ANCE

ITU - World Telecommunication/ICT Indicators Symposium 2017

Hammamet, Tunisia, 14 to 16 November 2017

Measuring Cybersecurity Effectiveness

Dr. Syrine Tlili

CEO, National Agency for Digital Certification

Broadband and Cybersecurity

ICT and broadband are key drivers to achieve economic growth and enhance well-being.

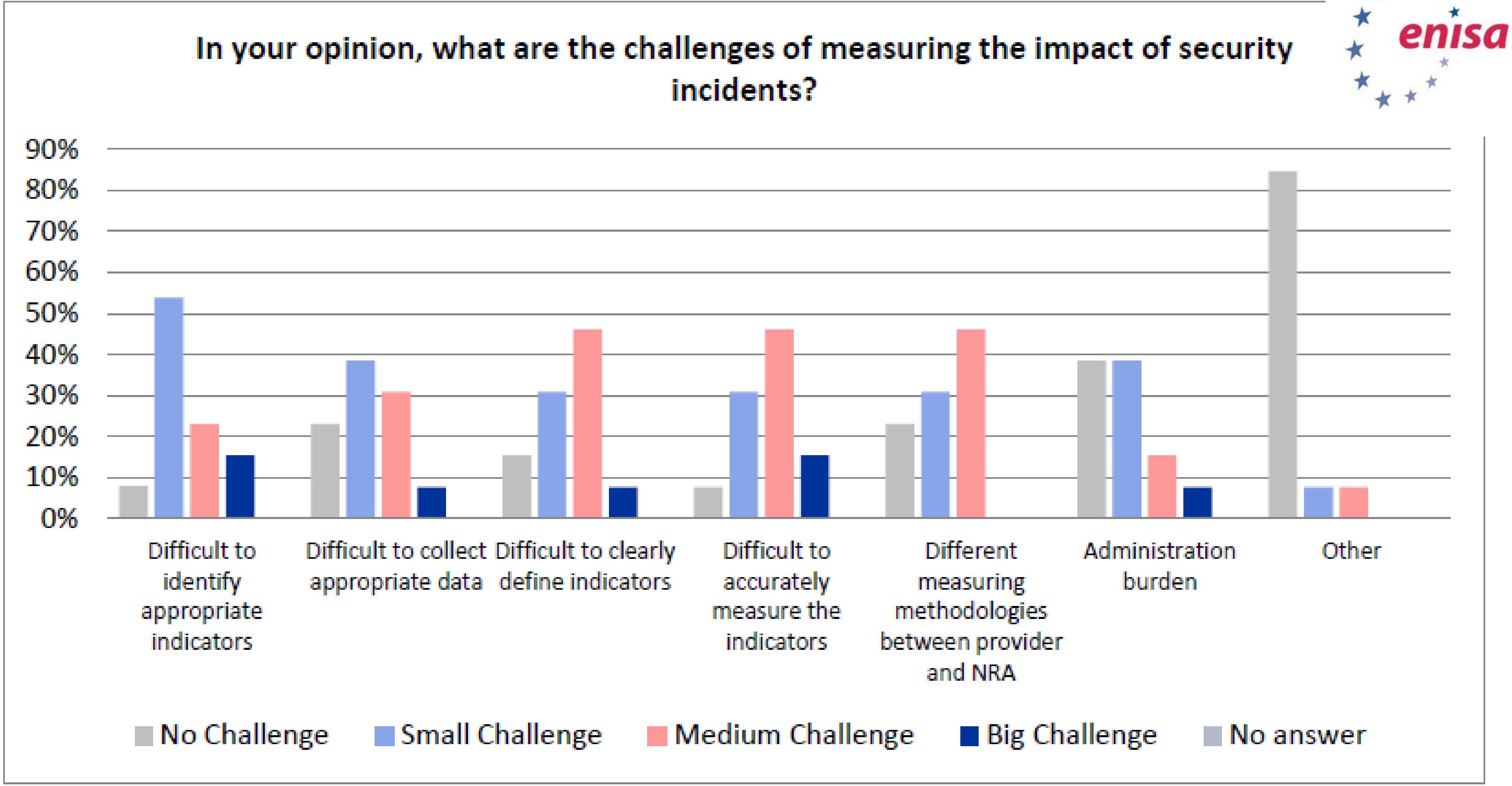
shopping, banking, water and electricity supply, social networking, health care, education, traffic management and commerce

Are we ready for this ever-growing digital world ?

