

Cyber security

consideration for advanced technology based support systems

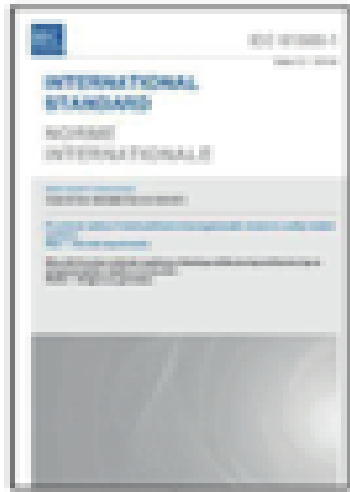
OECD-HRP/NKS decommissioning workshop – 6-7 December 2018, Lillehammer

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

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



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

Step 1: Value

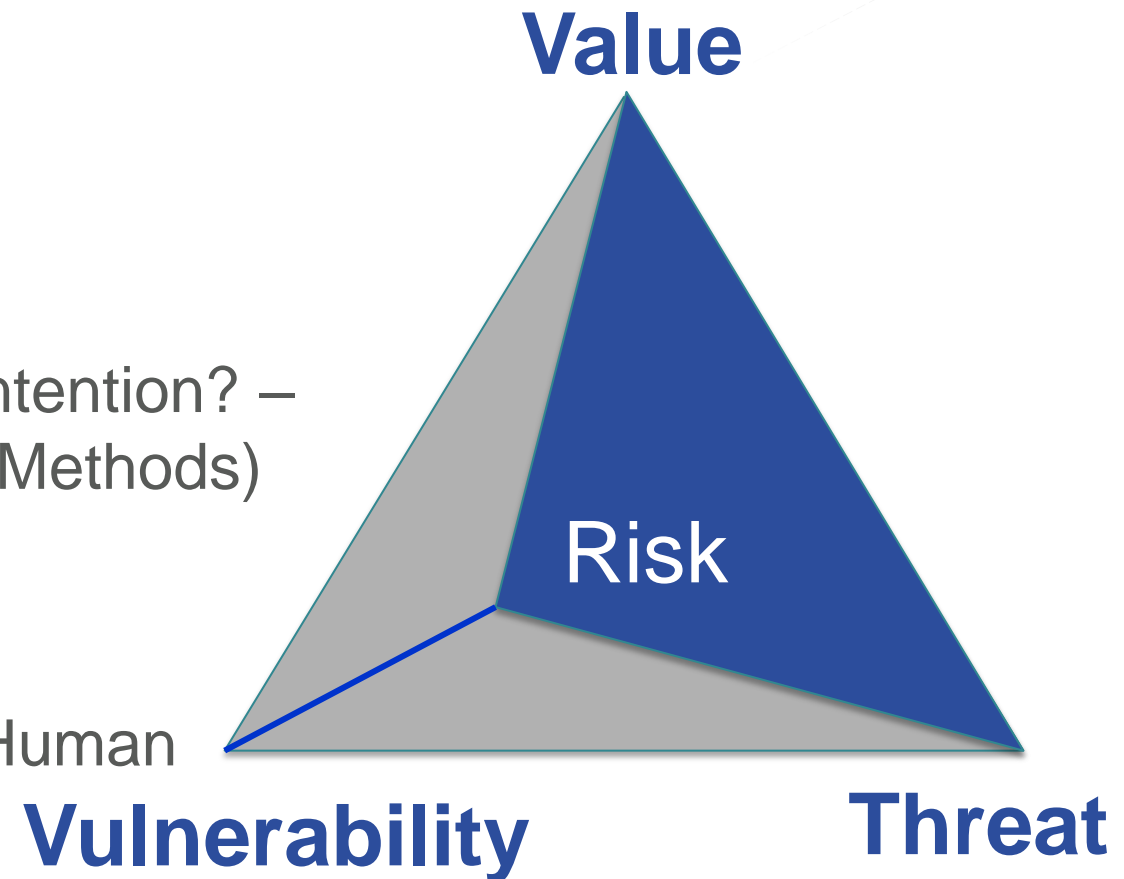
Which values/assets do you have?

