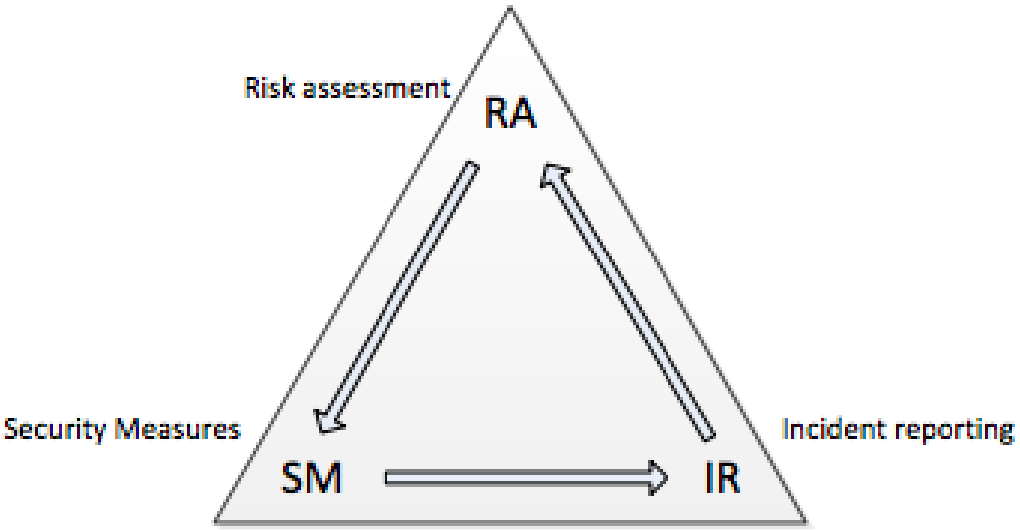
THE EU CYBERSECURITY AGENCY

TRUST SERVICES SECURITY INCIDENTS 2018

Eleni Vytogianni

24 | 9 | 2019

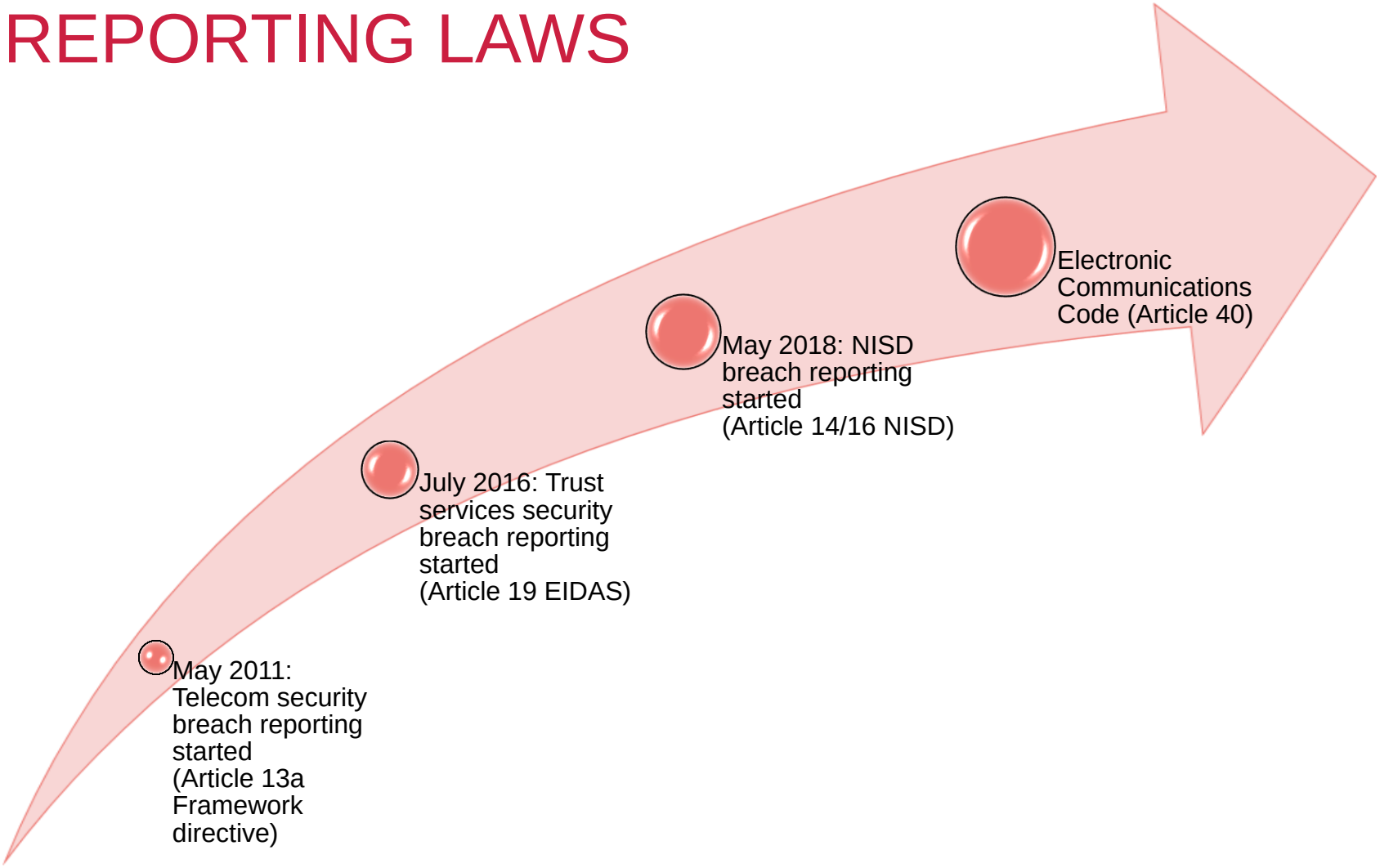
GENERAL SUPERVISION MODEL



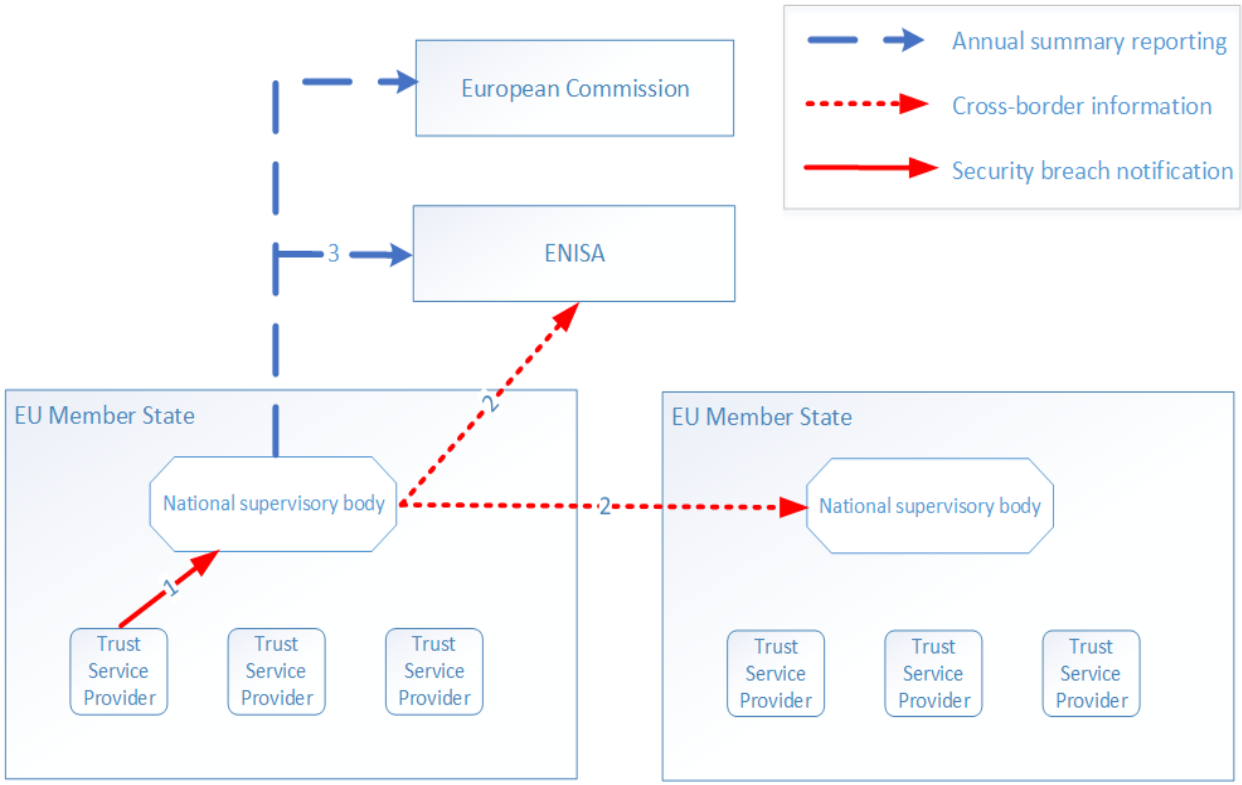
Market operators/providers assess security risks, take appropriate measures, and notify if things go wrong.

This triangle is supervised nationally by competent authorities and is present in Article 13a (telecom), Article 19 (EIDAS), Article 14 and 16 (NISD).

