European Standardization Organizations

We start at 10:00 CET

Workshop ’Security in the cyber-physical space’

8 February 2022

Your webinar moderator

Els Somers

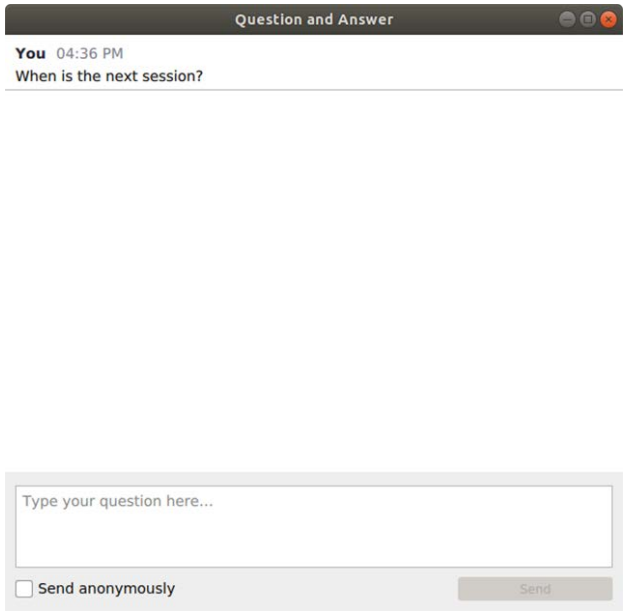
Project Manager

Policy & Partnerships

esomers@cencenelec.eu

Get the most out of the webinar today

- You are muted
- Use the Q&A panel to submit your questions



- Talk about us on Twitter #training4standards @Standards4EU

Introduction CEN & CENELEC

Christina THORNGREEN
Project Manager 'Energy & Living'
CEN-CENELEC
cthorngreen@cencenelec.eu

European Standardization Organizations

CEN - European Committee for Standardization

CENELEC - European Committee for Electrotechnical Standardization

ETSI - European Telecommunications Standards Institute

→ Recognized by European law (EU Regulation 1025/2012)

Standardization happens at different levels

- Aim: identical standards in Europe and worldwide

National

European

International

CEN and CENELEC deliverables

European Standards (EN)

Prime deliverable

Technical Specifications (TS)

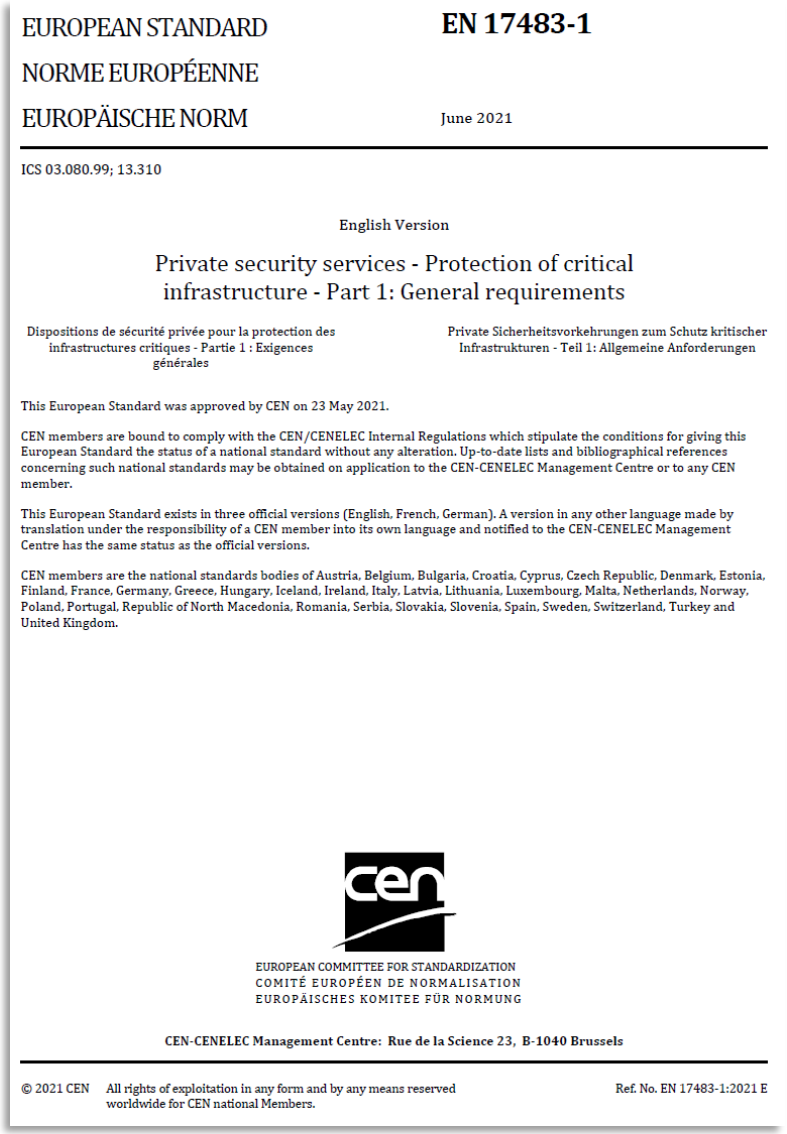
Pre-standard

Technical Reports (TR)

