Cybersecurity challenges and risks of critical infrastructure

TATIANA GALIBUS, CYBERSECURITY AMBASSADOR

innovation
forward

Agenda

- Introduction to cybersecurity
- Most common risks in critical infrastructure
- Key takeaways

Have you heard of

LATEST ATTACKS

Picanol

ASCO

Antwerp

TVH

Defense ministry (Log4j, dec 2021)

Belgacom

Le soir

BPOST

Belgian new fruit Wharf (Sea Invest) feb 2022

City of Antwerp (dec 2022)

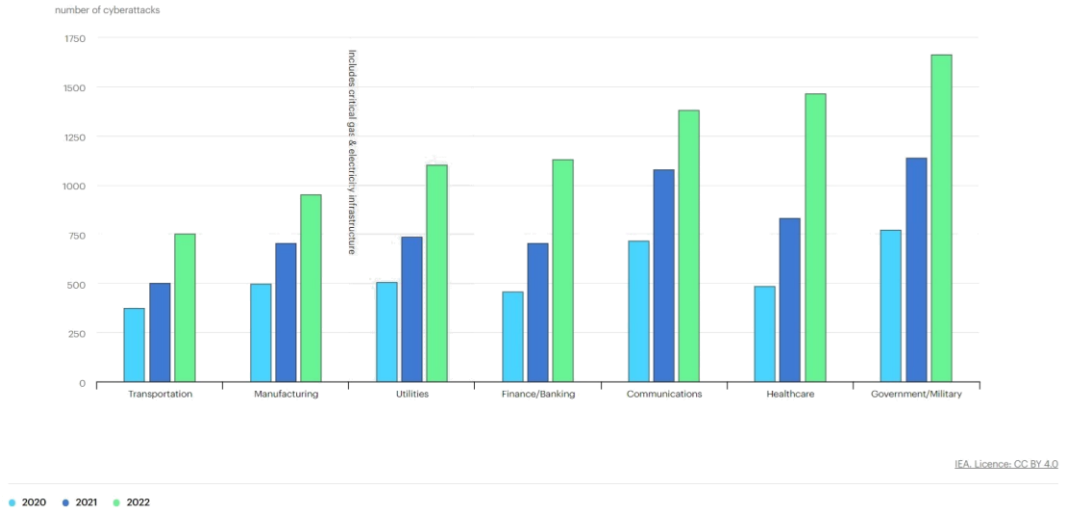
Belnet (May 2022)

Vivalia hospital (May 2022)

Hospital of Namur (June 2023)

Ministry of defense – huawei wifi routers (July 2022)

ChWapi hospital (Sept 2022)



Know who you're up to

DARK WEB

What is at stake?

ATTACKERS VS DEFENDERS

Attacker

- Needs **only one** hole to get in
- Needs to do a lot of research
- Needs to do a lot of steps
- Organized pros

Defender

- Difficult to defend **all** the assets
- Only need to **detect** one step
- Know your network/assets best
- **ICT, engineers, third party, operators**

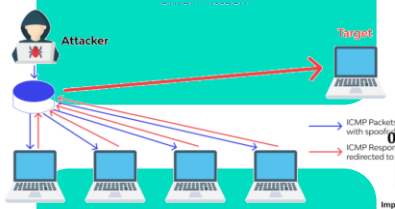
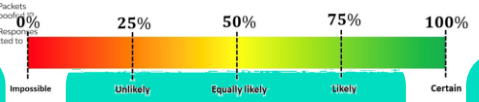
"It is not a question of IF but WHEN you're being hacked."