TIMELINE: EU SECURITY BREACH REPORTING LAWS



EU BREACH REPORTING



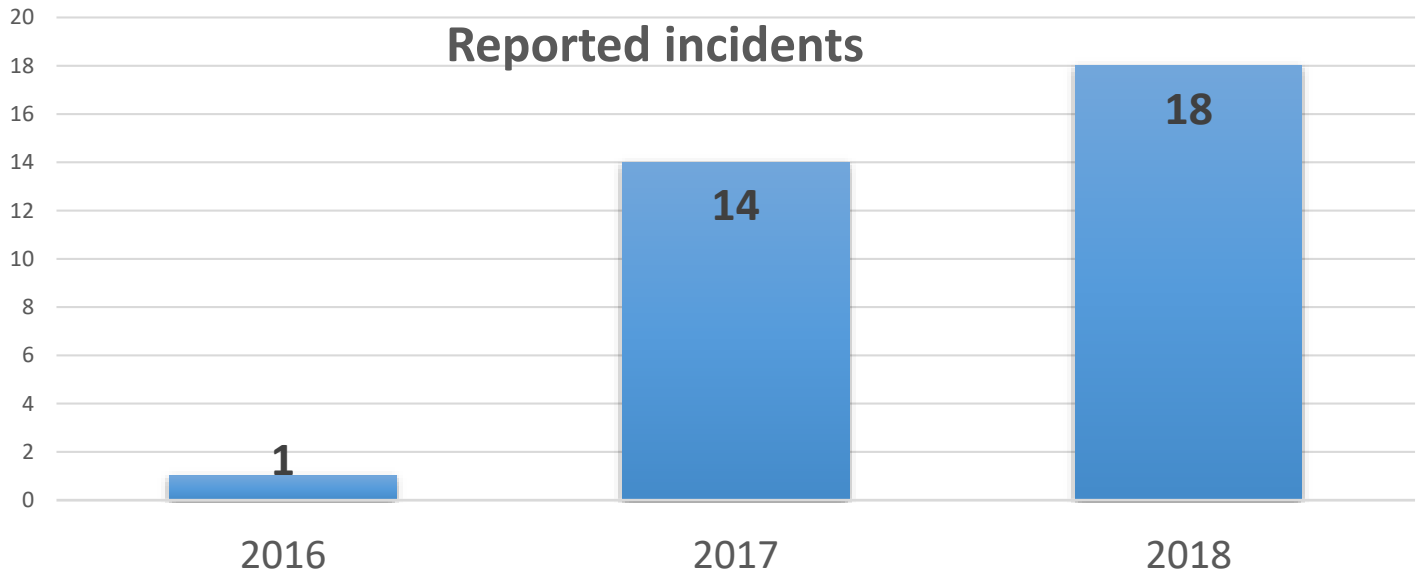
*) Mandatory security breach reporting is a cornerstone of security supervision.
The same general setup is present in Article 13a (telecoms), Article 19 (EIDAS), Article 14 and 16 (NISD).

BENEFITS OF INCIDENT REPORTING

- Important supervision mechanism for national authorities
  - No longer relying only on the news or customer complaints
- Input (root causes, trends) for appropriate policy decisions (e.g. guidelines)
  - Frequent and systemic issues can be followed up on
- Bilateral collaboration in case of cross-border incidents
- Statistics about security incidents (see next slides)
  - Basis to study on root causes and trends