Informative document / Guide

Workshop Agreements (CWA)

Document, developed by a Workshop, which reflects an agreement between identified individuals and organizations responsible for its contents



EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 17483-1

June 2021

ICS 03.080.99; 13.310

English Version

Private security services - Protection of critical infrastructure - Part 1: General requirements

Dispositions de sécurité privée pour la protection des infrastructures critiques - Partie 1 : Exigences générales

Private Sicherheitsvorkehrungen zum Schutz kritischer Infrastrukturen - Teil 1: Allgemeine Anforderungen

This European Standard was approved by CEN on 23 May 2021.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

© 2021 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. EN 17483-1:2021 E

Today's agenda

Catherine PIANA

Director General of CoESS – Confederation of European Security Services

Chair of CEN/TC 439 - Private security services

catherine@coess.eu

Today's agenda

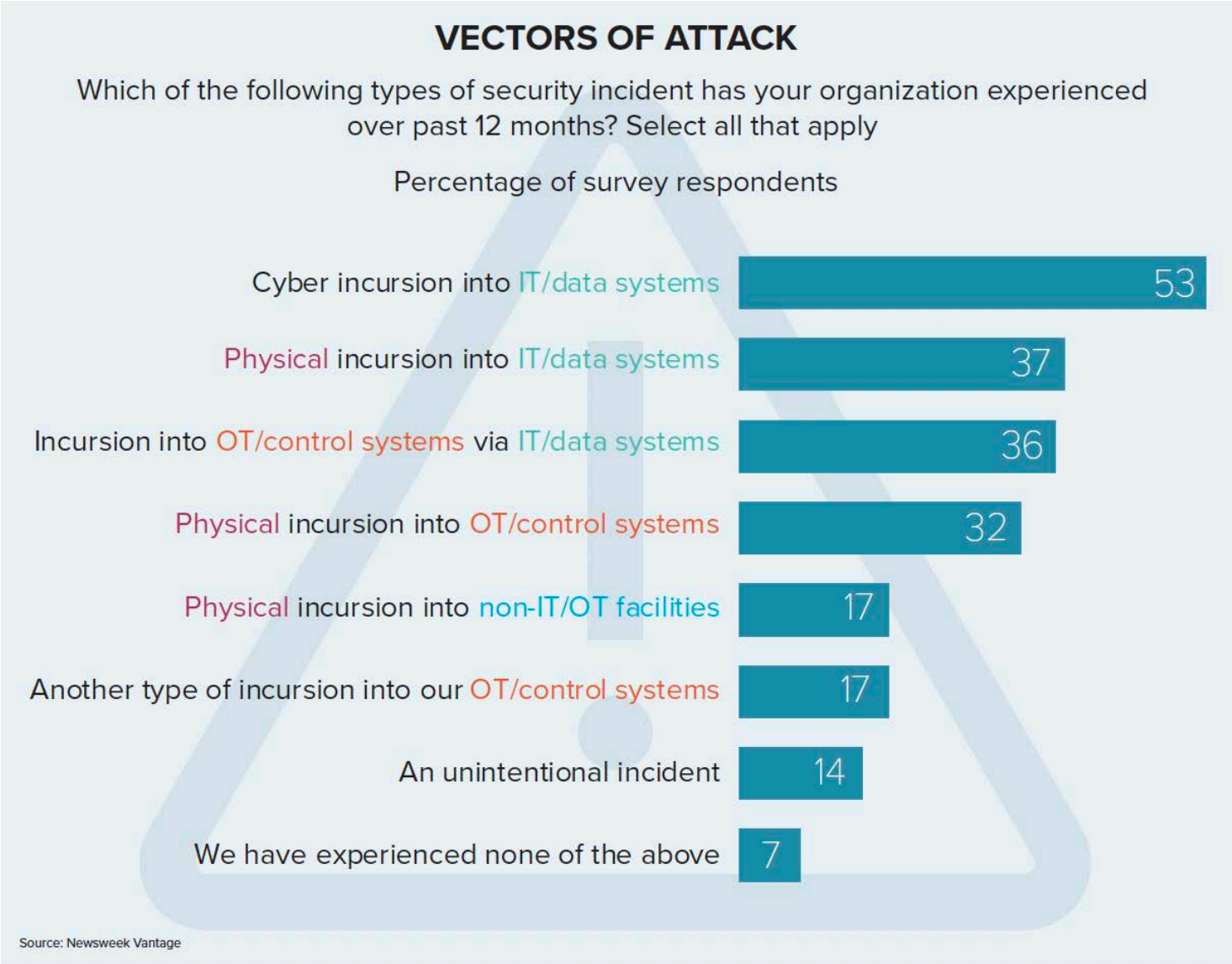
- Discuss if there are physical vulnerabilities arising from IT systems
- Likewise, find out if there are cyber vulnerabilities arising from the physical side
- If yes, what should we do about them?