Per Christensen
Cyber Security Architect, Prevas
IEC ACSEC Member

innovation forward

Risks, threats, attacks, assets

DEFINITIONS

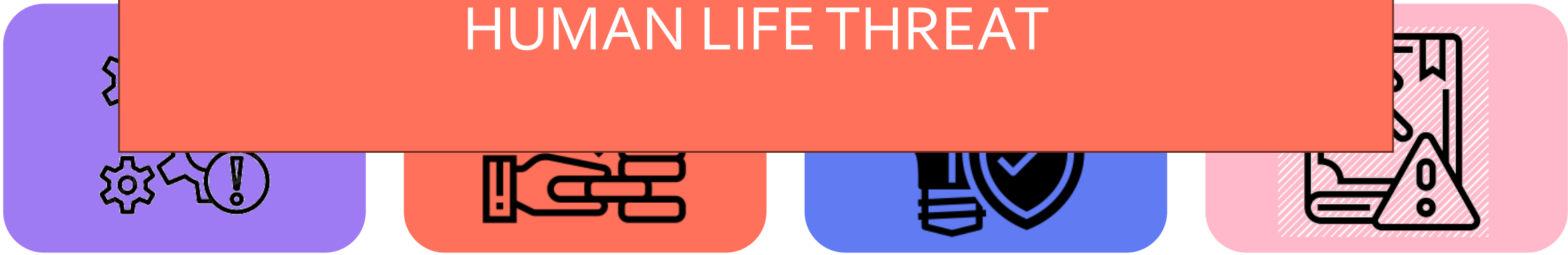
Threat	Vulnerability	Attack	Likelibility	Asset	Risk
			Certain, Likely, Unlikely, Impossible, Equally likely events 		
potential to harm	weakness that can be used to harm	threat realization scenario	chance for threat to happen	what can be damaged	how much you loose when this happens


VULNERABILITY
RISK
THREAT
ASSET

What are the risks – for critical infrastructure?

GIVE EXAMPLES

HUMAN LIFE THREAT



Operational risks

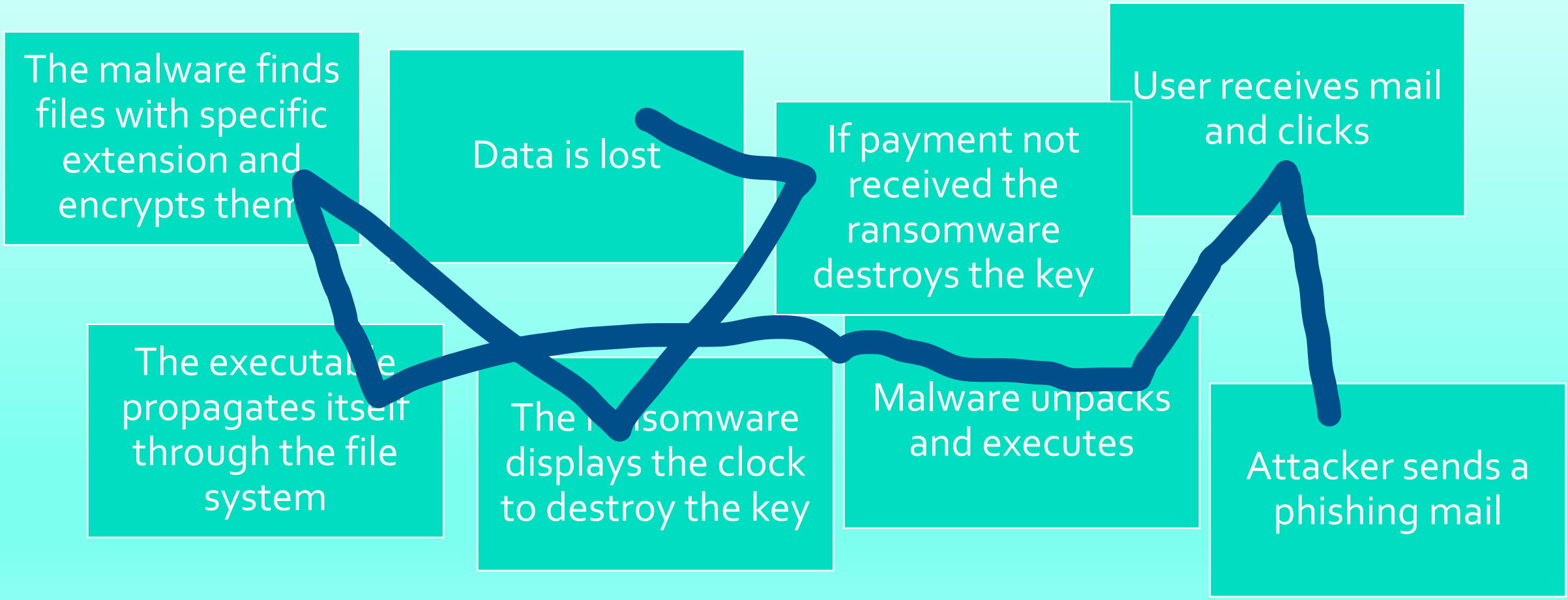
Financial risks for compromised personal data (PII)