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»

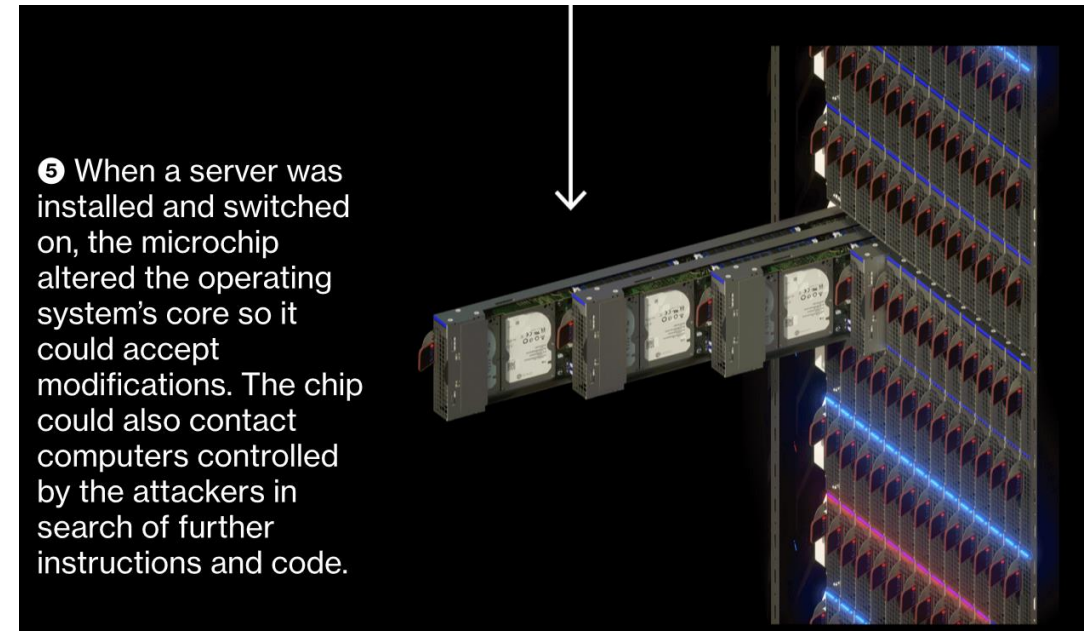
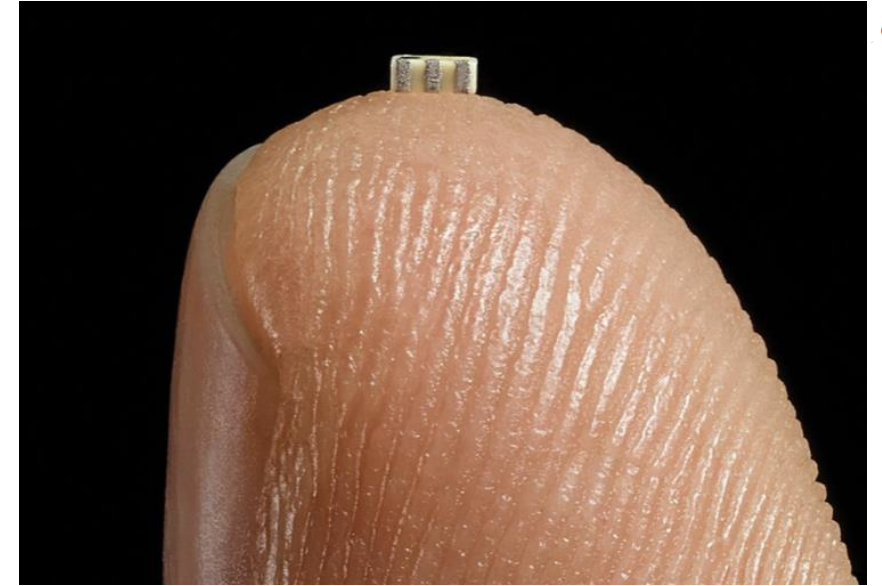
- 27 June 2017, the **NotPetya** virus ran through Maersk systems in Copenhagen
- Started with **"repairing file system on C:"** on office machines with a stark warning not to turn off the computer and also **"oops, your important files are encrypted"** and a demand of \$300 worth of bitcoin to decrypt them. Then, a wave of screens started turning black at the Maersk headquarters
- **Ground zero was actually Kiev** office in Ukraine, 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 Mondelez, 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)



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.