Definitions

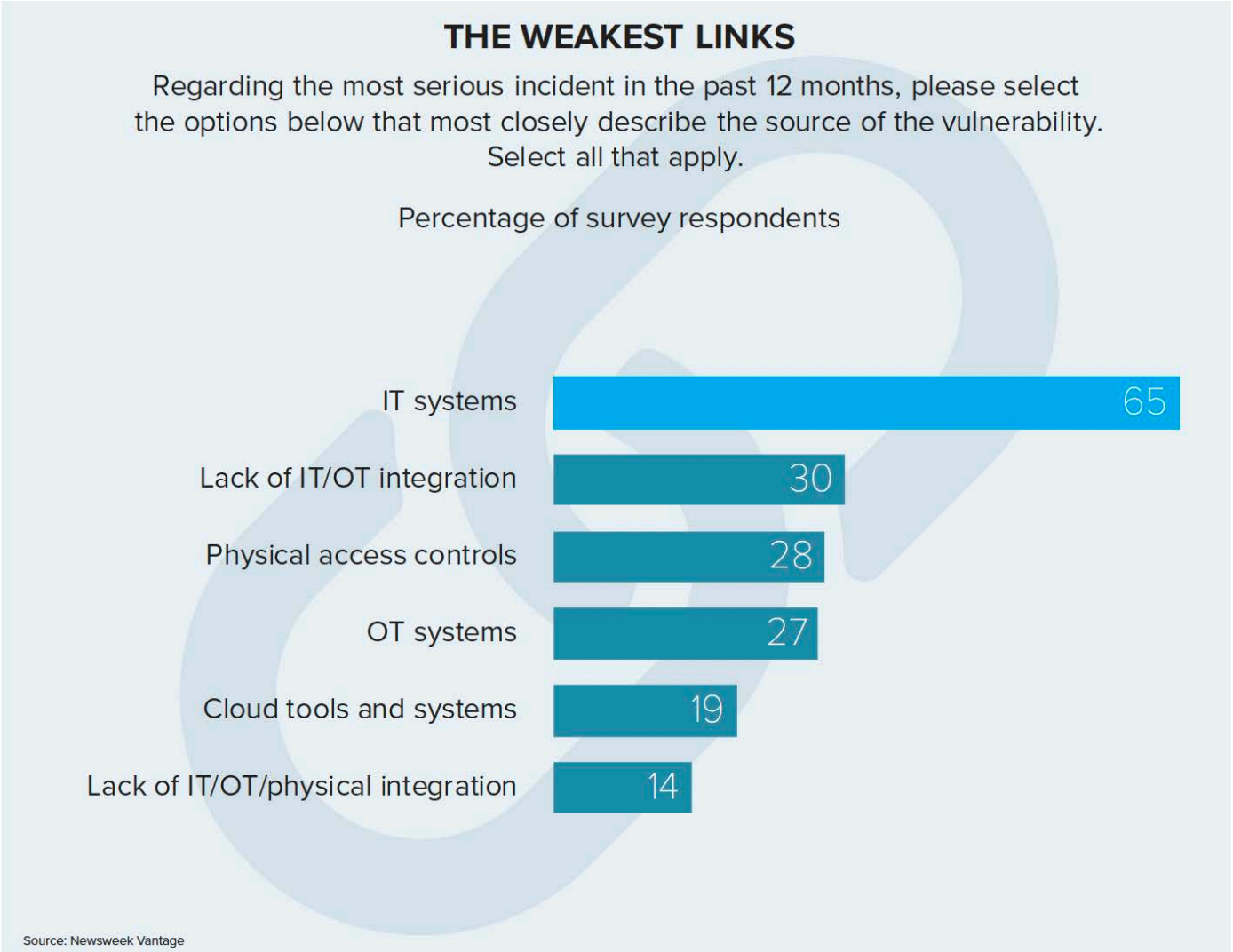
- Cybersecurity: the activities necessary to protect network and information systems, the users of such systems and other persons affected by cyber threats.
  - Cybersecurity Act – Regulation 2019/881

- CPS - Cyber-physical Systems: Engineered systems that orchestrate sensing, computation, control, networking and analytics to interact with the physical world (including humans) and enable safe, real-time, secure, reliable, resilient and adaptable performance.
  - From Newsweek Vantage report “Weathering the Perfect Storm”

Are cyber-physical threats real?



