# Cyber security

## consideration for advanced technology based support systems

**OECD-HRP/NKS decommissioning workshop – 6-7 December 2018, Lillehammer**

André Alexandersen Hauge
on behalf of Bjørn Axel Gran, Vikash Katta
Department of Risk, Safety & Security, IFE, Halden
andre.hauge@ife.no
(47) 99 61 66 90

Digital Systems

*Research for a better future*

# Why consider risk, safety and security?

- Lack of well defined and tested requirements for the support system
  can lead to unforeseen downtime and inefficient services.
- Lack of safety and risk assessment
  can lead to hazardous incidents working with high energy sources.
- Leak of sensitive data
  will potentially be breach of laws and regulations, and
  will undermine the trust in the services.
- Manipulation of data or denial of service attacks
  will besides having costs, also undermine the trust in the services.

# IEC 61508 about cybersecurity

IEC 61508-1

INTERNATIONAL STANDARD

NORME INTERNATIONALE

**Functional safety of electrical/electronic/ programmable electronic safety-related systems –**

**Reference to**:

- IEC 62443 series
- ISO/IEC/TR 19791

- requirement 7.4.2.3:
  - “If the hazard analysis identifies that malevolent or unauthorised action, constituting a security threat, as being reasonably foreseeable, then a security threats analysis should be carried out”
- requirement 7.5.2.2
  - “if security threats have been identified, then a vulnerability analysis should be undertaken in order to specify security requirements”
- the safety manual
  - “details of any security measures that may have been implemented against listed threats and vulnerabilities.”

# Security assessment

Step1: **Value**

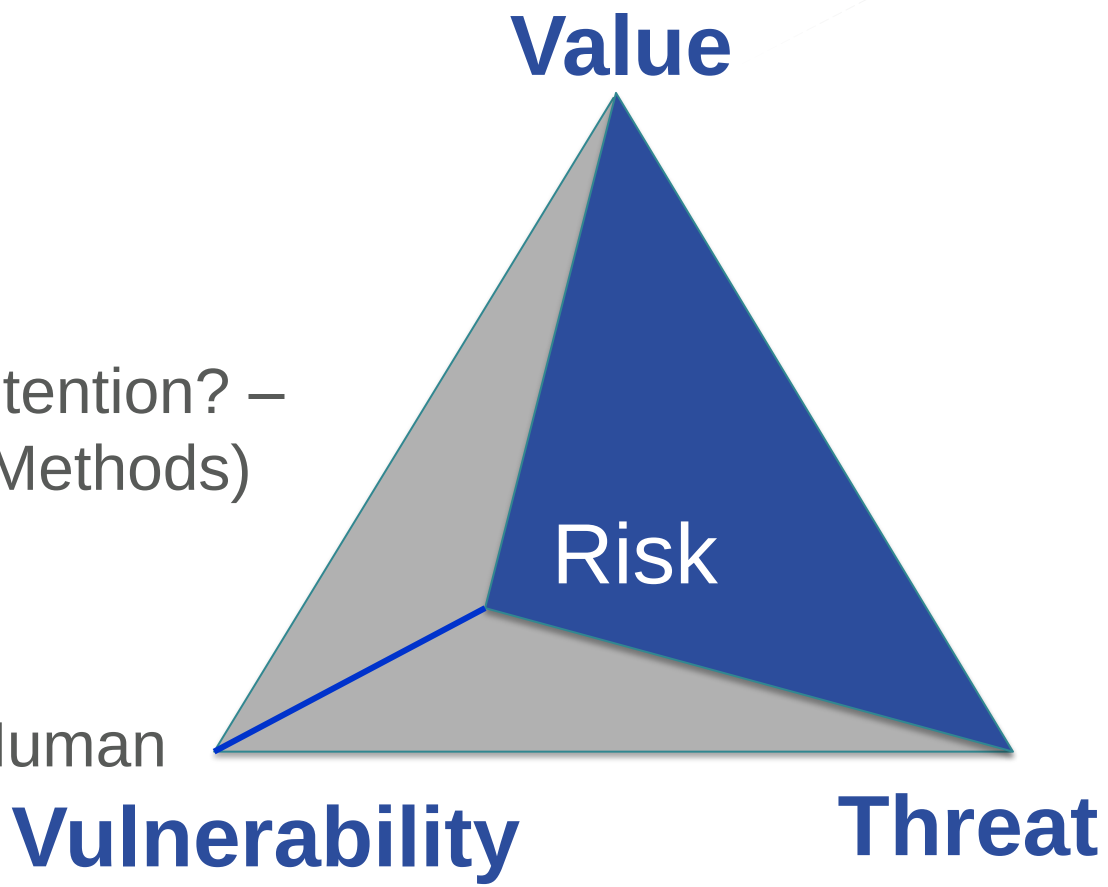
Which values/assets do you have?

