Live webinar

‘Hoe bescherm ik mijn fabriek tegen de top 3 Cyber threats?’

We starten om 09:30

29 oktober 2020 | Online kennisweek
INDUSTRIAL CYBER SECURITY

Spreker

Security en OT-expert

Mark Hellinghuizer

Yokogawa

CISSP®

GLOBAL INDUSTRIAL CYBER SECURITY PROFESSIONAL GICSP

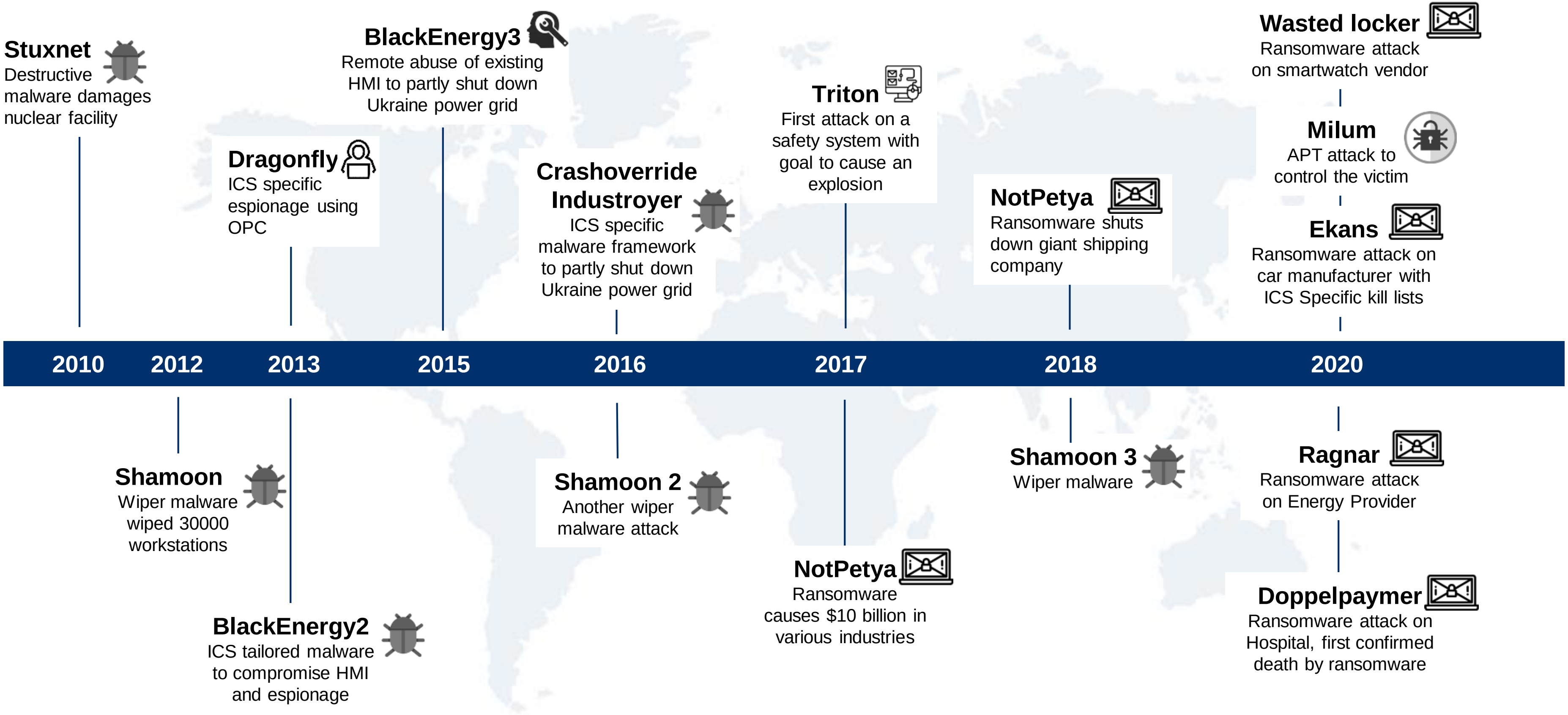
ISA/IEC 62443 CYBERSECURITY EXPERT ISA

C|EH™ Certified Ethical Hacker

Agenda

- History of security
- 3 Top Threats including protection
- Conclusion & 5 Key take aways

MAJOR HACKING ATTACK!



2010 2012 2013 2015 2016 2017 2018 2020

Stuxnet
Destructive malware damages nuclear facility

Shamoon
Wiper malware wiped 30000 workstations

Dragonfly
ICS specific espionage using OPC

BlackEnergy2
ICS tailored malware to compromise HMI and espionage

BlackEnergy3
Remote abuse of existing HMI to partly shut down Ukraine power grid

Crashoverride Industroyer
ICS specific malware framework to partly shut down Ukraine power grid