Financial risks for compromised intellectual property

Regulatory issues

Example of a kill chain – order the steps

RANSOMWARE ATTACK



What is this slide about

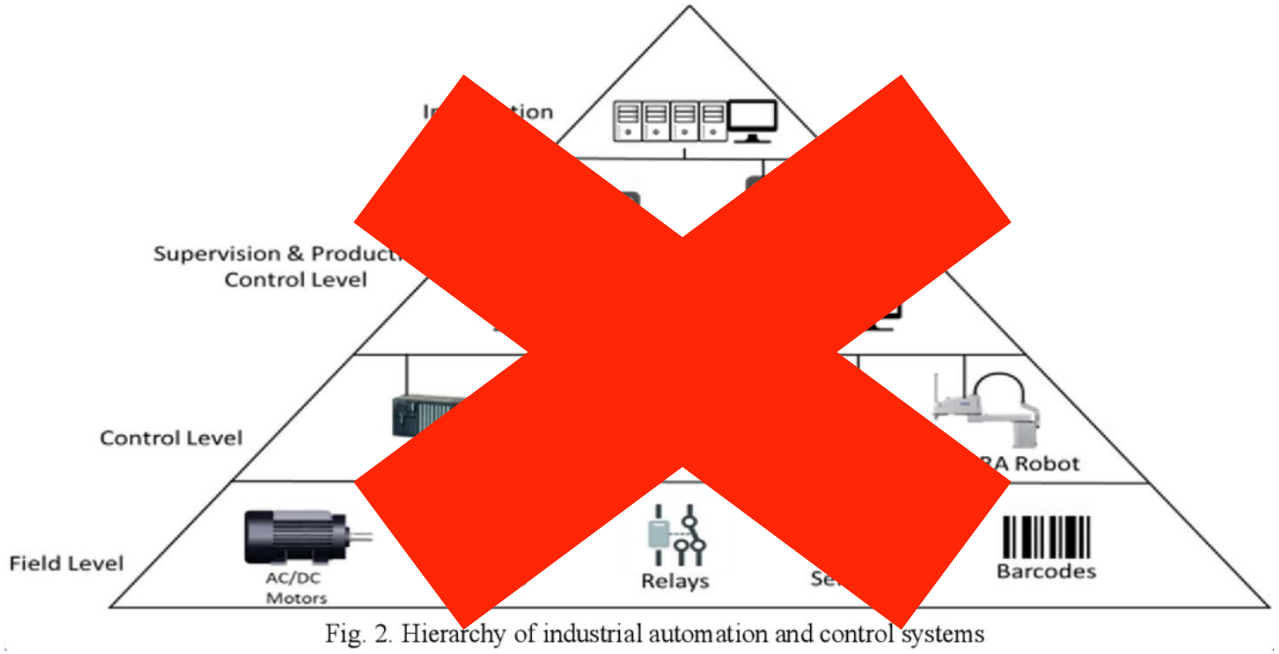
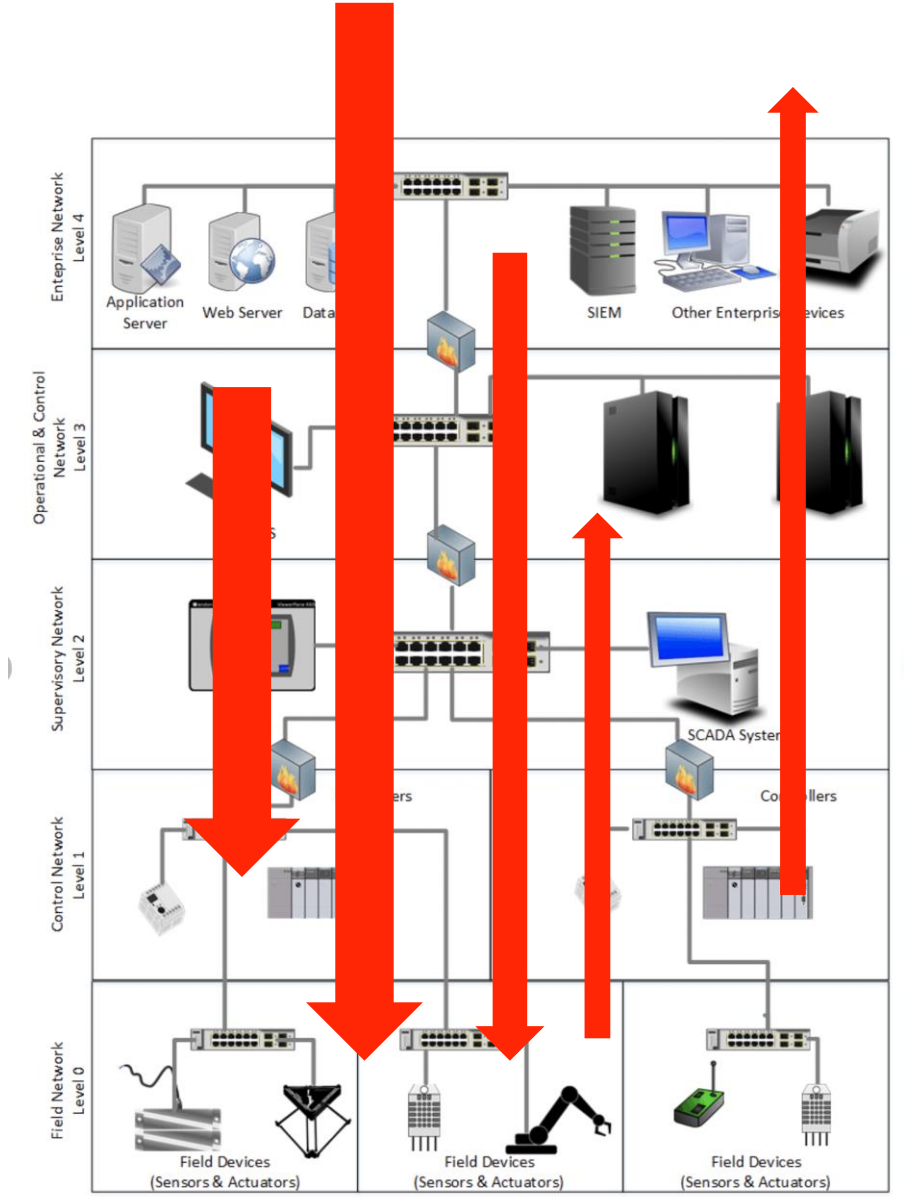