Cyber-physical: where is the biggest risk?

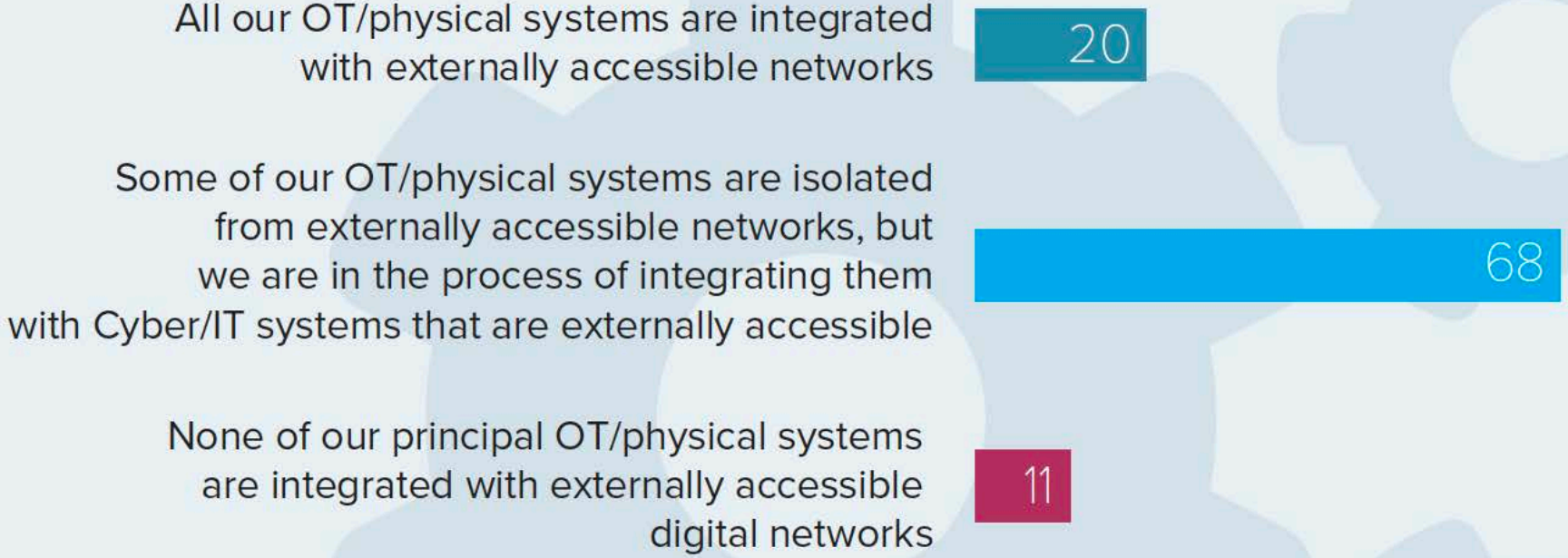


Reality check

FEW FULLY INTEGRATED

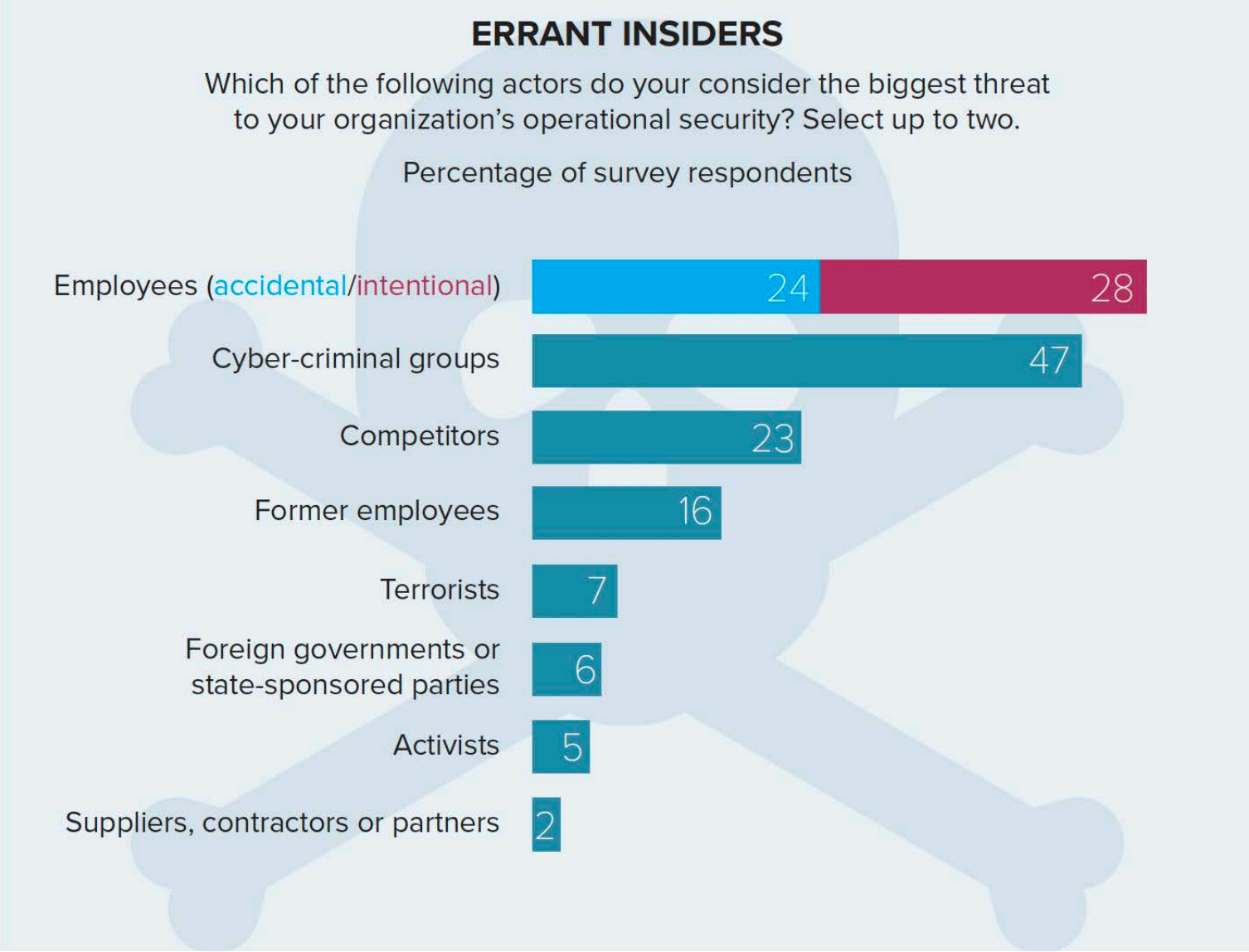
Which of the following statements best describes the state of integration between your organization's cyber systems and OT/physical systems?

Percentage of survey respondents



Source: Newsweek Vantage

What is the biggest threat?



Your speakers today

Johan GORDTS

Chairperson Aviation Security Services Association – international (ASSA-i)

VP Business Development, Securitas Transport Aviation

johan.gordts@securitas.be

Aviation Ecosystem

- Multiple stakeholders
- Highly interconnecting systems
- Increasing digitalisation
  - IoT
  - AI
  - Open architecture platform

CPS in aviation

- Merge of cyber and physical worlds
  - Enables remote management
  - Real-time processing
  - Optimising processes & costs
  - Improving standard levels, service delivery and end user experience (or PAX experience).

Essentials of EU AVSEC Cybersecurity **Regulation 2019/1583**

- New standards introduced: Reg 2019/1583 amending Implementing Reg 2015/1998
- Aligned with: Amendment 16 to **ICAO Annex 17** (4.9.1 NEW Standard)
- Subject: revision includes **cyber security provisions**
- Scope: airports, operators and **entities** that provide services or goods
- Date of implementation: 31/12/2021

Key challenges

- **Progress of harmonizing** processes of aviation cybersecurity approach (national/ regional levels);
- **Consistency of implementation** to avoid creates different dynamics and effectiveness at various operational levels;
- **Integration** approach of OT/ IT and physical security;
- **End-user education**. Your system is only as strong as its weakest link and in cybersecurity, the weakest link is very often the end-user.
