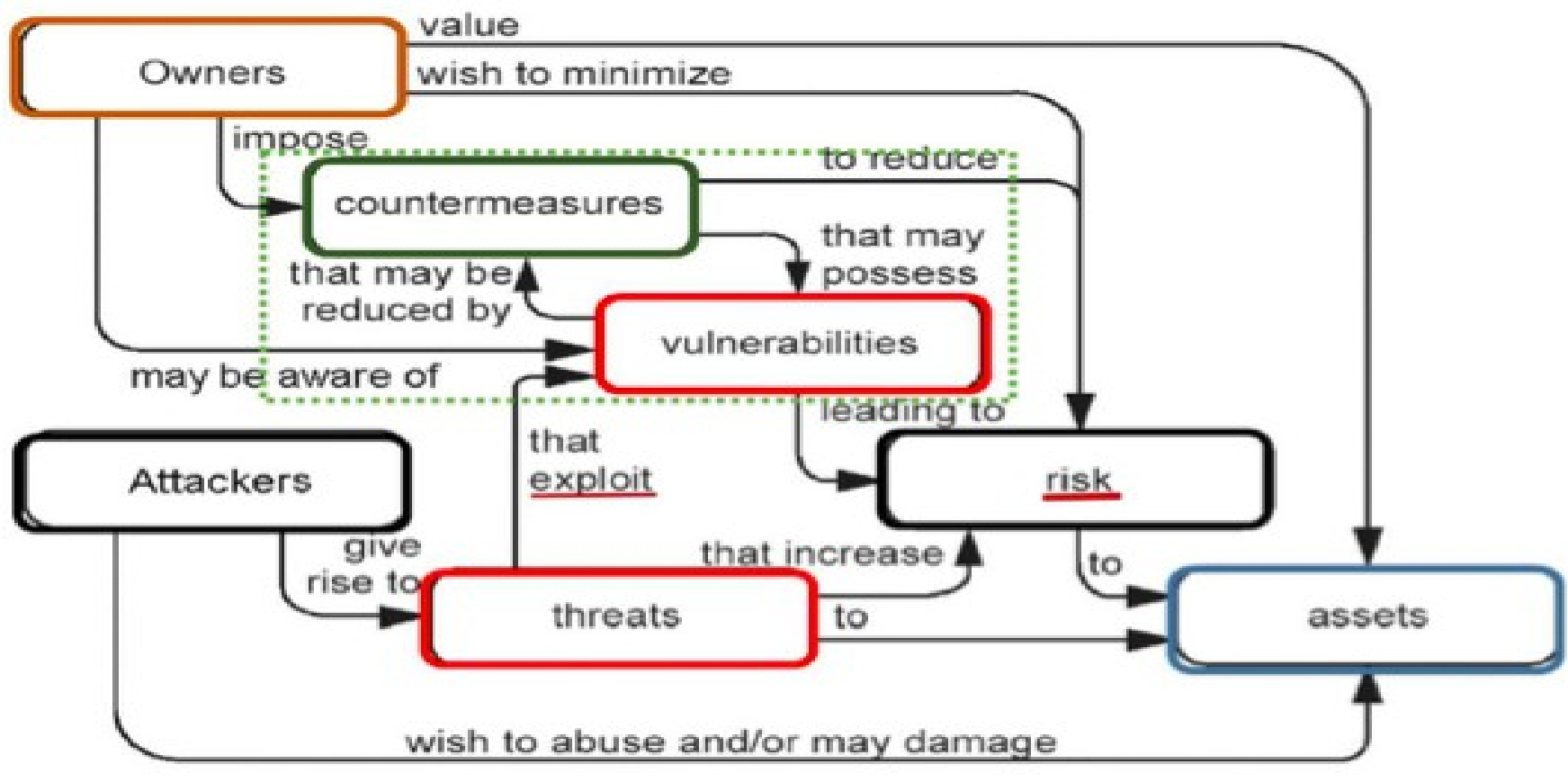
Litigation : Undang-undang ITE, European GDPR (General Data Protection Regulation)?

Regulation Bodies (eg BAPETEN utk nuklir, BPOM utk obat dan makanan) melalui perizinan dan inspeksi, misalnya

***) Schneier, B, 2018 : "Click Here to Kill Everybody : Security and Survival in a Hyper-Connected World", Norton**

UNIVERSITAS
GADJAH MADA

Terima Kasih



Pavol Zavarky,Computer Security at Nuclear Facilities,
Dept. Nuclear Safety Security Engineering,
Nagaoka University of Techology, Japan, 2017