Fig. 2. Hierarchy of industrial automation and control systems



Risks related to connectivity

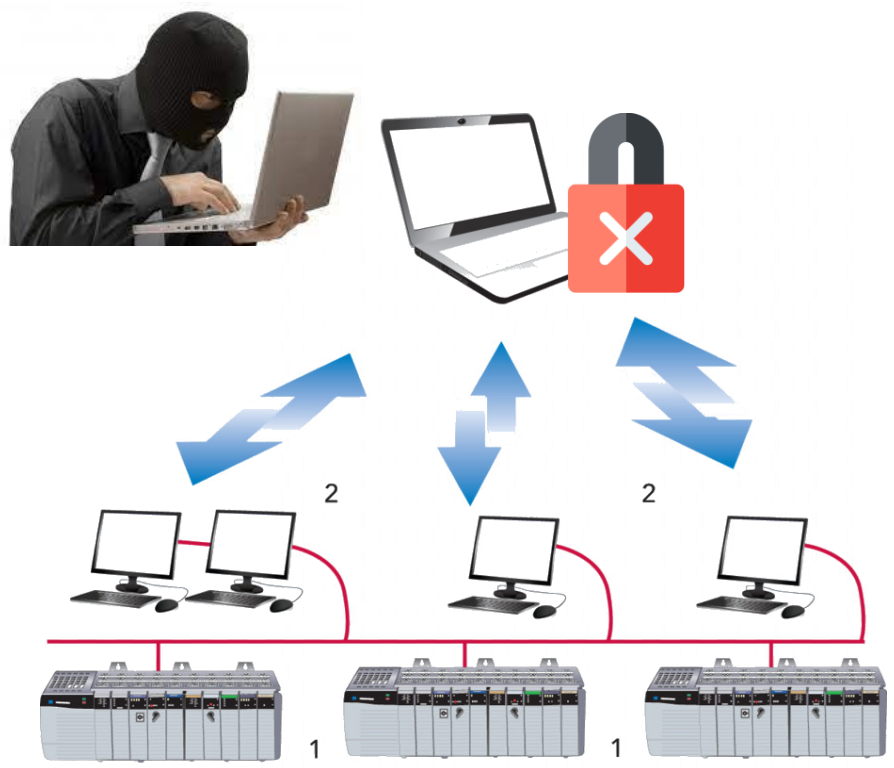
- REMOTE MAINTENANCE AND TRUSTED RELATIONSHIPS
- IT AND OT INTEGRATION
- NETWORK SECURITY GAPS, ABSENCE OF MONITORING
- ACCESS PRIVILEGE MISUSE

