# of cyber security

Speaker name
Title
Title

Event
Date
Location

IEC®
International
Electrotechnical
Commission

Dealing with cyber attacks

- Pinpoint most important assets
- Understand threats
- Establish defense architecture
- Assess resilience of defense (testing and certification)

Defense-in-depth

Multiple security counter measures needed

A Assessment

B Best practice to address risk

C Conformity assessment

Resilience: more than technology

- Risk management – right protection in right places
- Aligned with organizational goals
- Involve all stakeholders
- Systems approach

Three axes of cyber security

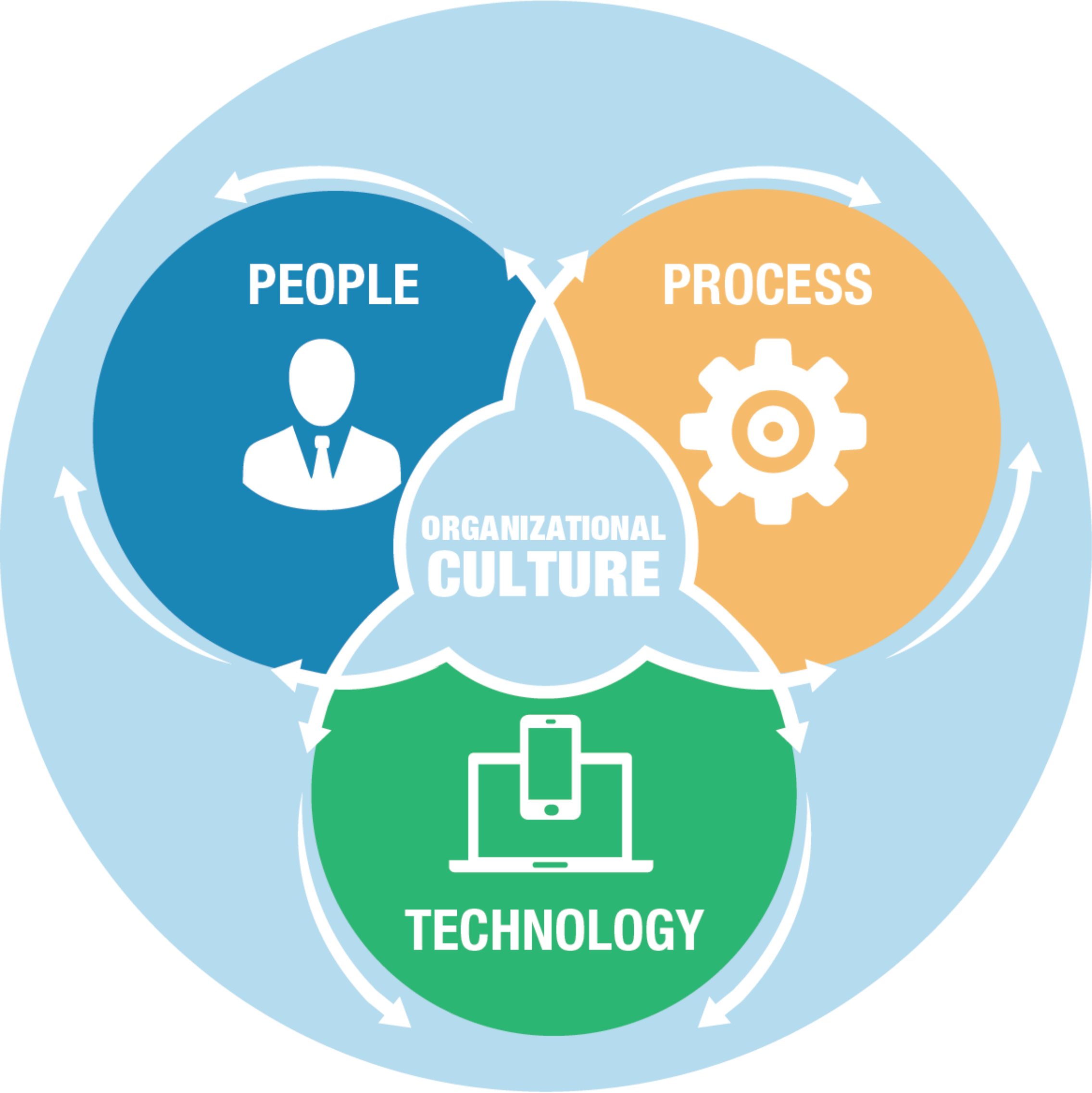


Image: Jonasblog.tk

Implementation

- Increase confidence of stakeholders
- Security measures based on best practice
- Effective and efficient
- Right Standards
- Right level of conformity assessment

