

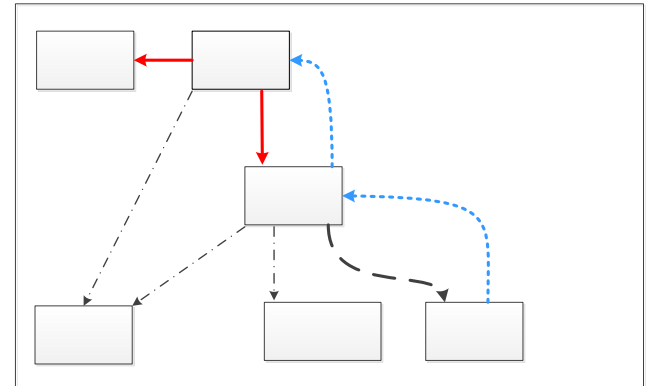


ENISA working on Article 19

Dr. Marnix Dekker

Dr. Kostas Moulinos

Security expert, Information security officer
ENISA



**REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 23 July 2014**

**on electronic identification and trust services for electronic transactions in the internal market and
repealing Directive 1999/93/EC**


THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee ⁽¹⁾,

A close-up photograph of a field of dark purple tulips. The flowers are in various stages of bloom, with some fully open and others as buds. The background is a soft-focus green, suggesting other tulips and foliage. Overlaid on the center of the image is white text.

Let's go back to summer 2011
Diginotar (operation black tulip)

Background: HTTPS is not working

- Public key crypto is great! But PKI is poor.
- Most widely used instance of PKI (HTTPS) is neither user-friendly nor secure (600 single points of failure) nor privacy-friendly (CAs track internet usage).
- Want to guess at the scale of exploitation?
 - Matt Blaze <http://www.crypto.com/blog/spycerts>: “large number of root authorities, from tiny, obscure businesses to national governments”
 - Moxie Marlinspike: “Do you even need to hack?”



A world map with a black background and white outlines of continents and countries. The landmasses are filled with a dark blue color. Two regions are highlighted in a bright red color: Iran in the Middle East and a cluster of countries in Western Europe, including the United Kingdom, France, Germany, and the Benelux region. The text "MITM on 300.000 Iranians" is overlaid in white on the map.