innovation forward

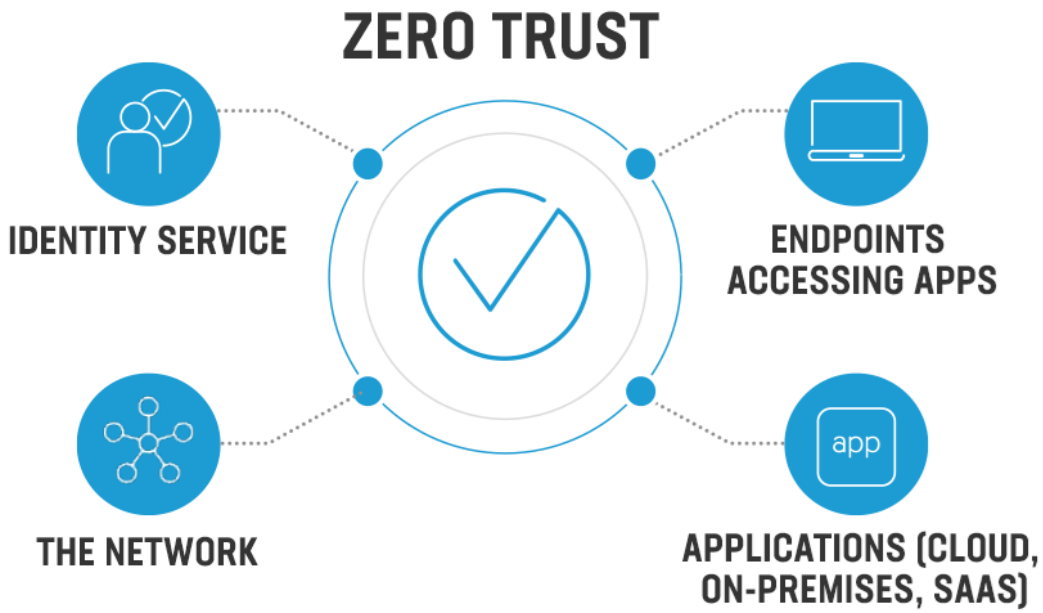
Why critical infrastructures need to look at network security

GROWING CONNECTIVITY

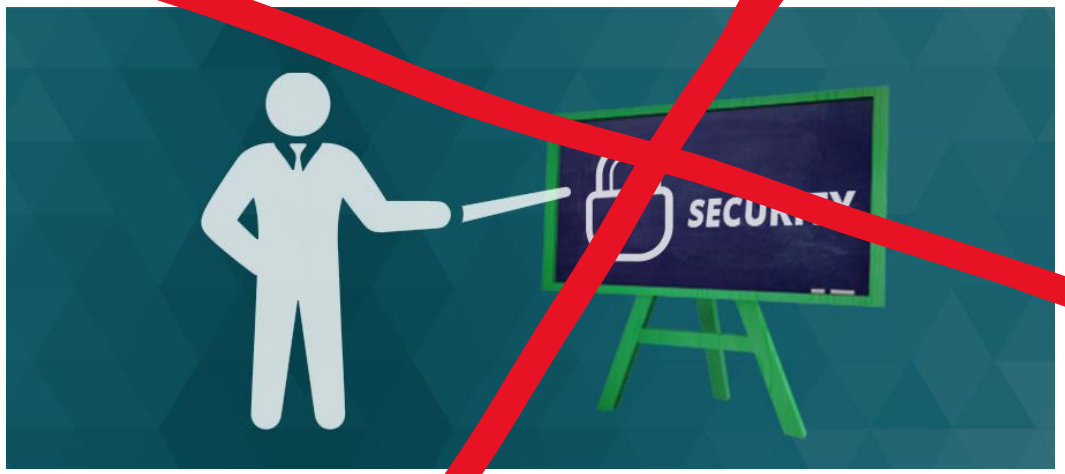
- Networks grow more complex
- Enterprises rely more on their networks and data to conduct business
- Difficult to manage
- Threat actors create new attack methods
- Security is everyone`s responsibility
- Every user is a potential vulnerability