Shamoon 2
Another wiper malware attack

Triton
First attack on a safety system with goal to cause an explosion

NotPetya
Ransomware causes $10 billion in various industries

NotPetya
Ransomware shuts down giant shipping company

Shamoon 3
Wiper malware

Wasted locker
Ransomware attack on smartwatch vendor

Milum
APT attack to control the victim

Ekans
Ransomware attack on car manufacturer with ICS Specific kill lists

Ragnar
Ransomware attack on Energy Provider

Doppelpaymer
Ransomware attack on Hospital, first confirmed death by ransomware

TOP3 Cyber security threats

1

Untrained Employees

2

Ransom ware

3

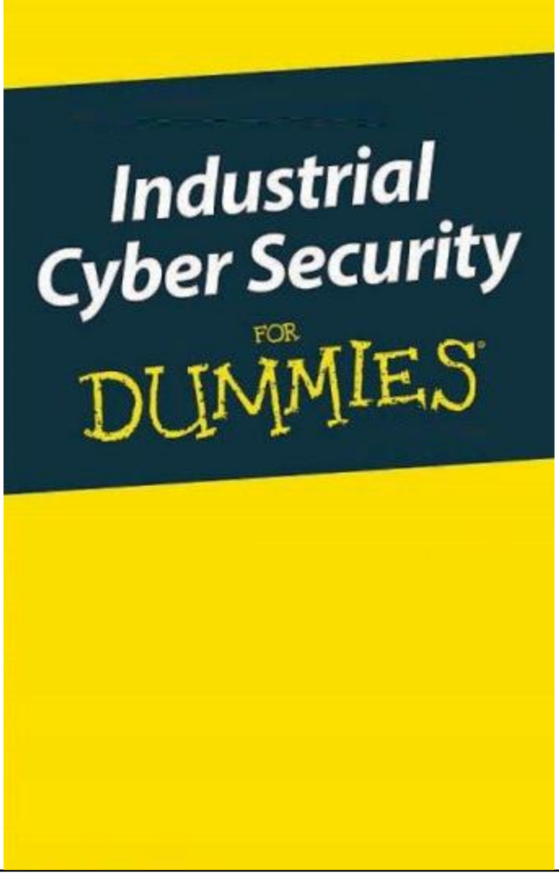
Nation state attacks

Untrained Employees

Untrained employees

- What are untrained employees?
- Untrained = not enough trained
- Trained in security awareness

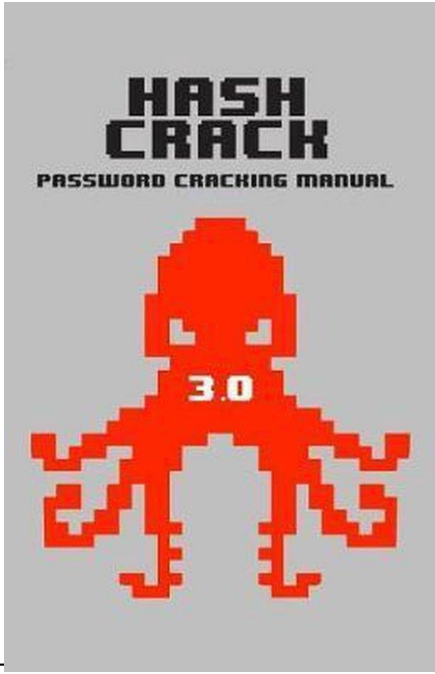
- Goal = real understanding of the risk in combination of the actions



Examples

- Charging a phone using the DCS or SCADA
  - Some phones will function as a normal USB stick

- Weak Passwords
  - Many passwords can be easily cracked
  - Zomer01, HarleyDavidson01
  - Passwords are everywhere
    - Firewall, network devices, Microsoft, DCS software



Examples

Gift USB per post

- Using Social Engineering find a victum
- USB contains malware

Phishing emails

- Compromise a laptop which is used for remote access to a DCS or SCADA
- Takeover the laptop, install keyloggers to grab the passwords…

Risks Untrained employees

Malware infection which can lead to

- Shutdown
- Ransomware infection
- Theft of secrets and information
- Impact to environment
- Worse case safety system mail function

Countermeasures

- Train the people during OT-awareness training
- The wake-up effect
  - I did not know this could happen
  - Show the people to hack to understand the ease
- Monitor your system
  - Anti virus, patch management, firewall, active directory
  - Who is monitoring the dashboard? Found viruses / login failures