MITM on 300.000 Iranians

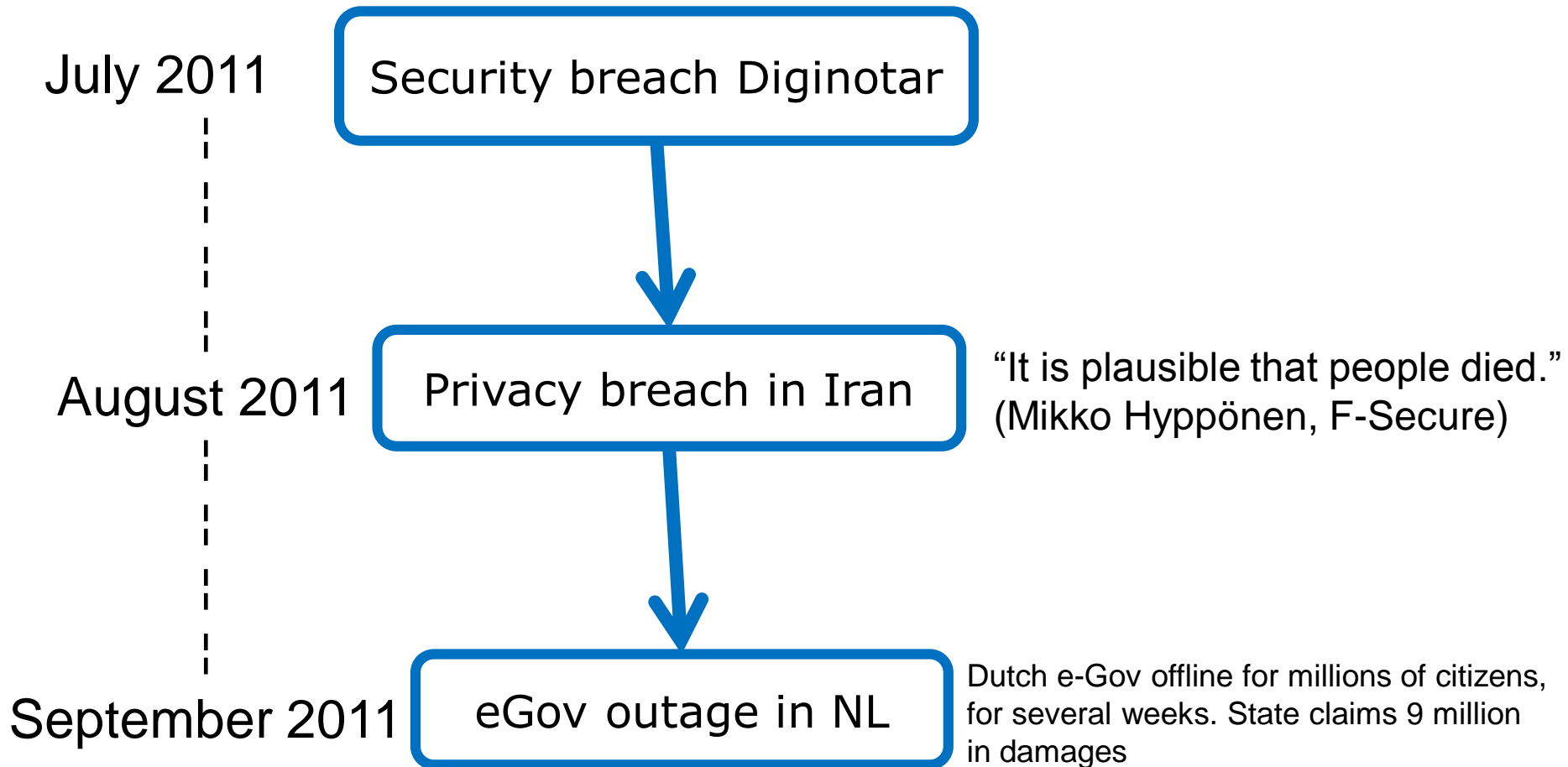
For several weeks in August 2011

Dutch e-Government offline