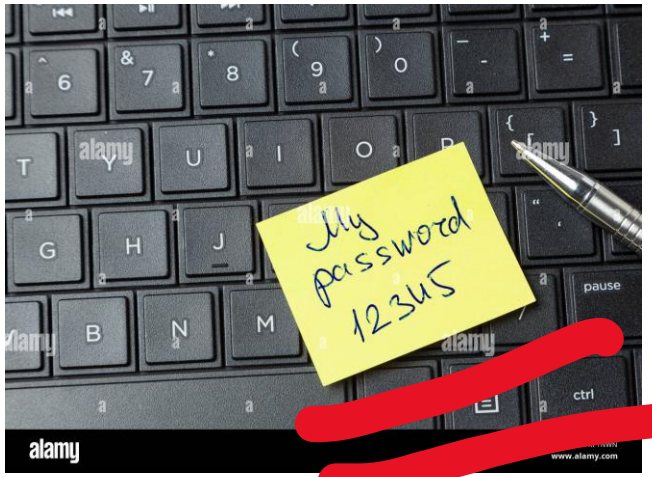


From Purdue -> to zero trust

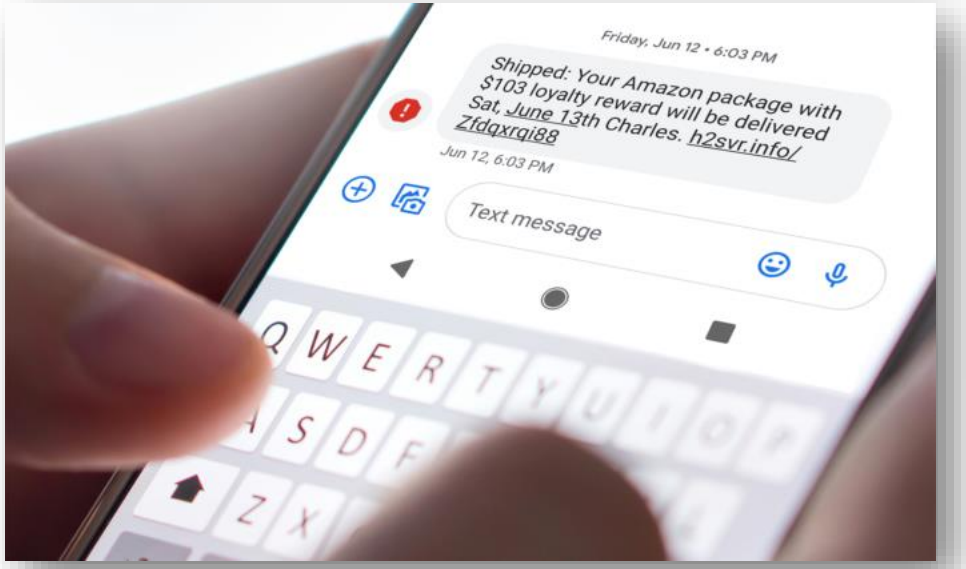


What is this slide about





And this



You missed a call | Transcription Available Play_Now ⏮ ▶ ⏭
03min25secs__3pmFriday-September-2023 11:29 AM

S

Sirris|PhoneSystem <stephan.witolla@jobticket.de>

Friday, 1 September 2023 at 2(

To: Tatiana Galibus

ATT00001.htm
2,3 KB

Download • Preview

This message is high priority.

The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful. This email has been scanned for viruses and malware, and may have been automatically archived by Mimecast Ltd, an innovator in Software as a Service (SaaS) for business. Providing a safer and more useful place for your human generated data. Specializing in; Security, archiving and compliance.