Ransomware

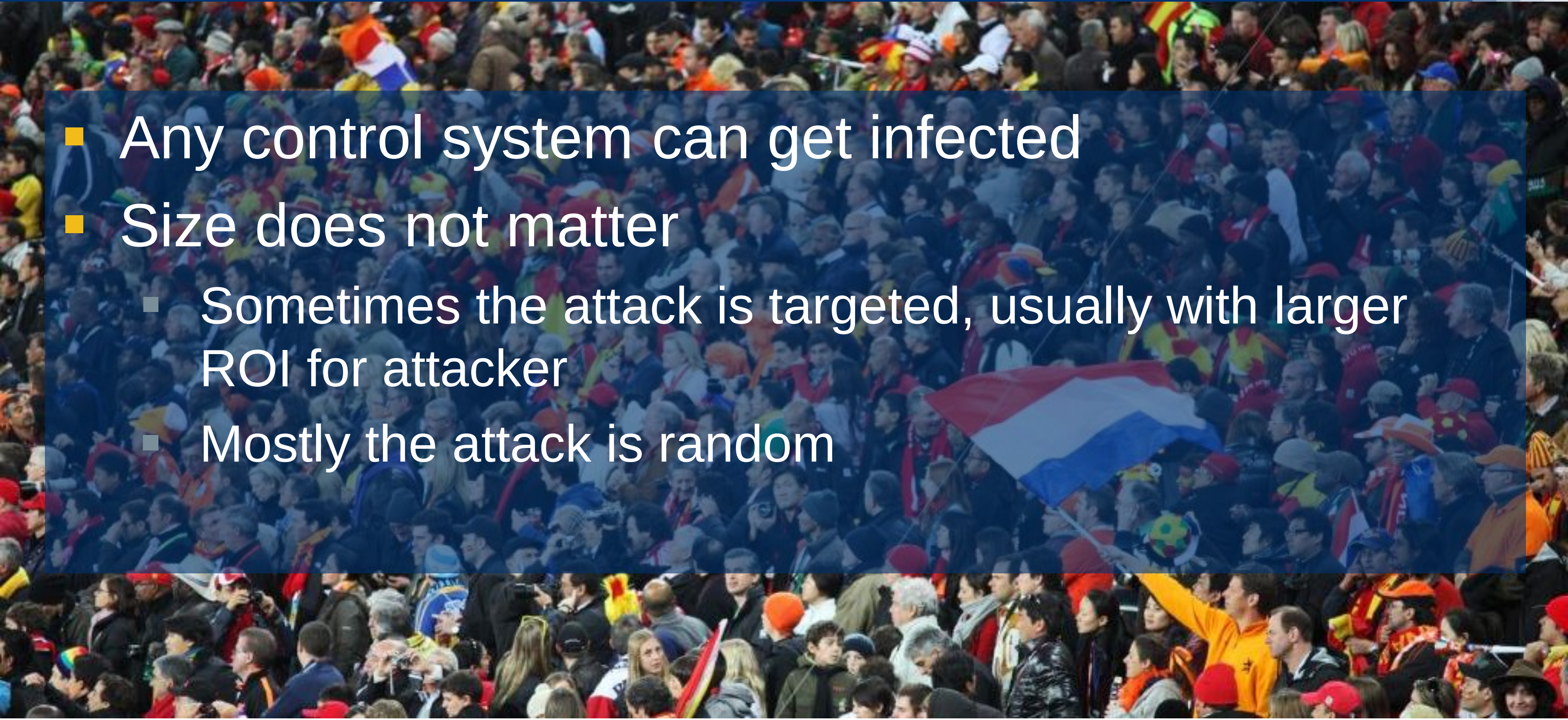
Ransomware Examples

- Honda hit by Ekans

- Power company hit by Ragnar

- Garmin hit by WastedLocker

Ransomware can happen to anybody



- Any control system can get infected
- Size does not matter
  - Sometimes the attack is targeted, usually with larger ROI for attacker
  - Mostly the attack is random

Ransomware risk goal is to make money

> *How much are you willing to pay if your plant gets ransomware?*

- Can information like annual reports be found?
- How vulnerable are you when hackers
  - shutdown your system?
  - make information public, like recipes?
- Or worse: threaten to manipulate recipe’s?

Counter measures

Have security measures fit for your purpose.

How?

Do a security risk assessment and setup a security program

- Have an (Offline) Backup available
- Implement security
- Monitor security

Nation State Attack

APT = Advanced Persistent Threat

Nations who are attacking other countries or companies. How to defend your company from other countries attacking? China, Russia, North Korea, America have a huge cyber army….

Purpose of Nation State Attack

- Steal technical knowledge, company secrets
- Intelligence gathering
- Strategic sabotage
- To be ready for a war, complementary to physical warfare

Risk

- Any tampering with the system can result in downtime
- Theft of company secrets
- Nation state can control your plant (like Gasline in Ukraine shutdown)