Critical vs. non-critical systems

Not every cyber attack is equal:

- Home network or consumer device – annoying for the individual
- Critical infrastructure attacks = threat to business and society

IT

Information & communication technology

Virtual world - free flow of data

Online and computer networks

Identify, correct, protect from constant and evolving attacks – safeguard every layer

Constant upgrades and patches

OT

Operational technology

Physical world - ensure that all actions are properly executed - on/off, open/closed

Physical devices and processes – focus on security and efficiency

Long-term investment, upgrades take time

Two separate worlds are merging

OT

Closed systems – physical security mechanisms

Data breaches: new territory for OT teams

IT

Connected systems – virtual security protocols

IT teams: little experience with physical security requirements

Industrial Internet

Integration of physical machines with network sensors and software

Failure in OT systems

Significant physical impact:

- Faulty goods
- Injuries or deaths
- Environmental disasters
- Blackout = shutdown of essential services

Blackout

Protecting OT and IT systems

Over 200 IEC International Standards for cyber security

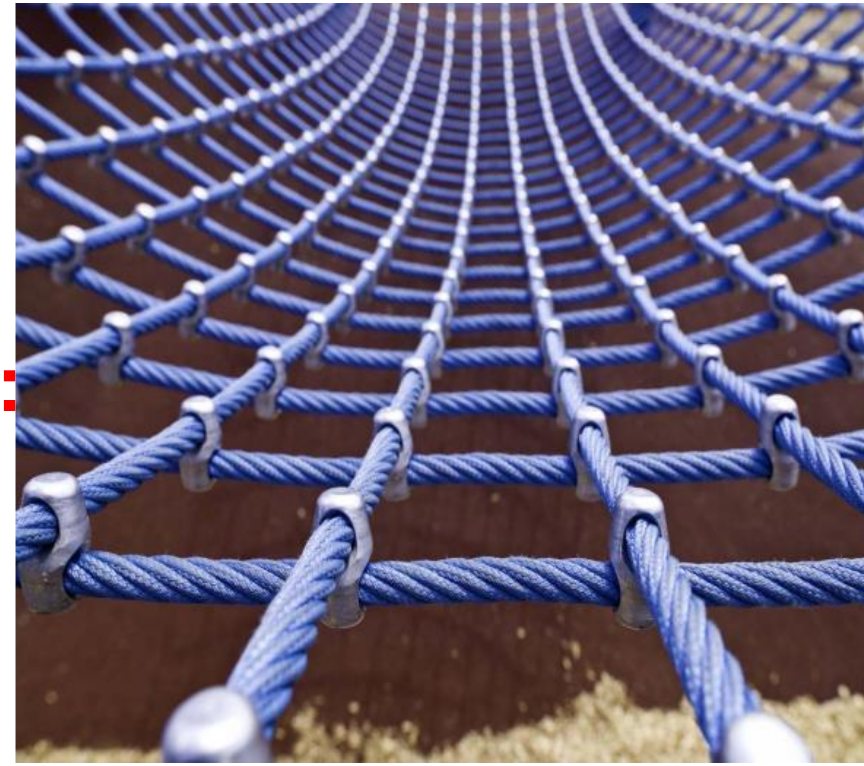
Horizontal: generic and flexible

Vertical: for specific needs

Secure overall Standards framework

Protection of IT systems:

ISO/IEC 27000



Protection of OT systems:

IEC 62443 series

IEC 61511

Customs solutions: vertical Standards

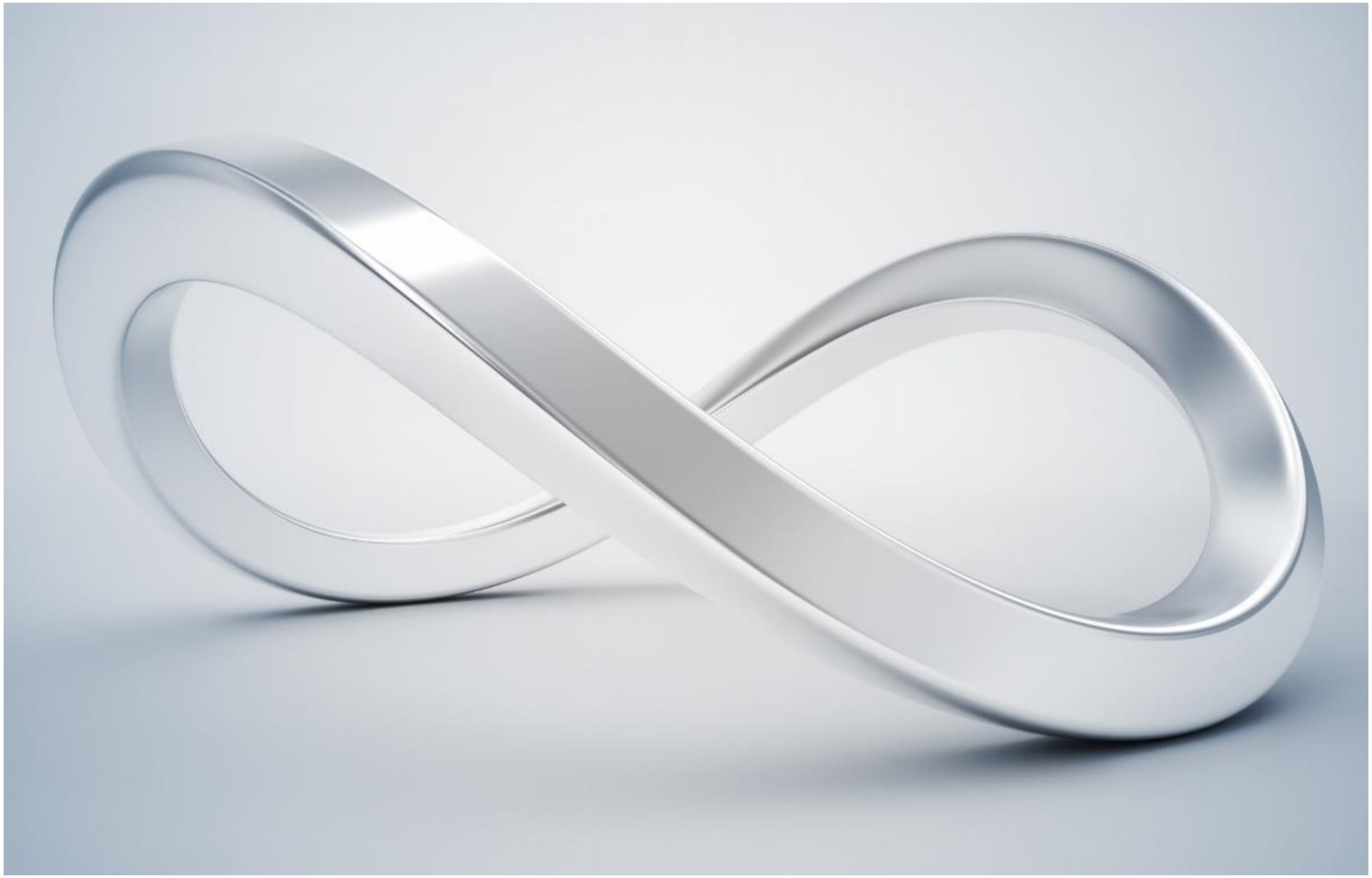
Nuclear – IEC 62859

Developed with IAEA

Standards + testing/certification

- Certification for information security management systems based on ISO/IEC 27001
- IECEE security Infrastructure Solution based on IEC 62443 series

Long-term cyber resilience: an on-going process



Global risks, global approach

Prefer common platforms that encourage cooperation and avoid island solutions

IEC Standards:

- Global reach – 171 countries
- Members = countries
  not companies
- Built-in high consensus value
- Neutral, independent

Provide input to standardization