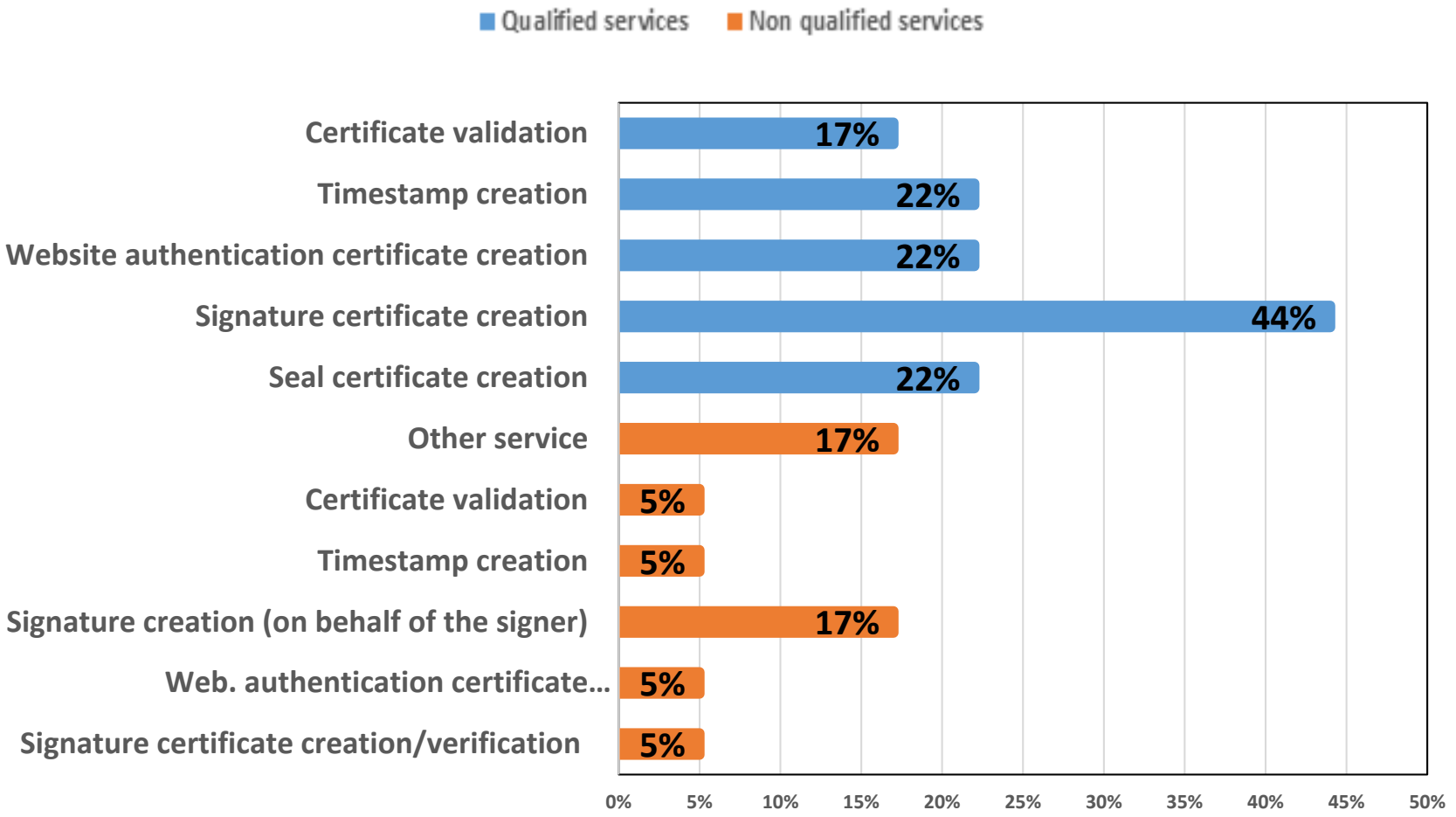
2018 REPORTING IN NUMBERS

- 29 countries submitted Annual Reports – 18 incidents reported in total



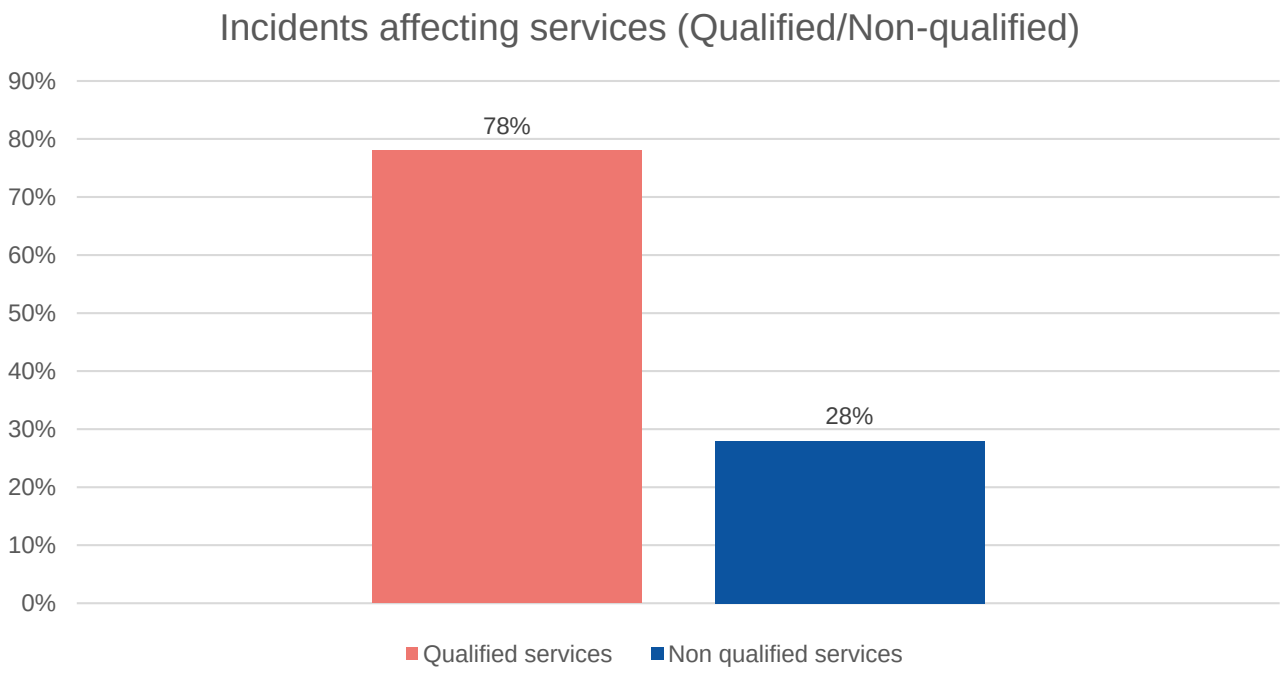
=> Notification slightly increase

KEY STATISTICS: SERVICES AFFECTED