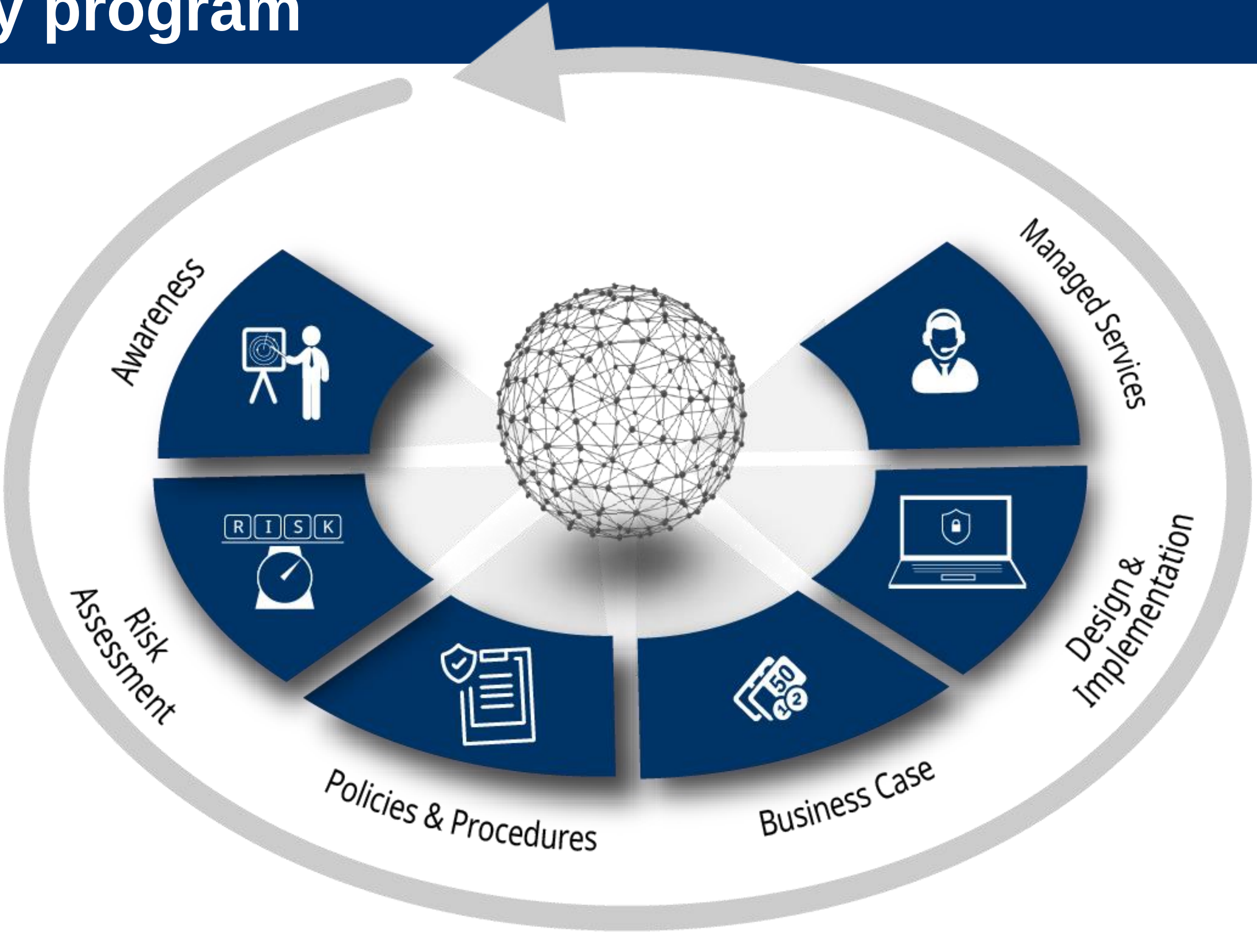
Countermeasure

Can you really defend against APT?

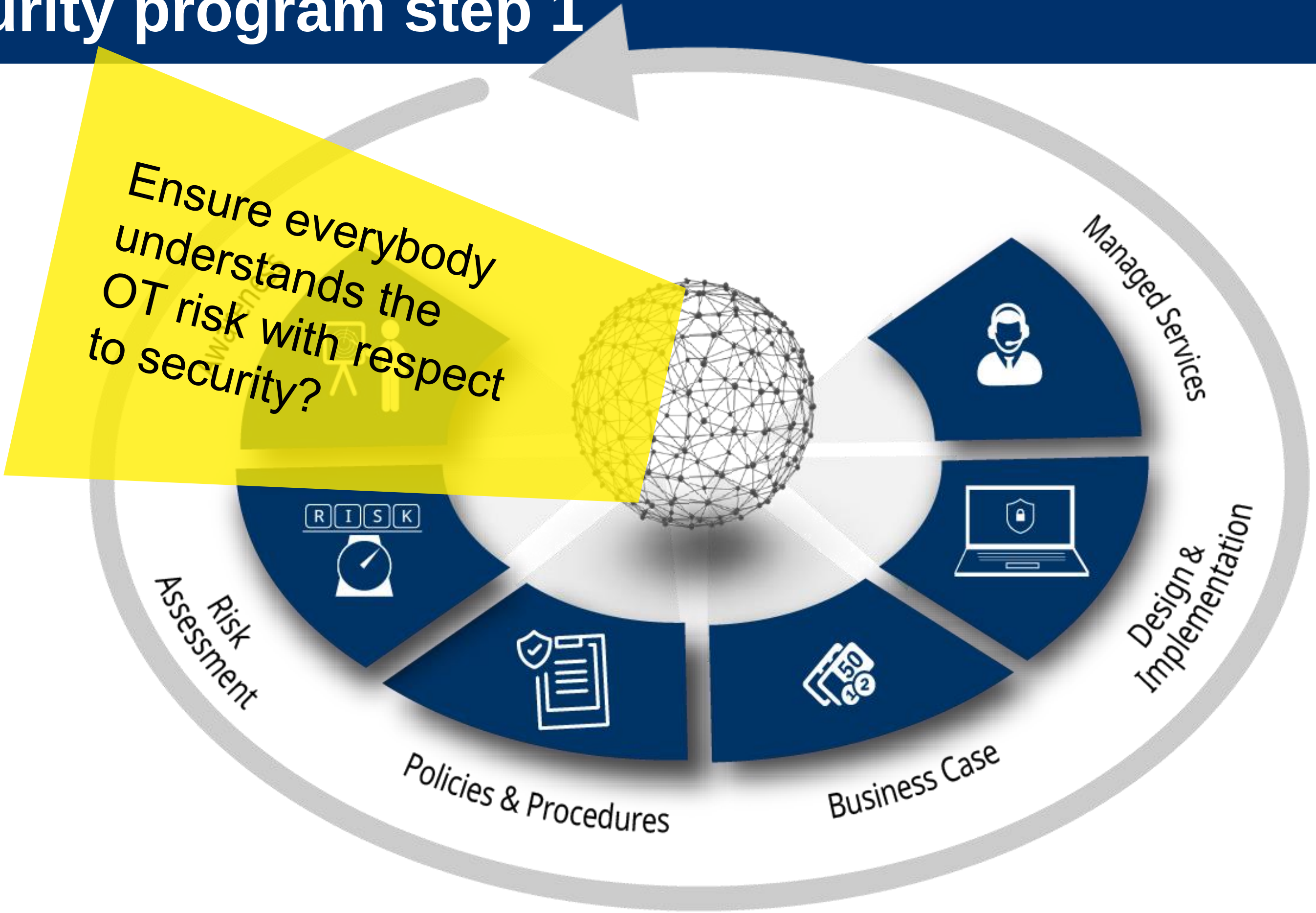
> *“If you really put your mind in it, you can make it really difficult for them”*