- Responsibility and **liability** concerns;

The way forward - step by step approach

- **Mapping and prioritising** of critical aviation information and physical systems;
- Implementation of **enhanced risk analysis** – new risk vectors, including **insider threats**;
- Focus on **training and educational processes** that stresses the importance of cyber security awareness and measures;
- Strengthening of **aviation cyber security culture** at all stakeholder levels;
- Continuously **update and implement standards** and legal framework with authorities and stakeholders including liability issues.
- Launching **internal quality control and compliance** measures aiming to ensure regulatory consistency, detect gaps and reinforce targeted trainings measures;

Aviation cybersecurity update

Alexis PERIER

Policy Officers

European Commission

DG MOVE – Directorate-General for Mobility & Transport

Directorate A – Policy Coordination

Unit A5 - Security

Máté GERGELY

Cybersecurity requirements under the AVSEC framework

- **Regulation 2019/1583** transposed relevant cybersecurity standards in ICAO Annex 17 by amending **Regulation 2015/1998** laying down detailed measures for the implementation of the common basic standards on aviation security
- Entry into force: 31 December 2021
- Member States and industry have been preparing for the implementation of the requirements
- DG MOVE has provided guidance

1.7.1 of Annex to Reg. 2015/1998

- "The appropriate authority shall ensure **that airport operators, air carriers and entities… identify and protect their critical information and communications technology (ICT) systems and data from cyber attacks** which could affect the security of civil aviation."