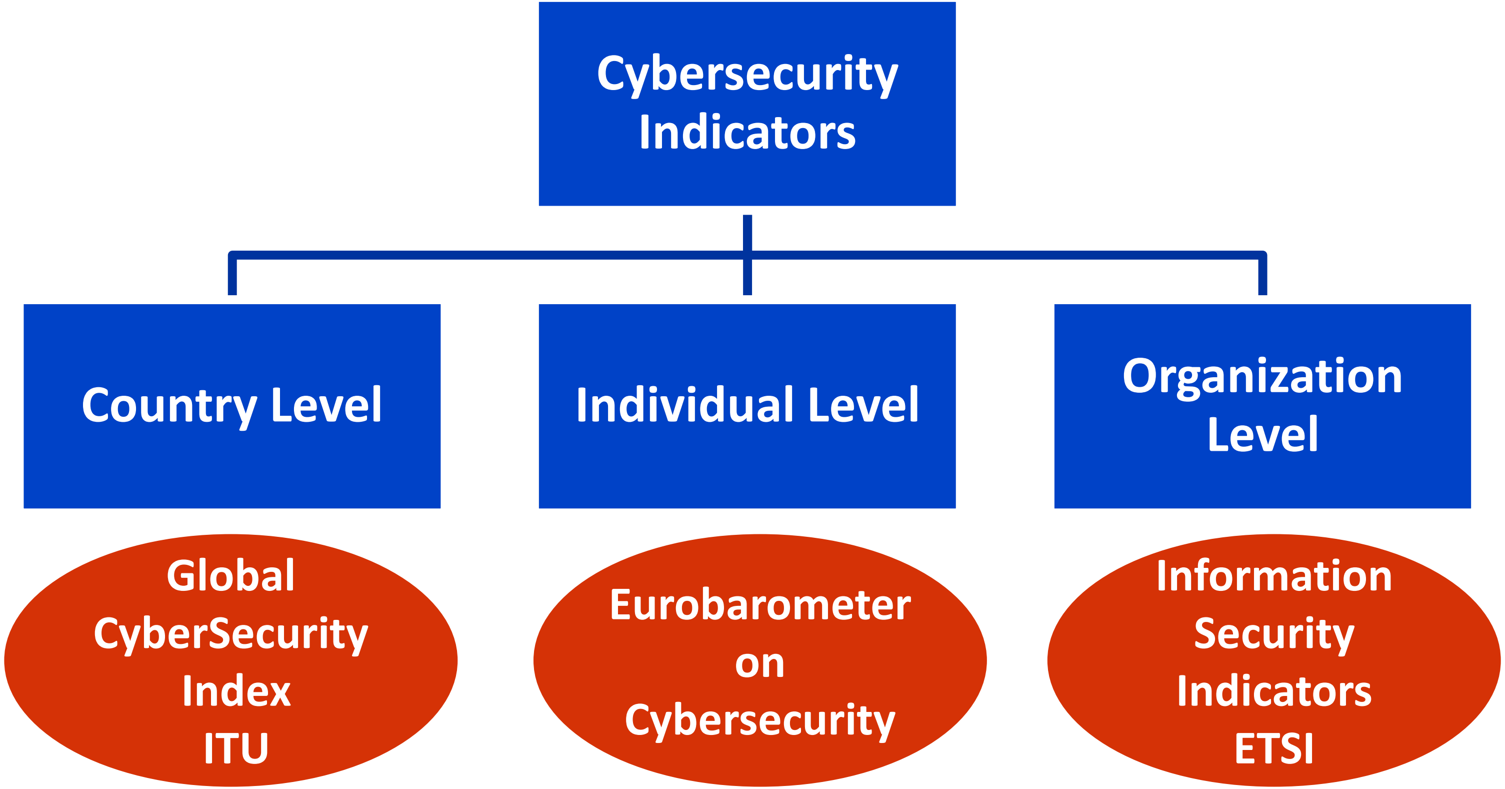
CyberSecurity Challenges

« If you can’t measure it,
you can’t manage it »