- Implement a full security program
- From management level enforce security mindset
- Use a standard, for example IEC 62443
  - Choose highest target security levels

Security program

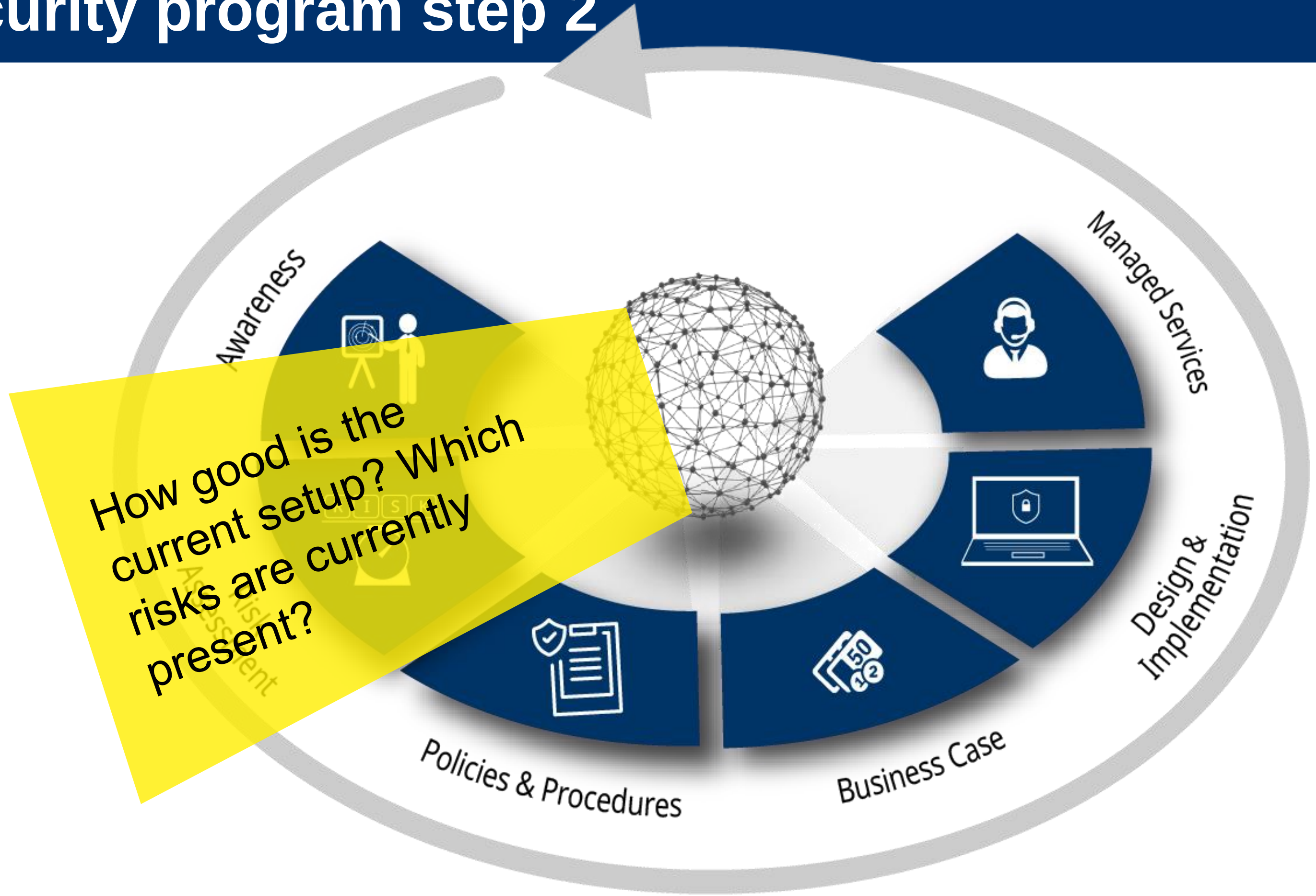