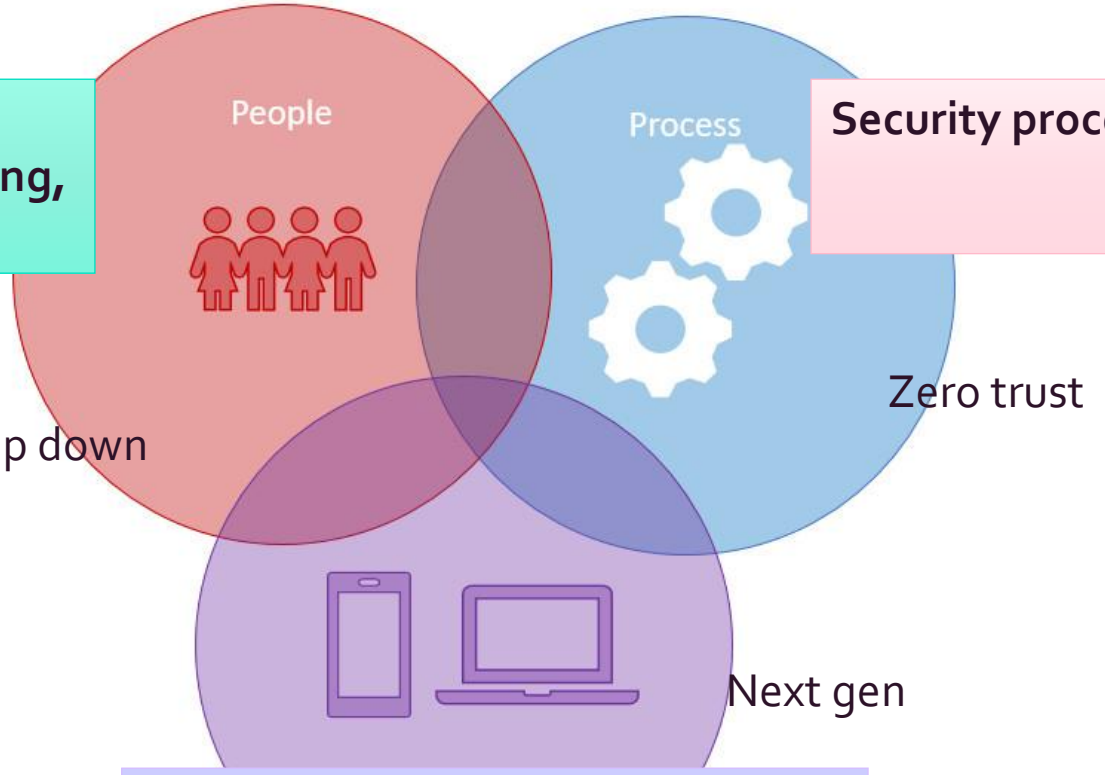
What if I am breached?

- CHECK THE INSURANCE AND VERIFY THE INCIDENT RESPONSE PLAN
- KNOW WHO DOES WHAT AND MAKE SURE OPERATORS KNOW
- CEOS – PERSONAL RESPONSIBILITY (NIS2)
- CHECK THE CONTRACT WITH IT PARTNER, VENDOR
- BASIC RULE – NOTICE ANY ANOMALY AND REPORT ON TIME

innovation forward

Cybersecurity culture to critical infrastructure

Positive cybersecurity culture, learning, dialogue



Security procedures/policies

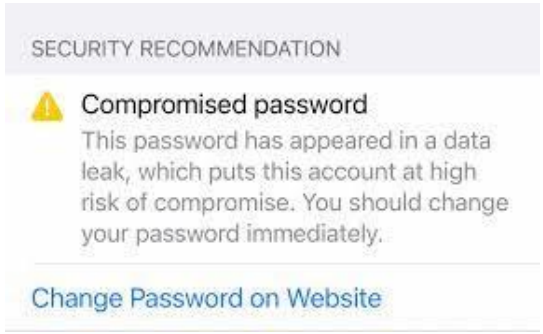
Technological frameworks/solutions

Risks related to cybersecurity culture and awareness

- ABSENCE OF CYBERSECURITY TRAINING
- NOT PREPARED TO INCIDENT RESPONSE AND RECOVERY
- SOCIAL ENGINEERING - PHISHING & SPEAR PHISHING
- CREDENTIAL STEALING/REUSING , PASSWORD SHARING

innovation forward

What is this about?