For several weeks in September 2011



Operation Black tulip – impact timeline



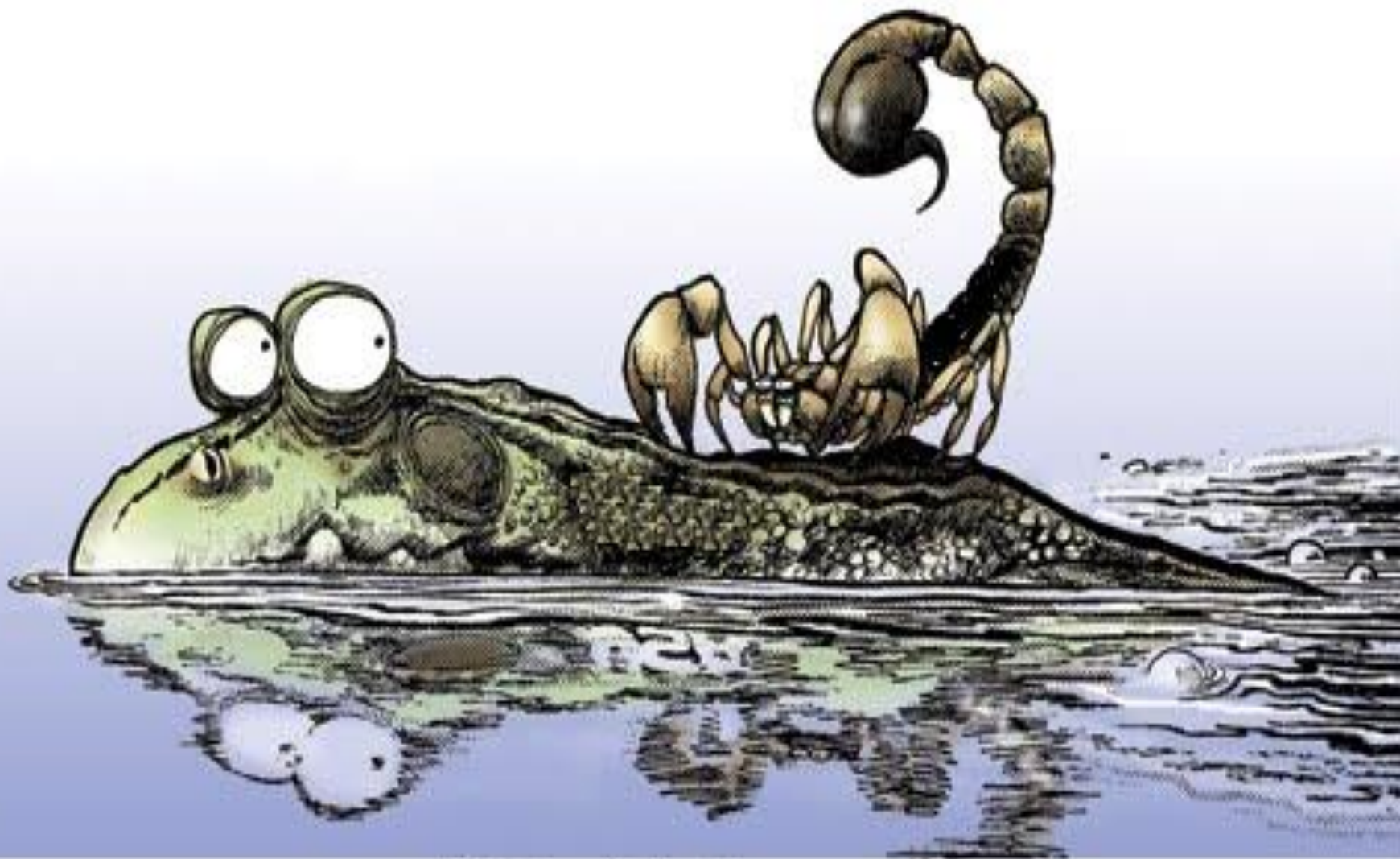
... after the incident response?