Security program step 1



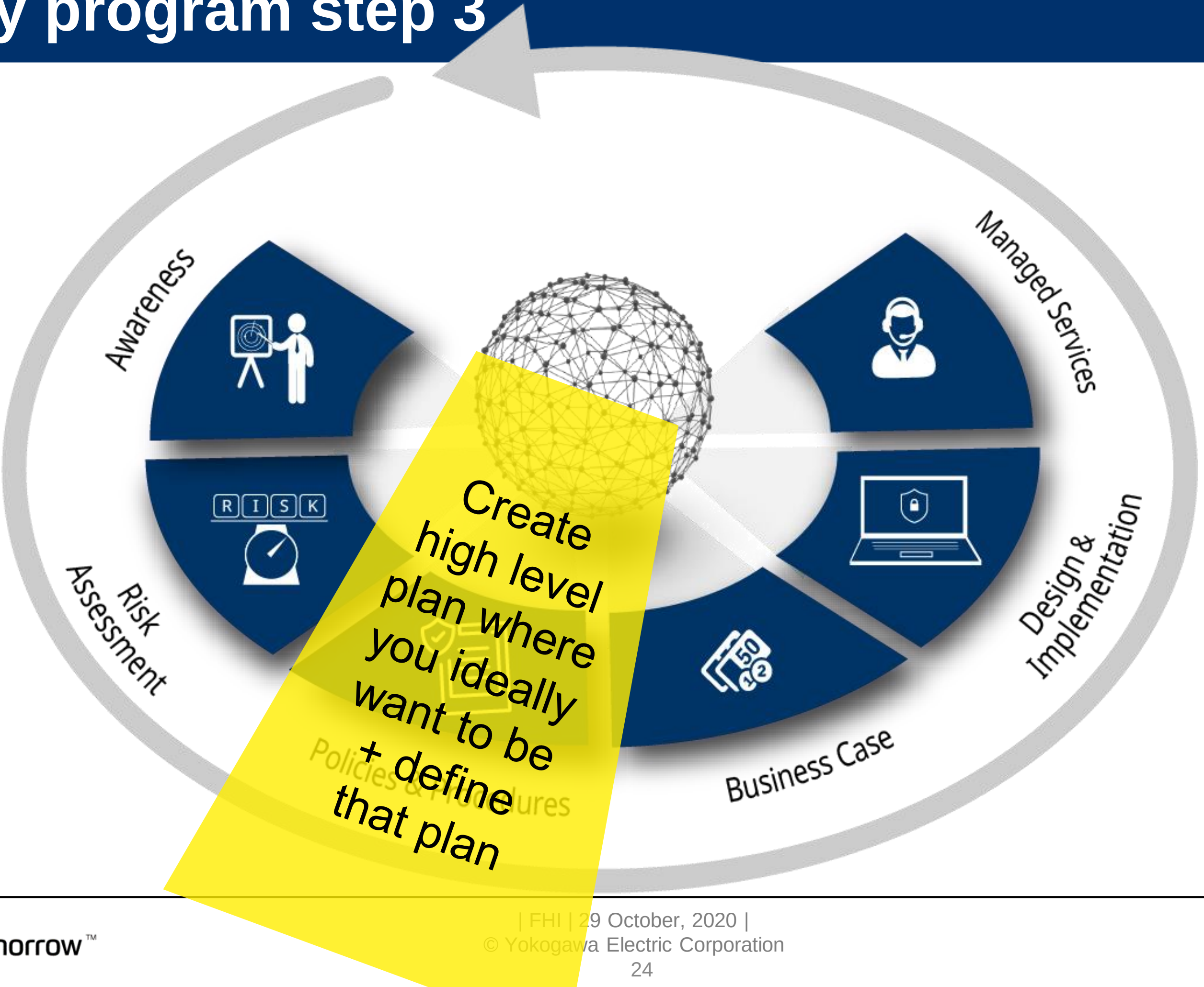
Ensure everybody understands the OT risk with respect to security?

Security program step 2



How good is the current setup? Which risks are currently present?