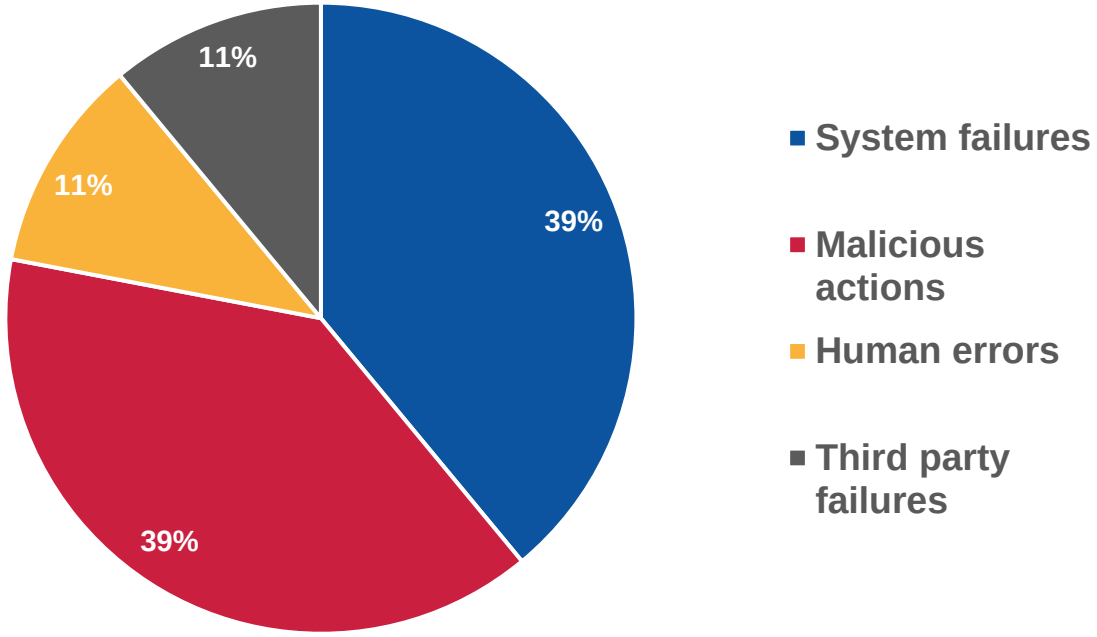
Creation of Qualified signature certificates the most affected service

KEY STATISTICS: SERVICES AFFECTED



KEY STATISTICS: ROOT CAUSES

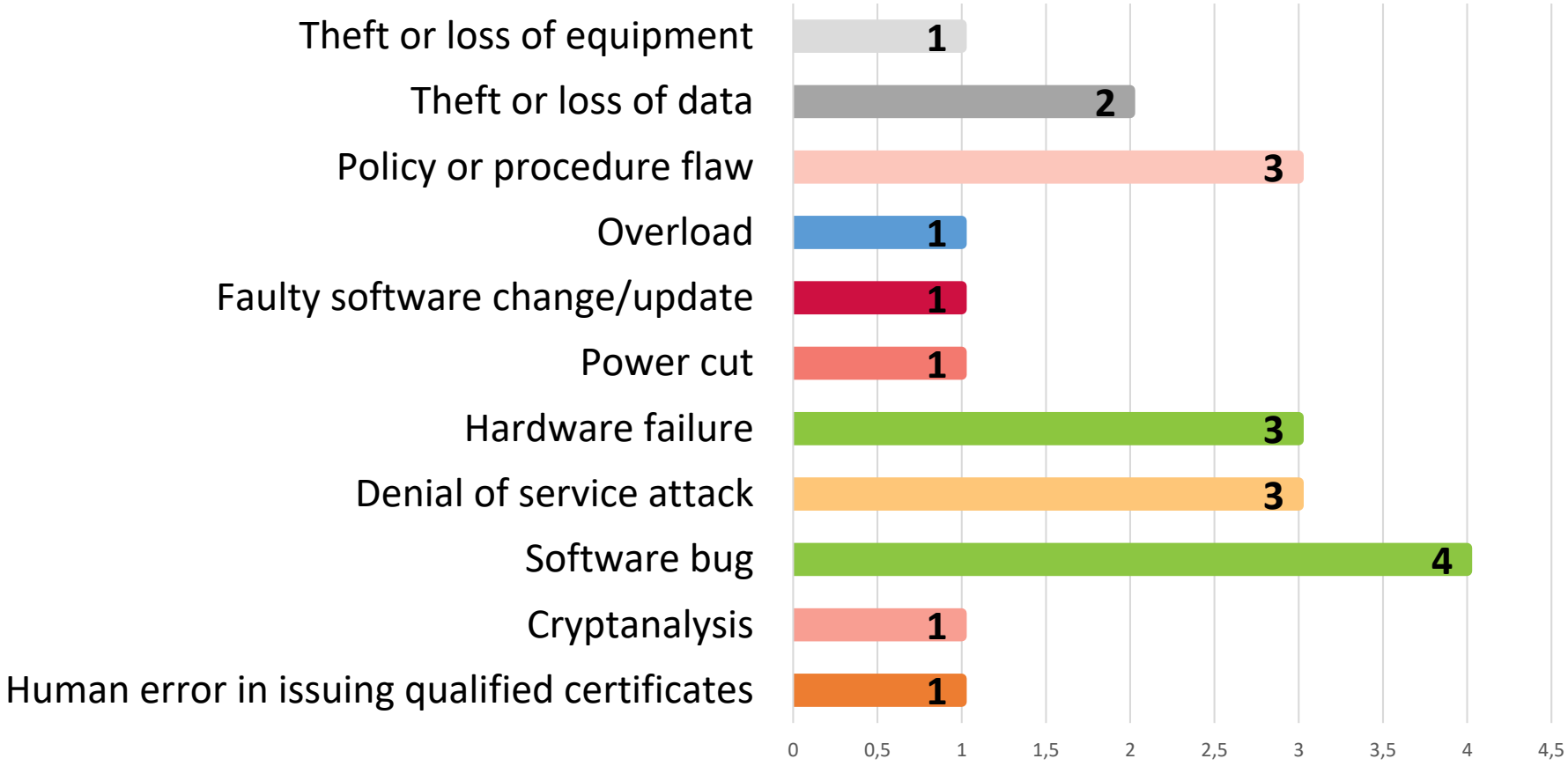
Root causes of trust services security incidents - 2018