After the Diginotar incident

- **CERT network worked well** -- i.e. response phase
- Aart Jochem (NCSC): "But **PKI crisis** is still ongoing".
- EU-wide market issue and a global issue
- Technical discussions
 - Google removes OCSP from Chrome (snapping seatbelt)
 - Discussion about PKI, ENISA criticises HTTPS and CAs
 - "*Security economics in the HTTPS value chain*"
- Political discussions
 - No incident notification/reporting obligations for Diginotar
 - Weak legal grounds for the government to intervene
 - Breach at a small firm had severe impact abroad.
- Political push for **NIS legislation**
 - Extend **Article 13a** to CA's eTrust providers: **Art19, EIDAS**
 - Extend other to critical ICT: Art14, NIS directive proposal

... our customers



The Frog & The Scorpion.

ENISA's work on Article 19 of eIDAS

- Article 19 obliges qualified and non-qualified trust service providers (CA's typically) to
 - assess risks,
 - take appropriate measures
 - notify and report about security breaches



- Supervised by a national authority (regulator, DPA, etc.)
in collaboration with regulators abroad (single market)

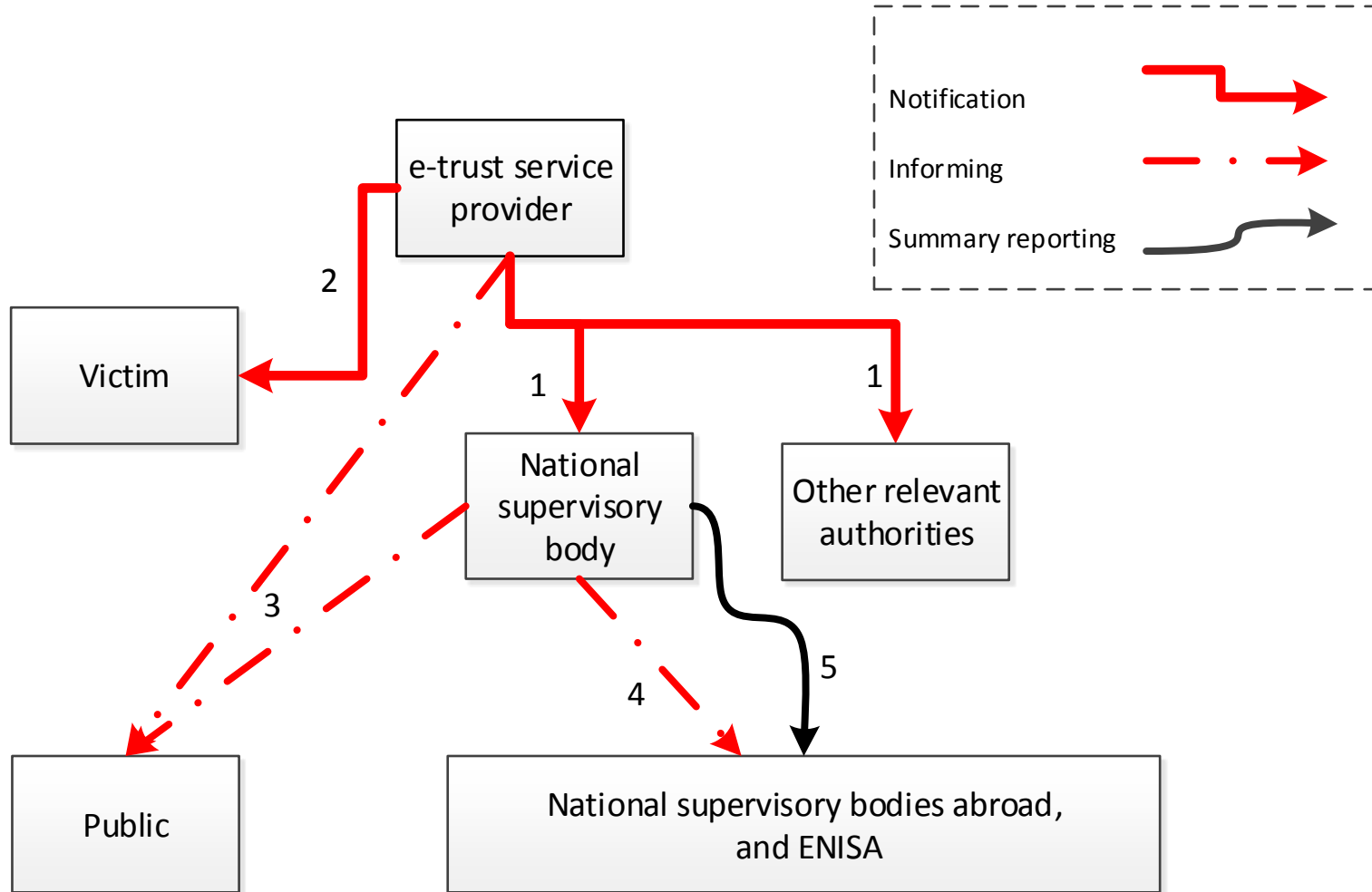


ENISA Article 19 Expert group

- Chaired by ENISA, composed of experts from authorities
 - ENISA liaises with industry (such as CAB forum, TSP forum)
 - EC liaises with other legislation (such as NIS directive).
 - AT liaises with FESA
- Scope: Article 19 but focus: breach reporting (par 19.2)
 - Security practices (par 19.1) relevant, point/refer to them.
- 3 meetings per year, in different EU+EFTA countries
- First meeting on the 17th of November 2014.
 - 25 experts from ministries and agencies from 15 different countries (EU + EFTA).
- Second meeting on the 12th of February,
 - 22 experts from ministries and agencies from 15 countries (EU + EFTA)



Incident reporting in Article 19





Article 13a: Thresholds for annual summary reporting

- NRAs are calibrating their national thresholds.
 - What is significant impact differs per country.
- One EU-wide threshold for reporting to EC and ENISA.
 - Baseline + whatever else is 'interesting'
- Recent threshold change
 - V2.1 => relative threshold + absolute threshold
 - Relative threshold (see picture)
 - Absolute threshold (1M user-hours)

	1h-2h	2h-4h	4h-6h	6h-8h	>8h
1% - 2%	Green	Green	Green	Green	Red
2% - 5%	Green	Green	Green	Red	Red
5% - 10%	Green	Green	Red	Red	Red
10% - 15%	Green	Red	Red	Red	Red
> 15%	Red	Red	Red	Red	Red



Article 13a: CIRAS – Online reporting tool for NRAs

- CIRAS: Cyber Incident Reporting and Analysis System
- Main functions for NRAs
 - pan-EU annual summary reporting
 - pan-EU ad-hoc cross-border notifications
 - archive, searching, analysis of (anonymized) incidents
- Supports ENISA annual report

Countries

Country	Incident reports	Annual reports	Empty report
view Green Europe	5	0	0
view Legoland	3	1	0
view Pavland	4	1	0
view Crymogaea	3	0	0
view Wadiya	2	1	0
view Laputa	2	0	0
view Atlantis	3	1	0

Annual Reports

Year	Submission date	Contained incident reports	Export to
<input type="checkbox"/> 2012	08-01-2013 17:13:53	452250, 612291	XML CSV HTML

[Send 2013 empty annual report](#) [Unsubmit report](#)