Figure 1: Challenges of measuring security incidents - NRAs



Qualitative / Quantitative Indicators



Cybersecurity Indicators

Country Level

Individual Level

Organization Level

Global CyberSecurity Index ITU

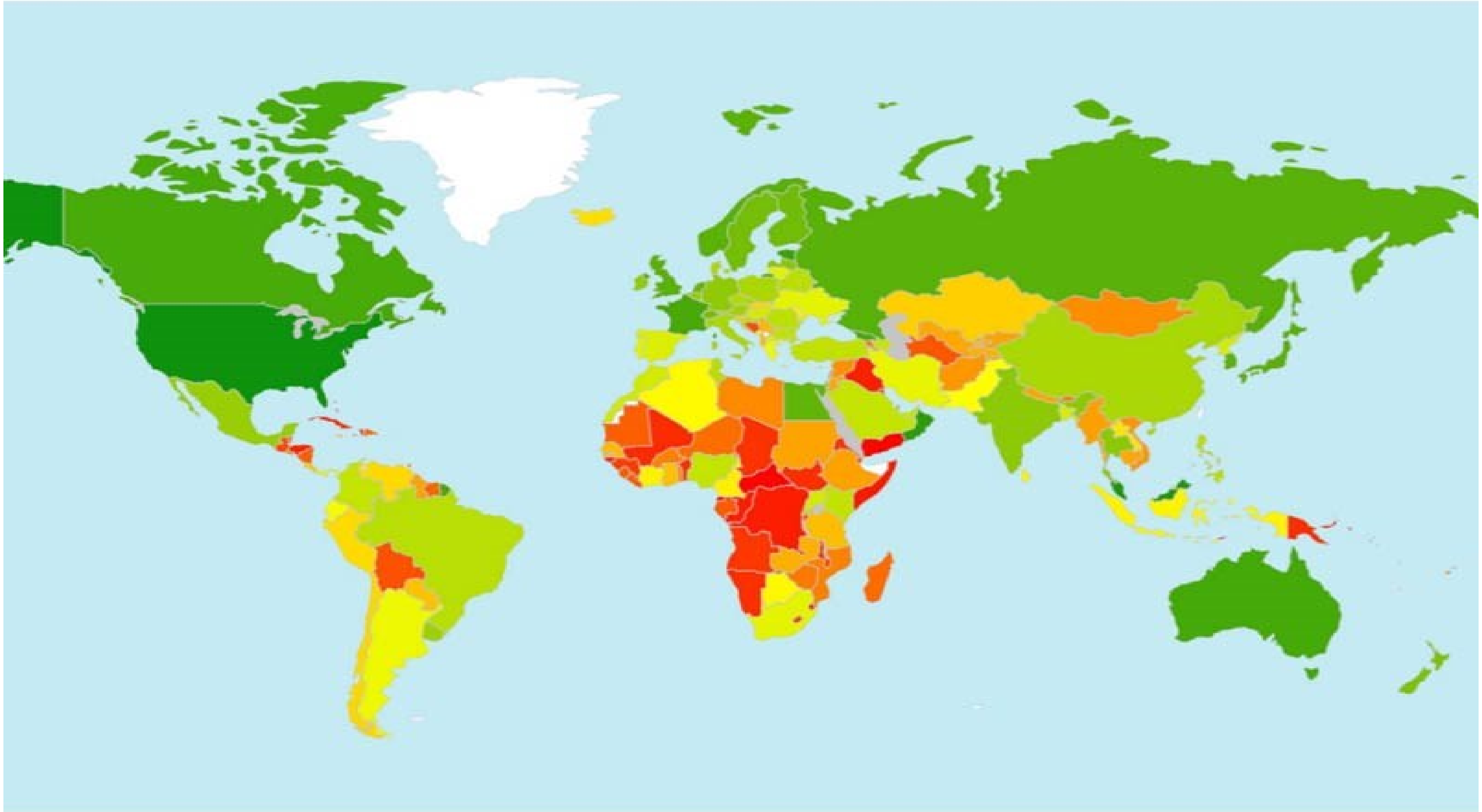
Eurobarometer on Cybersecurity

Information Security Indicators ETSI

The Global Cybersecurity Index (developed by ITU-ABIresearch)

Legal	• Existence of **legal institutions and frameworks** dealing with cybersecurity and cybercrime
Technical	• Existence of **technical institutions and frameworks** dealing with cybersecurity