Most common root causes:

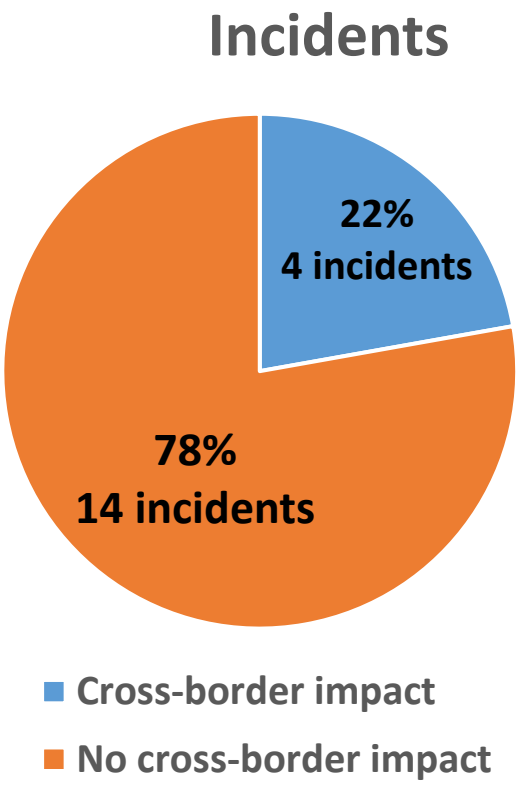
- ***system failures (7 incidents, 39% of the total)***
- ***malicious actions (7 incidents, 39% of the total) have been trending up rapidly since last year (7% of the total in 2017).***

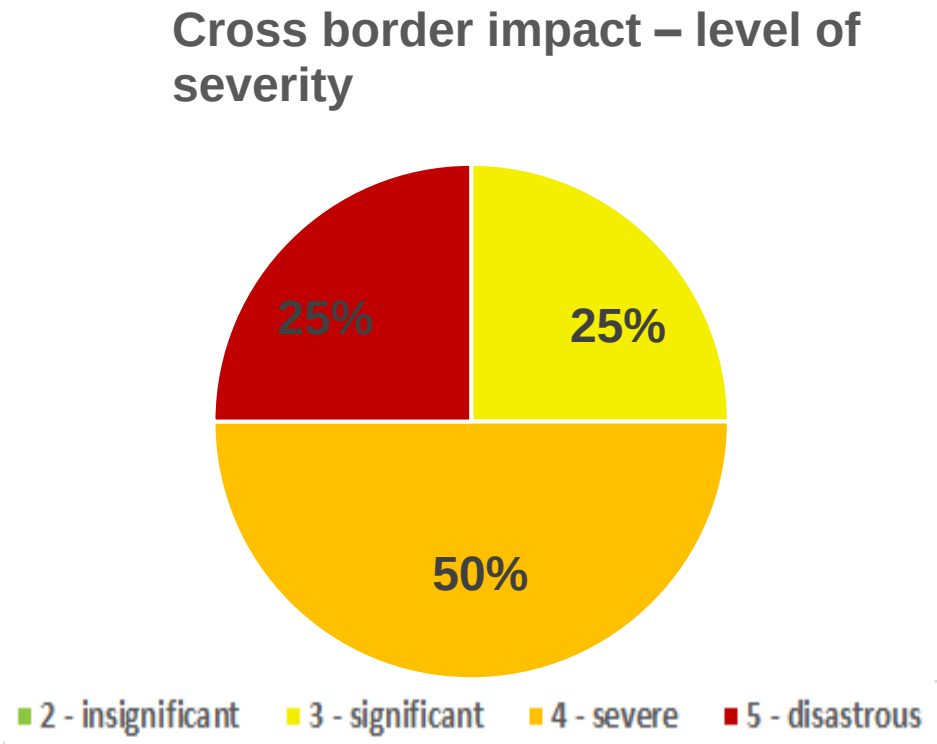
KEY STATISTICS: DETAILED CAUSES



=> Top four detailed causes: Software bugs, Hardware failures, DDoS attacks and policy/procedure flaws