- General requirement on cyber protection as part of aviation security

1.7.2 of Annex to Reg. 2015/1998

- Airport operators, air carriers and entities shall **identify**… the **critical ICT systems and data**.
- They shall introduce **detailed measures** to ensure the protection from, detection of, response to and recovery from cyber-attacks.
- In accordance with a **risk assessment**.

11.1.2 of Annex to Reg. 2015/1998

- Persons having administrator rights or unsupervised and unlimited access to critical ICT systems and data…, or having been otherwise identified in the risk assessment shall be subjected to
- **Background checks**

11.2.8.1 of Annex to Reg. 2015/1998

- Persons implementing the [cybersecurity] measures shall have the skills and aptitudes required to carry out their designated tasks effectively.
- They shall be made aware of relevant cyber risks on a need-to-know basis.

- **Training + access to information** (need-to-know)

11.2.8.2 of Annex to Reg. 2015/1998

- Persons having access to data or systems shall receive appropriate and specific job-related training commensurate with their role and responsibilities, including being made aware of relevant risks where their job function requires this. The appropriate authority… shall specify or approve the content of the course.
- **Specific training** of key staff with access rights + inform them
- Training to be established or approved by authority

Transport Cybersecurity Toolkit

- DG MOVE published a Transport cybersecurity toolkit in all EU languages (available here)
  - Objective is to contribute to higher levels of cyber-awareness in the transport sector
  - The toolkit lists practical tips and recommended practices
  - It is organized in two levels: Basic and Advanced
- While not its main focus, the toolkit recommends practices relevant for cyber-physical security:
  - Locking physically and digitally all systems and devices if unattended
  - Considering physical security as an integral part of an organisation's cybersecurity management system
  - Implementing access control
  - Revoking credentials upon contract termination

EN IEC 62443
Cyber Security Standards for Operational Technology

Judith ROSSEBO

Chairperson CLC/TC 65X 'Industrial-process measurement, control and automation'

Co-Convenor CLC/TC65X WG 3 'Cyber Security'

judith.rossebo@no.abb.com

Cyber Attacks Happen!

Destroy industrial processes

Derail city trams with injuries

Cause Power outages

Poison water supply

Sources:
https://www.wired.com/2008/01/polish-teen-hac/
https://www.wired.com/story/crash-override-malware/
https://www.wired.com/story/oldsmar-florida-water-utility-hack/

EN IEC 62443

Cyber Security Standards for Operational Technology

- Systematic approach
- Risk based
- Applied across a wide range of sectors
  - Utility grids and systems
  - Hydropower facilities
  - Offshore wind
  - Railway, shipping and aviation
  - Building control
  - Industrial automation and IIoT

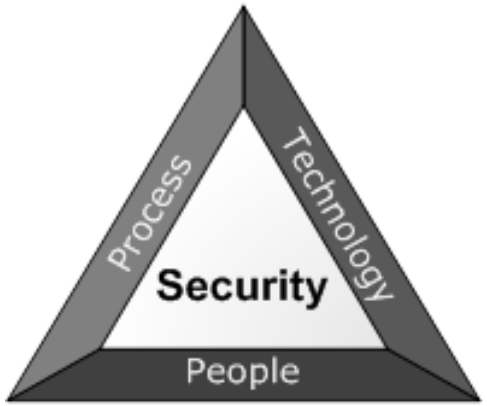
Photo: https://etech.iec.ch/issue/2020-04/iec-62443-standards-a-cornerstone-of-industrial-cyber-security