Organizational	• Existence of **policy coordination institutions and strategies** for cybersecurity development at the national level
Capacity building	• Existence of **R&D, education and training programmes; certified professionals and public sector agencies fostering capacity building**
Cooperation	• Existence of **partnerships, cooperative frameworks and information sharing networks.**

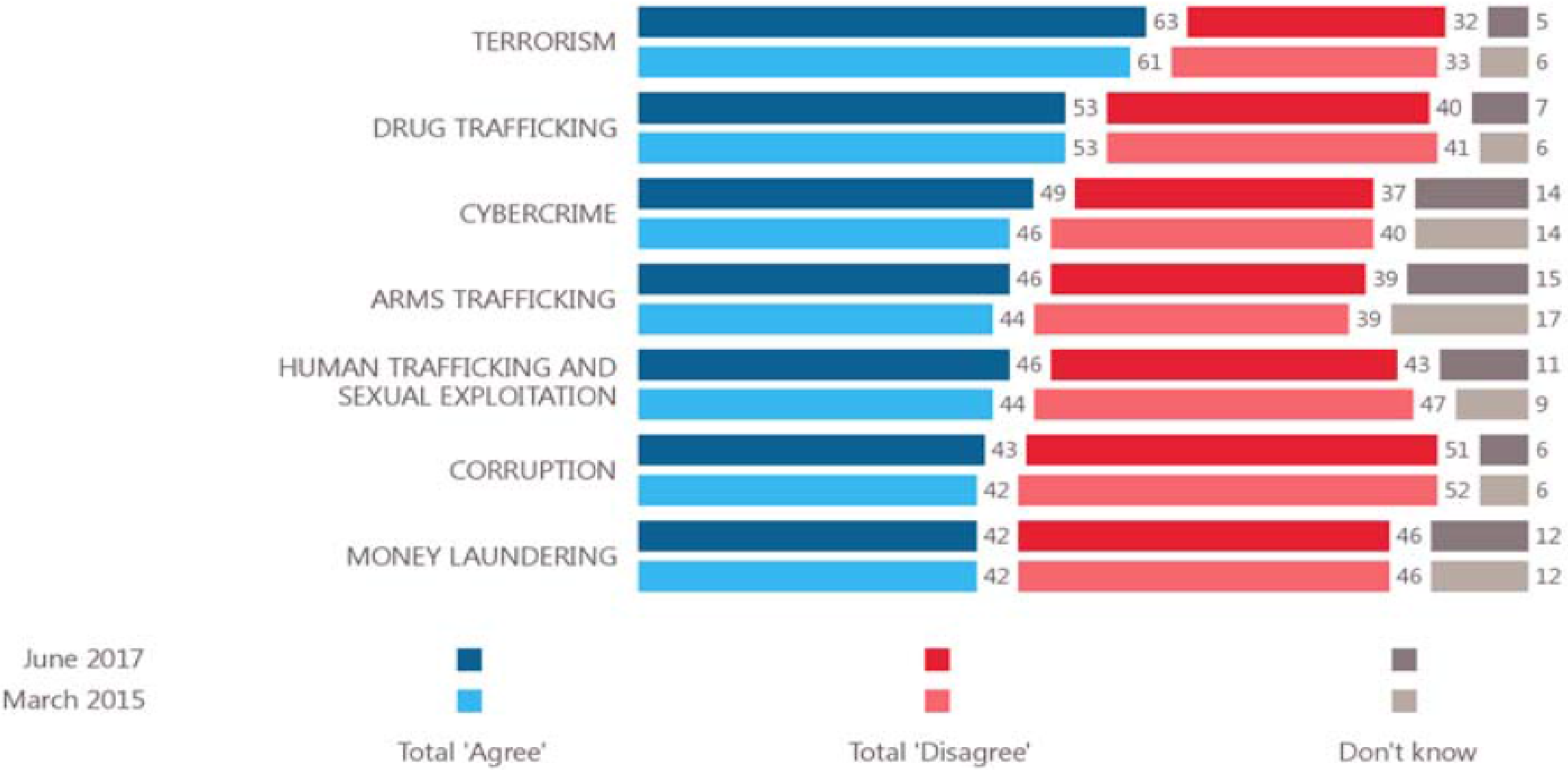
The Global Cybersecurity Index (developed by ITU-ABIresearch)