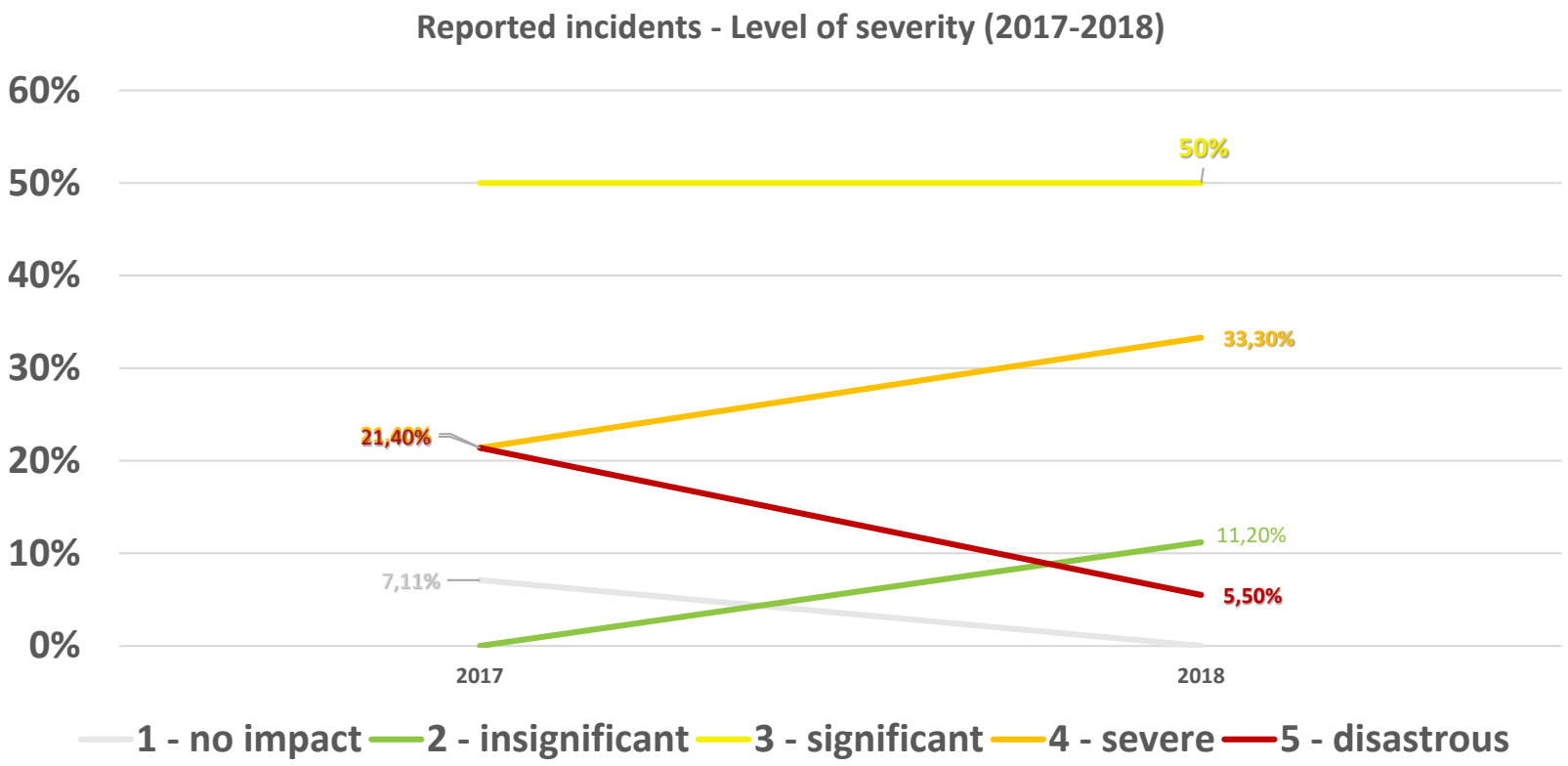
CROSS BORDER IMPACT





=> A few but critical security breaches with cross border impact

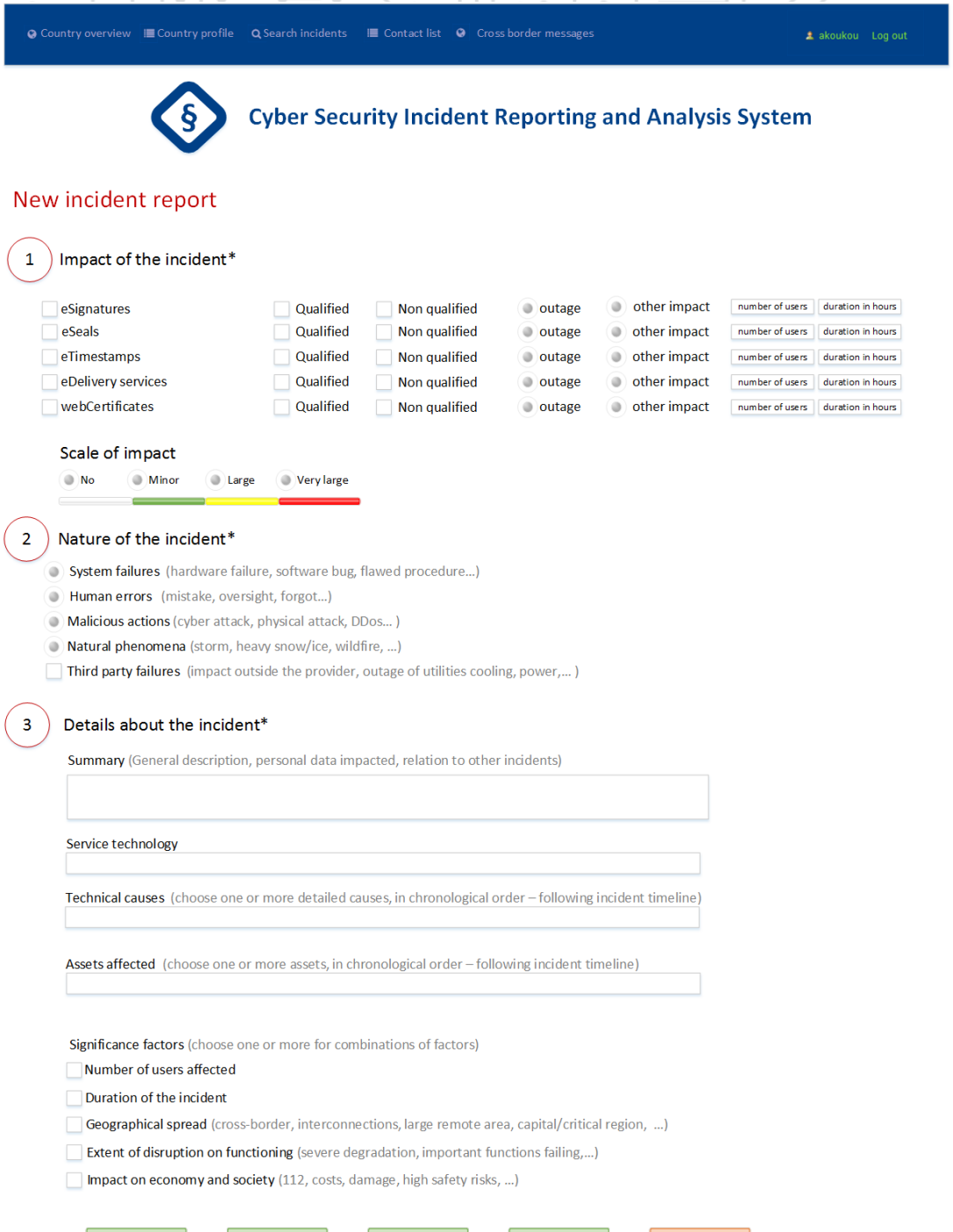
REPORTED INCIDENTS 2017-2018 LEVEL OF SEVERITY



eIDAS INCIDENT REPORTING FRAMEWORK

- ENISA Guidelines “Incident reporting framework for eIDAS art. 19” in cooperation with art. 19 Expert Group
  Thresholds: two approaches were used
  - Scenarios/examples of security incidents in the context of eIDAS article 19
  - Assets assigned impact values according to the eIDAS services

  Article 19 EG preference was the first one, however both are included in CIRAS-T
- CIRAS Tool (redesigned)


Country overview
Country profile
Search incidents
Contact list
Cross border messages
akoukou
Log out
Cyber Security Incident Reporting and Analysis System
New incident report
1
Impact of the incident*
eSignatures
eSeals
eTimestamps
eDelivery services
webCertificates
Qualified
Non qualified
outage
other impact
number of users
duration in hours
Scale of impact
No
Minor
Large
Very large
2
Nature of the incident*
System failures (hardware failure, software bug, flawed procedure...)
Human errors (mistake, oversight, forgot...)
Malicious actions (cyber attack, physical attack, DDos...)
Natural phenomena (storm, heavy snow/ice, wildfire, ...)
Third party failures (impact outside the provider, outage of utilities cooling, power,...)
3
Details about the incident*
Summary (General description, personal data impacted, relation to other incidents)
Service technology
Technical causes (choose one or more detailed causes, in chronological order – following incident timeline)
Assets affected (choose one or more assets, in chronological order – following incident timeline)
Significance factors (choose one or more for combinations of factors)
Number of users affected
Duration of the incident
Geographical spread (cross-border, interconnections, large remote area, capital/critical region, ...)
Extent of disruption on functioning (severe degradation, important functions failing,...)
Impact on economy and society (112, costs, damage, high safety risks, ...)

ENISA INCIDENT REPORTING PAPERS

Annual Report Trust Services Security Incidents 2018

https://www.enisa.europa.eu/publications/trust-services-security-incidents-2018

Article 19 Incident reporting framework

https://www.enisa.europa.eu/publications/article19-incident-reporting-framework

THANK YOU FOR YOUR ATTENTION

Vasilissis Sofias Str 1, Maroussi 151 24,
Attiki, Greece

+30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europa.eu