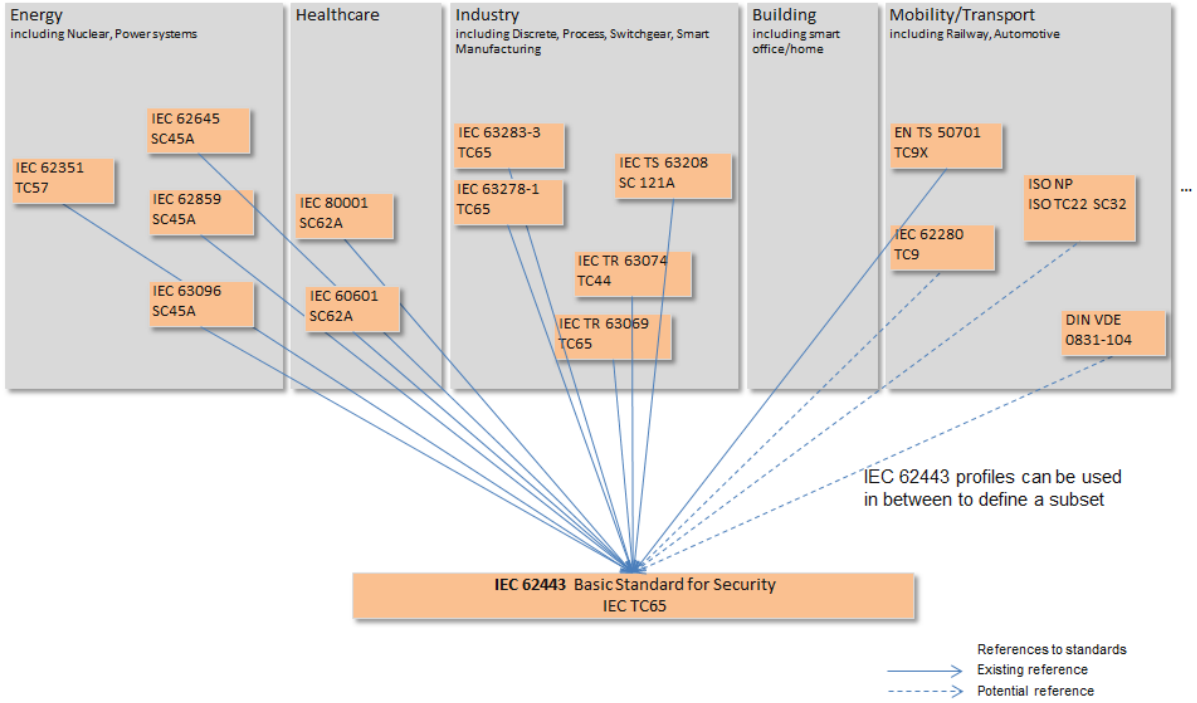
Cyber Security for OT and IT

- 62443 is a series of standards being developed by two groups:
  - ISA99 → ISA-62443
  - IEC TC65/WG10 → IEC 62443 → EN IEC 62443 (CLC/TC65X)
- In consultation with:
  - ISO/IEC JTC1/SC27 → ISO/IEC 2700x → EN ISO/IEC 2700x (JTC13)