Risks related to data protection

- INSECURE DATA EXCHANGE AND STORAGE
- PRIVACY VIOLATION

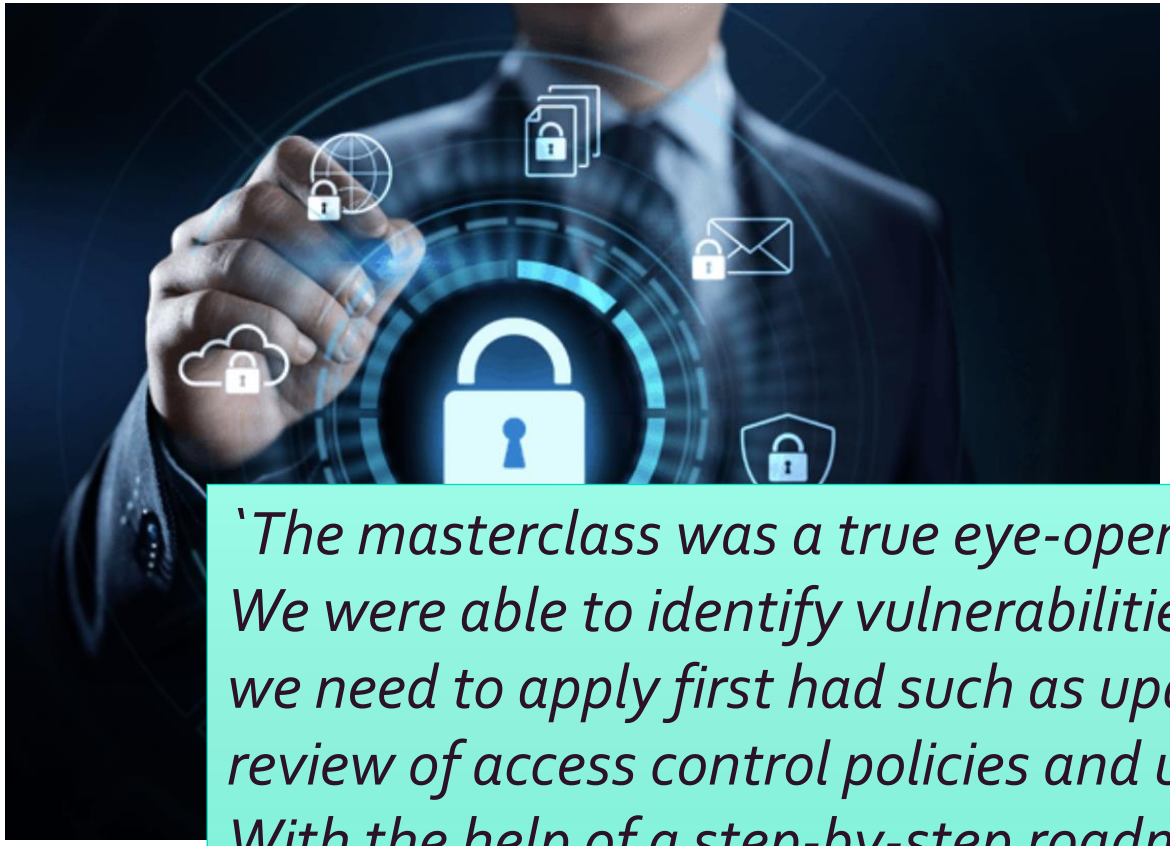
innovation forward

Main takeaways

- Major cybersecurity risks are related to connectivity, culture and data security.
- What are the challenges in your company ? -> answer our questionnaire
- How Sirris and Howest can help -> COOCK+ project
- Cybersecurity training for critical infrastructures (subsidized by VLAIO): January 2024.

innovation forward

Bootcamp Cybersecurity – Energy sector, harsh environments, and utilities



- in-depth 8-week learning journey for the critical infrastructures
- 7 masterclass modules + live Q&A, lessons learned, homework discussions, expert advice, and micro-coaching.
- most critical topics, which are usually not covered by the standard cybersecurity measures and require special attention due to rapid digitalization.

`The masterclass was a true eye-opener for us.
We were able to identify vulnerabilities in our network and the actions we need to apply first had such as updates, network segmentation, review of access control policies and user accounts.
With the help of a step-by-step roadmap we will be able make our cybersecurity posture more resilient.`

innovation forward

Your input

ANSWER 10 QUESTIONS TO KNOW YOUR NEEDS

Short link: https://su.vc/rnaxxkos

Tatiana Galibus

tatiana.galibus@sirris.be

+32 493 31 15 76

innovation
forward

sirris innovation forward

FACEBOOK.COM/SIRRIS.BE

@SIRRIS_BE

LINKEDIN.COM/COMPANY/SIRRIS