Security program step 3

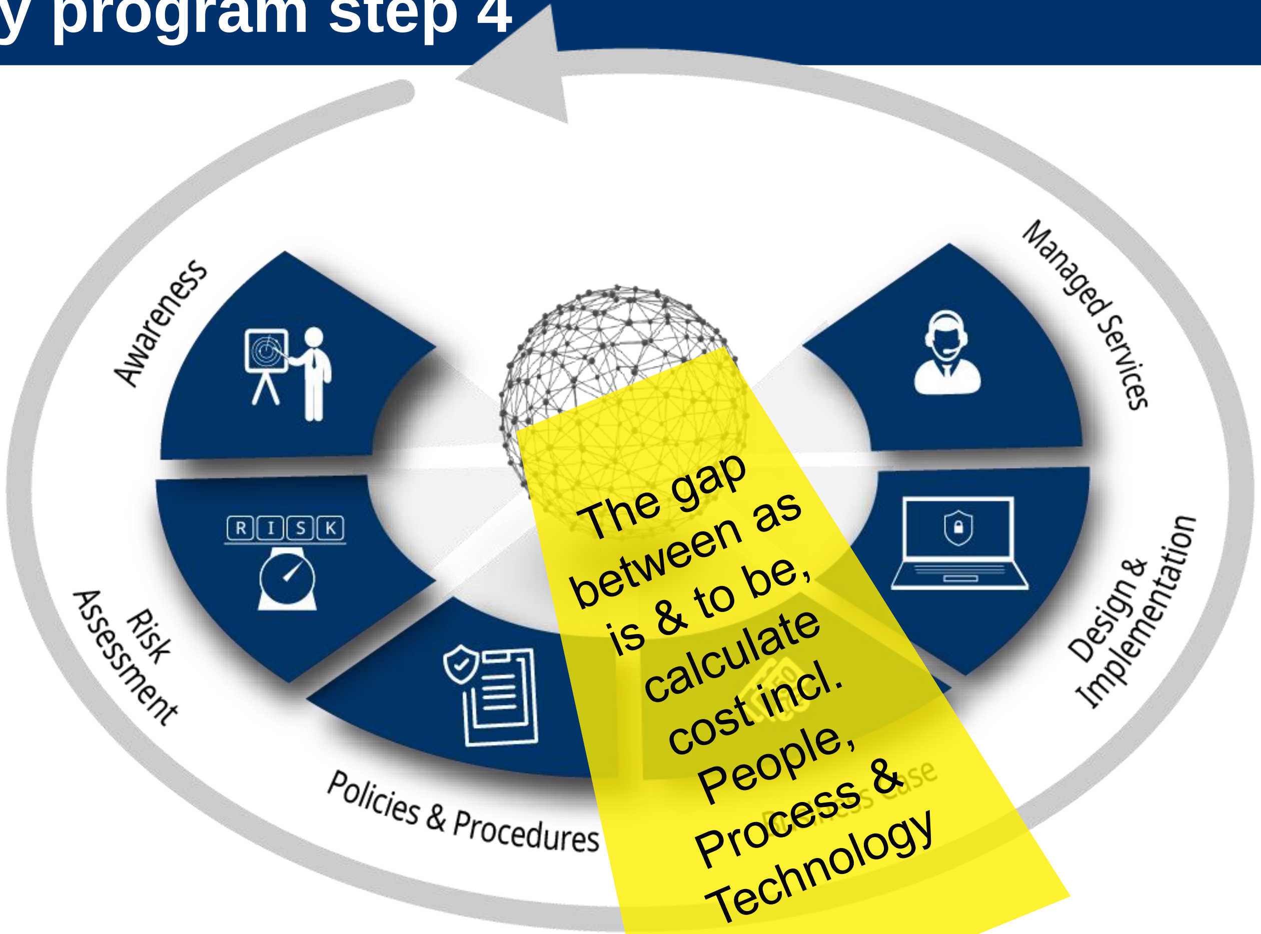


Create high level plan where you ideally want to be + define that plan

Co-innovating tomorrow™

YOKOGAWA

Security program step 4

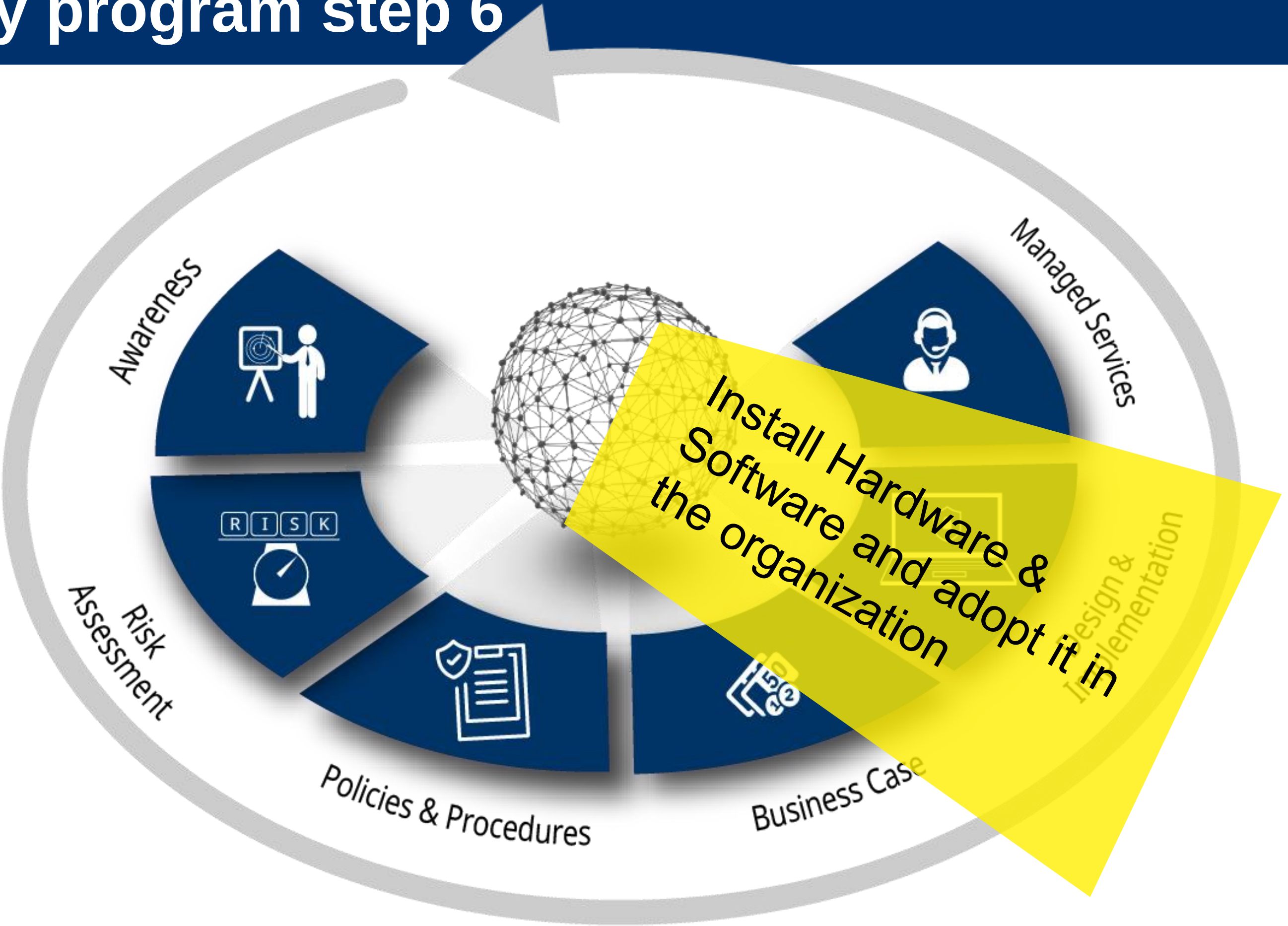


The gap between as is & to be, calculate cost incl. People, Process & Technology

Co-innovating tomorrow™

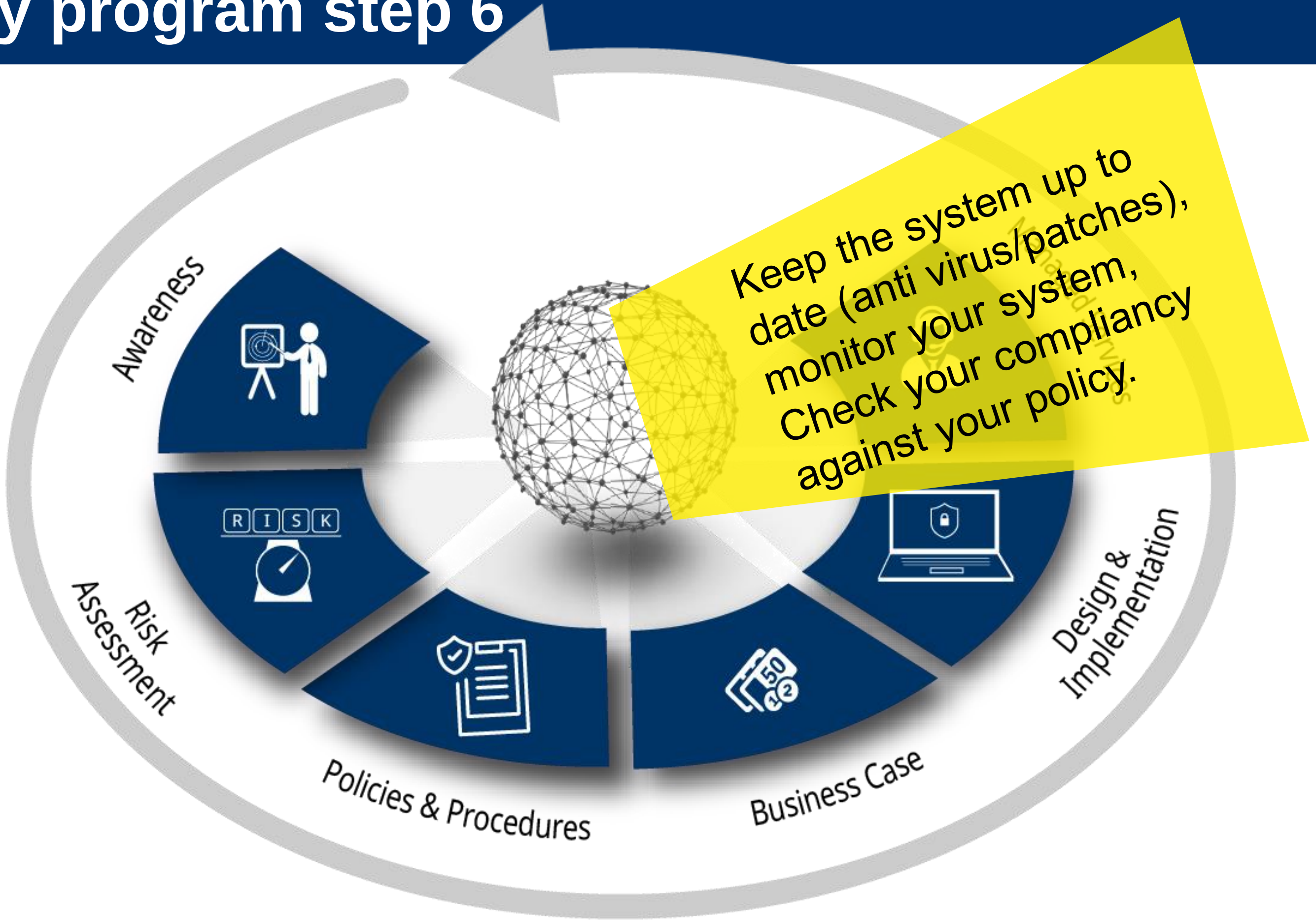
YOKOGAWA

Security program step 6



Install Hardware & Software and adopt it in the organization

Security program step 6



Keep the system up to date (anti virus/patches), monitor your system, Check your compliancy against your policy.

KEY TAKEAWAYS

1

Setup a security program, which defines the roadmap

2

Know your current status by doing a security risk assessment

3

Security counter-measures which are fitting to your system

4

Have up to date backups, including offline

5

Monitor your system with respect to security

Thank you for your attention

More information? Contact

Mark.Hellinghuizer@nl.yokogawa.com

INDUSTRIAL THREAT ANALYSIS NEWSLETTER

2020-02

e we have the following highlights:

Lessons learned of recent ransomware attacks

Want to stay up to date with the current threats?
Subscribe to the Security Newsletter →