Special Eurobarometer 464a

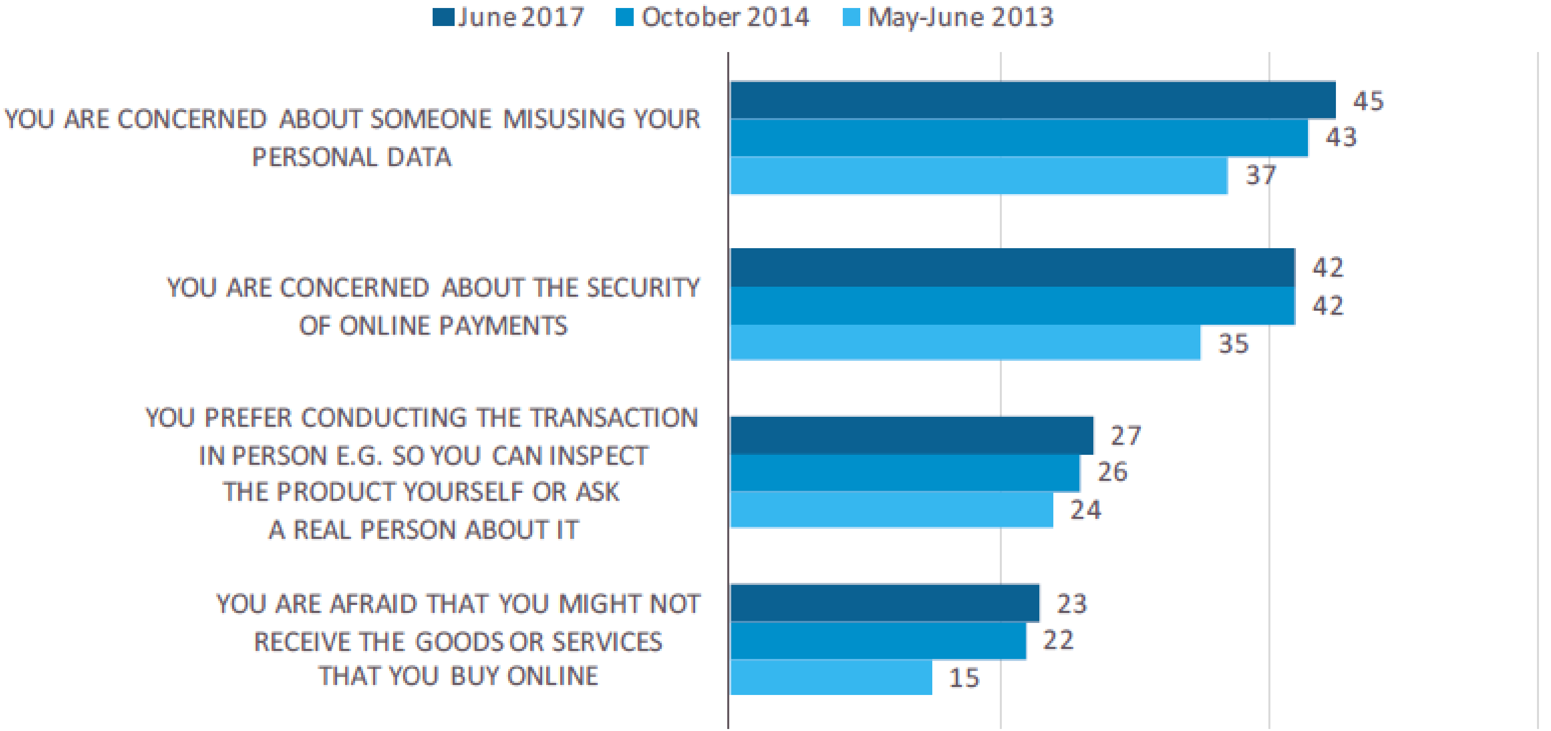
QB3 To what extent do you agree or disagree with the following statements: The police and other law enforcement authorities in (OUR COUNTRY) are doing enough to fight...