85675867	0023555460	125675867	24685675867	0023555460	12545022321	24685675867	0023555460	12545022
52768597	02605554864	22301123254	56452768597	02605554864	22301123254	56452768597	02605554864	22301123
97546567	52107905648	89780158595	45197546567	52107905648	89780158595	45197546567	52107905648	89780158
66666666	9201.265340	46243801255	67666666666	9201.265340	46243801255	67666666666	9201.265340	46243801
65468597	5326498235.	56897845022	66665468597	5326498235.	56897845022	66665468597	5326498235.	56897845
21342430	03125643754	24584686530	52421342430	03125643754	24584686530	52421342430	03125643754	24584686
29752834	34201326497	44565752389	43529752834	34201326497	44565752389	43529752834	34201326497	44565752
56749758	88260214687	70122648654	01356749758	88260214687	70122648654	01356749758	88260214687	70122648
01326798	95462032156	89901245984	53701326798	95462032156	89901245984	53701326798	95462032156	89901245
60546412	87546200012	56578021657	78760546412	87546200012	56578021657	78760546412	87546200012	56578021
01352679	56489854222	89535670000	56701352679	56489854222	89535670000	56701352679	56489854222	89535670
524.2134	30215021569	01444587901	886524.2134	30215021569	01444587901	886524.2134	30215021569	01444587
54240404	87459823654	89564875564	54654240404	87459823654	89564875564	54654240404	87459823654	89564875
21404359	85123030213	02654895465	23421404359	85123030213	02654895465	23421404359	85123030213	02654895
53402213	13311123150	13025165465	78553402213	133111000011	13025165465	78553402213	13311125644	13025165
58672464	25468952654	76540215497	49758672464	25468952654	76540215497	49758672464	25468952654	76540215
68652031	78021328503	87654860216	97968652031	78021328503	87654860216	97968652031	78021328503	87654860
79561203	57920045685	54897564202	25679561203	57920045685	54897564202	25679561203	57920045685	54897564
56530979	48314904153	15465465460	26456530979	48314904153	15465465460	26456530979	48314904153	15465465

SYSTEM FAILURE

32031246	18946516746	21654621	1246	18946516746	21654621	1246	18946516746	21654621
56452123	51561687515	40216548	2123	51561687515	40216548	2123	51561687515	40216548
45754545	23162685421	56102165	4545	23162685421	56102165	4545	23162685421	56102165
91675425	62964975421	62165054	5425	62964975421	62165054	5425	62964975421	62165054
59782135	35656497652	13245450154	34659782135	35656497652	13245450154	34659782135	35656497652	13245450
23100002	31200124556	84987984301	64023100002	31200124556	84987984301	64023100002	31200124556	84987984
56462857	87976423120	24568765435	13656462857	87976423120	24568765435	13656462857	87976423120	24568765
45622256	31655976421	01235435435	55645622256	31655976421	01235435435	55645622256	31655976421	01235435
66566433	05234605242	43021648576	79866566433	05234605242	43021648576	79866566433	05234605242	43021648
23101346	59257561221	53441100000	59823101346	59257561221	53441100000	59823101346	59257561221	53441100
57242104	56024565237	00000001243	56457242104	56024565237	00000001243	56457242104	56024565237	00000001
68976543	85421245454	53727672034	23168976543	85421245454	53727672034	23168976543	85421245454	53727672
12124567	45456402124	25375763520	24212124567	45456402124	25375763520	24212124567	45456402124	25375763
12054976	24575454012	43597572672	54212054976	24575454012	43597572672	54212054976	24575454012	43597572
23051564	42245454440	40133727967	85323051564	42245454440	40133727967	85323051564	42245454440	40133727
46791630	55546520303	97801322479	65246791630	55546520303	97801322479	65246791630	55546520303	97801322
52675642	40555120245	69675014372	21352675642	40555120245	69675014372	21352675642	40555120245	69675014
21000231	21205512563	97846520434	13421000231	21205512563	97846520434	13421000231	21205512563	97846520
00000005	23564012452	52768975403	24000000005	23564012452	52768975403	24000000005	23564012452	52768975
24242412	54545450215	24214672732	42424242412	54545450215	24214672732	42424242412	54545450215	24214672
52424524	88879564501	03427679854	75452424524	88879564501	03427679854	75452424524	88879564501	03427679
01243424	55556523154	64031254596	97501243424	55556523154	64031254596	97501243424	55556523154	64031254

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