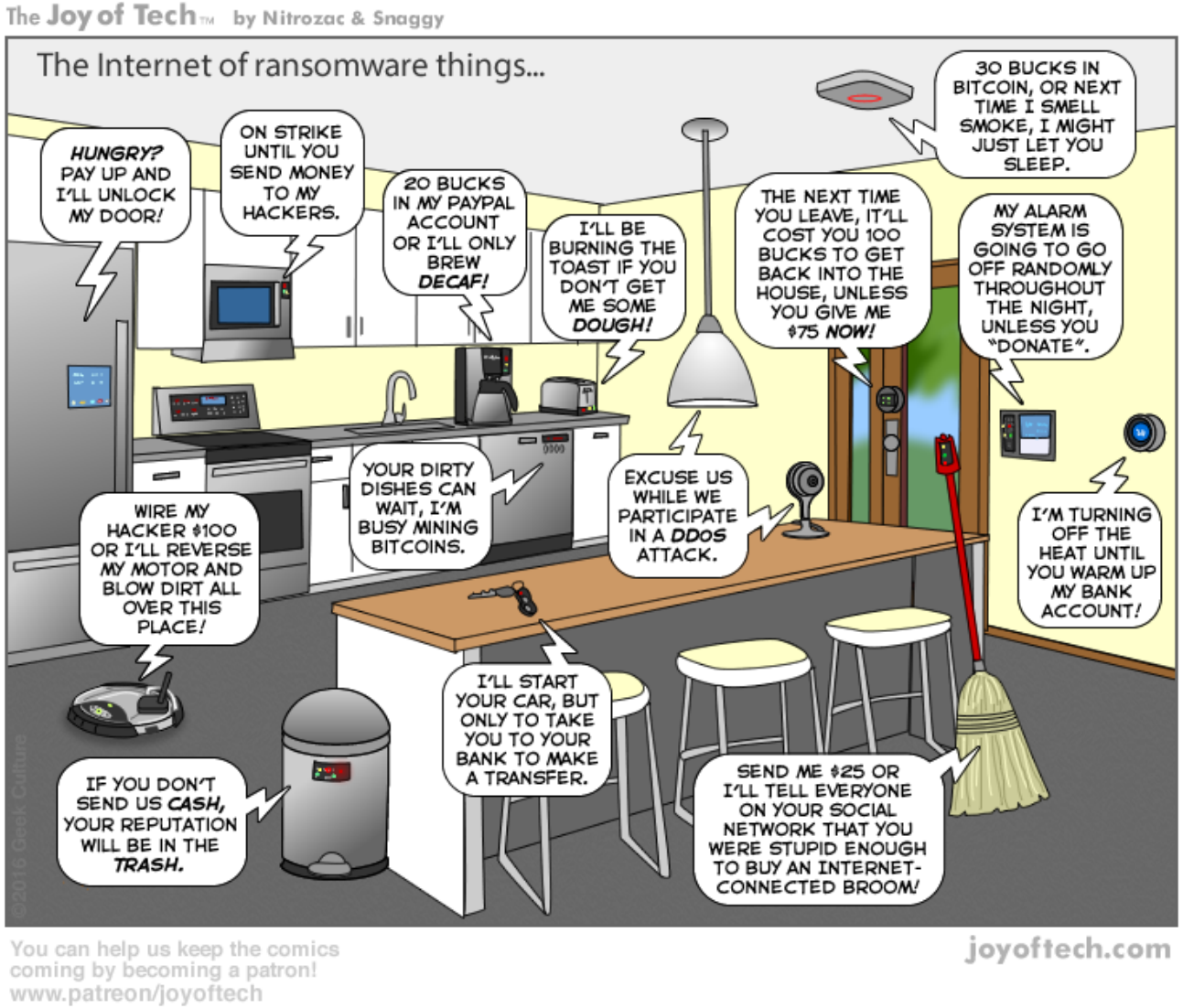
IEC 62443 horizontal standards for OT

- -1-1 Terminology, concepts and models
- -2-1 Establishing and IACS security program
- -2-4 Security program requirements for service providers
- -3-2 Security risk assessment for system design
- -3-3 System security requirements and security levels
- -4-1 Secure product development lifecycle requirements
- -4-2 Technical security requirements for IACS components



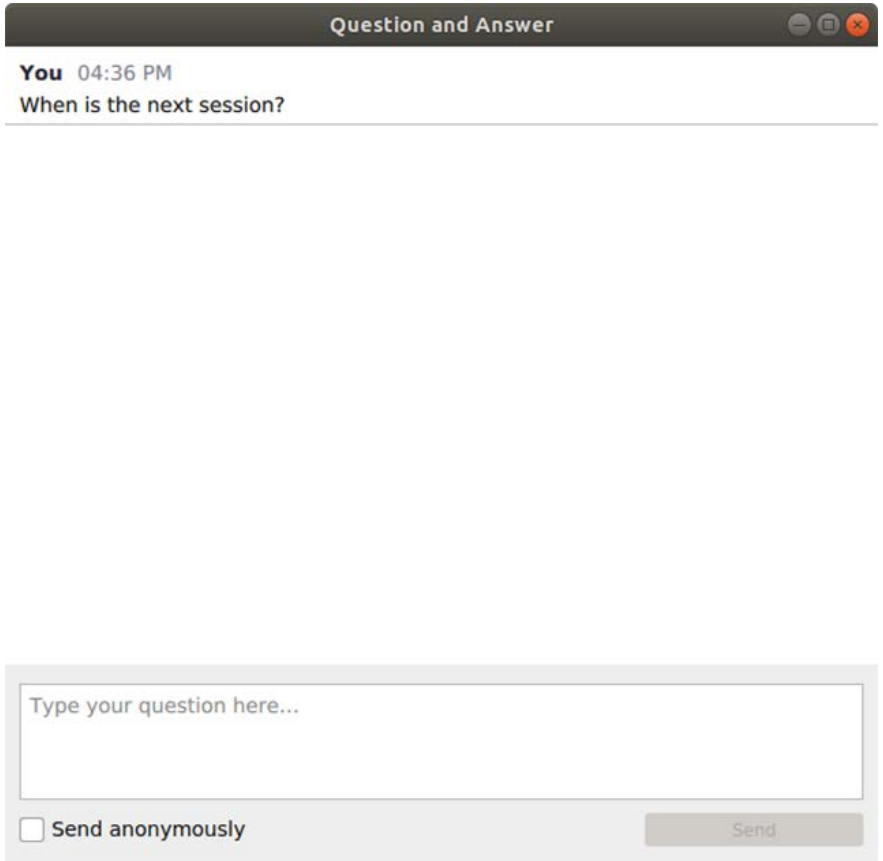


Thanks for listening!



Question time

- Use the Q&A panel to submit your questions



European Standardization Organizations

Thank you for your participation!

Next webinars

2022-02-28 - Workshop 'Standardisation synergies between civil security, defence and space industries'

2022-03-15 - Cybersecurity Standardisation Conference 2022 (cooperation between ENISA, ETSI, CEN & CENELEC)

2022-04-21 – Workshop 'Interoperability of security'