(% - EU)



Special Eurobarometer 464a

QB8 What concerns do you have, if any, about using the Internet for things like online banking or buying things online?
(MULTIPLE ANSWERS POSSIBLE)
(% - EU)



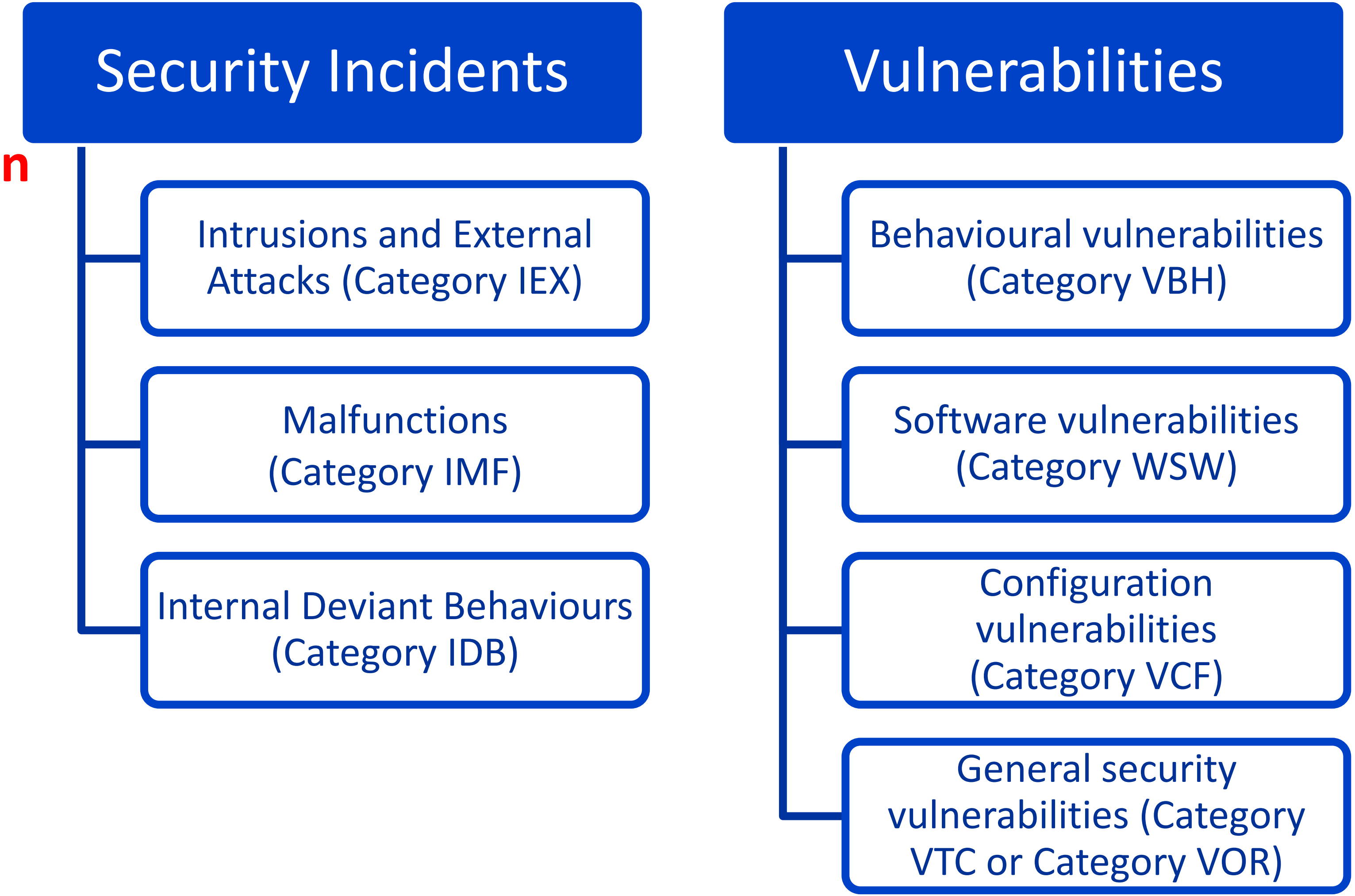
Organizations cybersecurity indicators

- From Qualitative to Quantitative Indicators
  - Assess the level of assurance
  - Measure the effectiveness of cybersecurity investments and performance
  - Benchmark the effectiveness of security measure
- The emergence of commonly recognized and reliable statistics.

ETSI Information Security Indicators

- □ ISI 001 Part 1: « A full set of operational indicators for organizations to use to benchmark their security posture »
- □ ISI 001 Part 2 : « Guide to select operational indicators based on the full set given in part 1 ».
- □ ISI 002: A security event classification model and taxonomy
- □ ISI 003 : A set of Key Performance Security Indicators (KPSI) for security event detection
- □ ISI 004 : Guidelines for event detection implementation
- □ ISI 005 : Guidelines for the testing of security event detection capabilities

ETSI Information System Indicators



Security Incidents

- Intrusions and External Attacks (Category IEX)
- Malfunctions (Category IMF)
- Internal Deviant Behaviours (Category IDB)

Vulnerabilities

- Behavioural vulnerabilities (Category VBH)
- Software vulnerabilities (Category WSW)
- Configuration vulnerabilities (Category VCF)
- General security vulnerabilities (Category VTC or Category VOR)

Examples of Vunerabilities Indicators

- **Not patched vulnerabilities VOR_VNP.2: Rate of not patched systems**
  - Not patched systems to be taken into account are the ones which are **not patched beyond the time limit defined in security policy.**
- **Passwords illicitly handled or managed VBH_PSW.1: Weak passwords used**
  - The required strength of passwords depends on the organization's security policy, but usable general recommendations in ISO/IEC 27002.
- **Workstation used without relevant usual security VBH_WTI.1:**
  - The use of workstation with a disabled or lacking update AV and/or FW.

Examples of Security Incidents Indicators

- **Denial of Service IEX_DOS.1: Denial of service attacks on websites**
  - Detection of an attack on a given website **coming from the same origin within a limited continuous timeframe**, and a significant incident defined as a user **noticeable disturbance and performance drop in the website access**
- **Malware IEX_MLW.1: Attempts to install malware on workstations**
  - Detection of a malware on workstations by organization's Antivirus and IPS
- **Phishing IEX_PHI.1: Phishing targeting company's customers' workstations spoiling company's image or business**
  - Customer reporting of a phishing attempt.

Thank you for your attention