Step 2: **Threats**

What are the actors capacity and intention? – (4M: Motivation, Mission, Mindset, Methods)

Step 3: **Vulnerability**

Physical, Logical, Organizational, Human



# «See it coming: The Four M's of Digital Espionage»

Ref:

**Frode Hommedal**

On LinkedIn 21. sep 2014

Former: Senior Advisor Difi

Now: Cyber security specialist, Telenor

- Motivation

  *«These «viruses» are security incidents, and the results of deliberate actions from hostile entities»*

  *«Spying on you gives the threat actor – your adversary – some kind of advantage over you, or someone else through you»*

- Mission

  *«They are highly trained professionals – cyber special forces so to speak – who have been purposely deployed within the perimeters of your network»*

- Mindset

  *«How can we subvert this» and «what can we make this do», «how can we break into it» and «how can we hide within it».*

- Methods

  «The list of methods employed by the wide range of possible cyber adversaries is way too long for me to even contemplate compiling»

# Didn’t see this coming: Short on the Maersk story

full text at wired.com «THE UNTOLD STORY OF NOTPETYA, THE MOST DEVASTATING CYBERATTACK IN HISTORY»

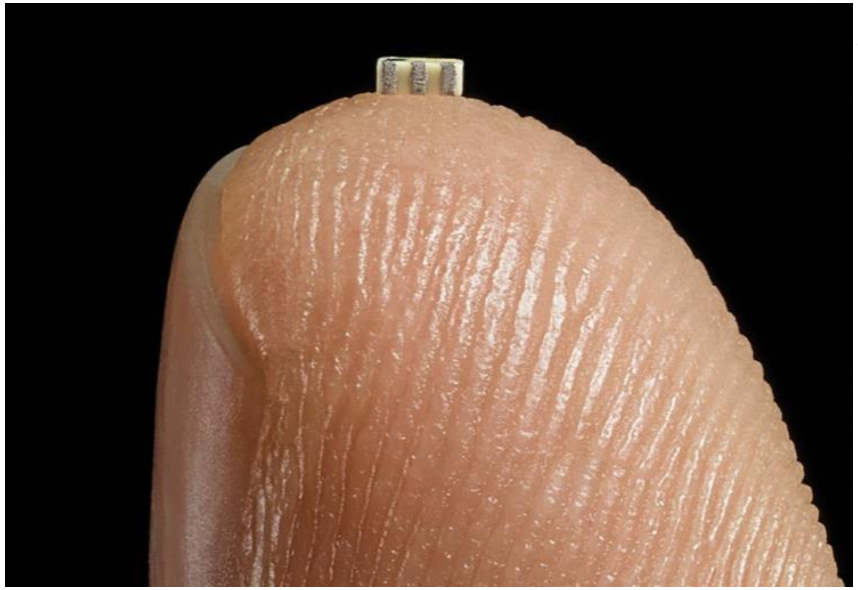
- 27 june 2017, the **NotPetya** virus run through Maersk systems in Copenhangen
- Started with **”repairing file system on C:”** on office machines with a stark warning not to turn off the computer and also **“oops, your important files are encrypted”** and a demand of $300 worth of bitcoin to decrypt them. Then, a wave of screens started turning black at the Maersk headquarters
- **Ground zero was actually Kiev** office in Unkrain, an attack that began, at least, as an assault on one nation by another. Russian cyber agents known as Sandworm used a Windows back door to release a piece of malware called NotPetya to different targets.
- It **irreversibly encrypted computers’ master boot records**, the deep-seated part of a machine that tells it where to find its own operating system
- It **crippled multinational companies** including Maersk, pharmaceutical giant Merck, FedEx’s European subsidiary TNT Express, French construction company Saint-Gobain, food producer Mondelēz, and manufacturer Reckitt Benckiser. In each case, it inflicted nine-figure costs. It even spread back to Russia, striking the state oil company Rosneft.
- The result was more than **$10 billion in total damages**

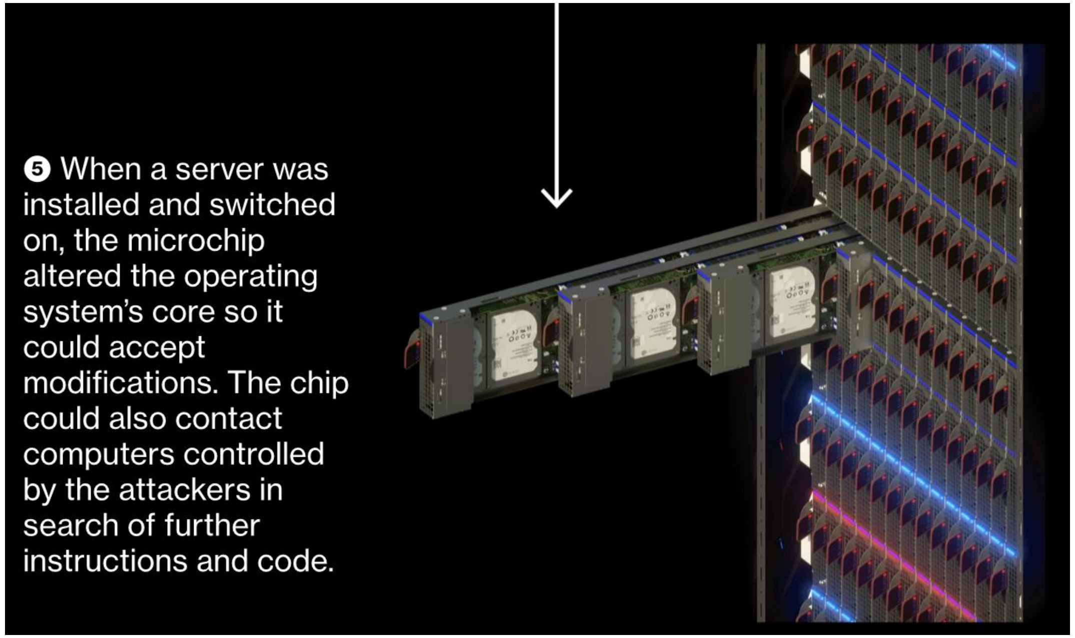
# Any assets in decommissioning?

- Examples:
  - Man down – there is a need to not share position & video to outsiders
  - Radioactive materials - there is a need to not share data to outsiders
  - Sensitive data – should not be shared with outsiders
  - Critical data/procedures – signals sent from app. A to app. B shall not be corrupted
  - Critical data/procedures – signals sent from app. A to app. B shall not be delayed
  - ..
  - AND: your advanced technology based support systems

# The Big Hack (full text at bloomberg.com)

- Amazon started investigating Elemental in 2015
- Elemental's staff boxed up several servers and sent them to Ontario, Canada, for the third-party security company to test. Servers were assembled for Elemental by Super Micro Computer
- The testers found a tiny microchip
- Elemental's servers could be found in Department of Defense data centers, the CIA's drone operations, and the onboard networks of Navy warships. And Elemental was just one of hundreds of Supermicro customers.
- Investigators found: The chips had been inserted during the manufacturing process (Made in China)





❺ When a server was installed and switched on, the microchip altered the operating system's core so it could accept modifications. The chip could also contact computers controlled by the attackers in search of further instructions and code.

# Is cyber a problem?

- The process is not connected.
- And if it is, they can not stop it.
- .. and other system protect the people from harm.

SYSTEM FAILURE

# It is a problem!

- *My process is not connected.*
- *And if, they can not stop it.*
- *.. and other system protect the people from harm.*

- They studied the design
- … studied the vulnerabilities
- … used it for a DoS
- … and gained 1M$ on their stocks