Incident reports

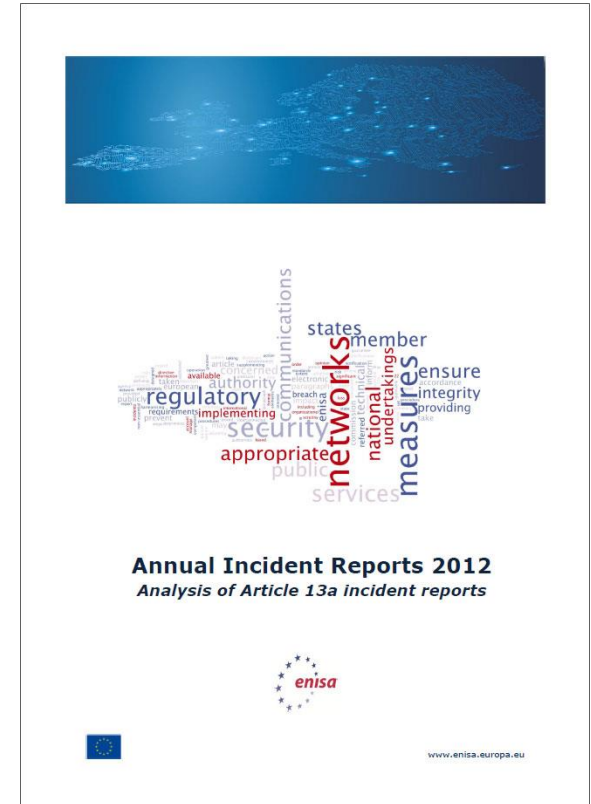
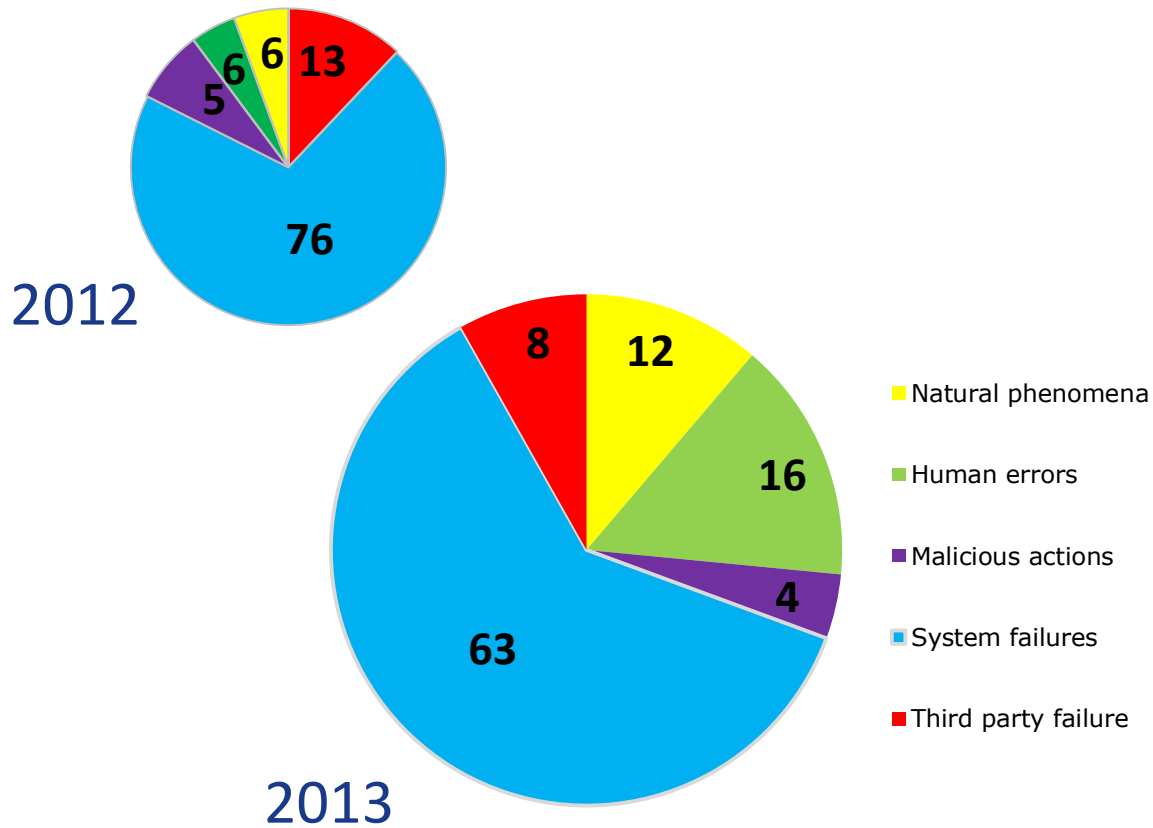
Incident ID	Year	National ID	Impact	Date added	Date modified	
2013						
<input type="checkbox"/> 199374	2013	-	Mobile telephony(23h, 150000) satellite tv(10h, 13140)	14-01-2013 14:08:46	22-01-2013 17:19:01	view edit delete
2012						
<input type="checkbox"/> 452250	2012	-	Mobile telephony(3h, 50000)	08-01-2013 16:53:45	08-01-2013 16:53:46	view edit delete
<input type="checkbox"/> 612291	2012	-	Fixed telephony(1h, 800)	27-12-2012 15:52:31	08-01-2013 16:49:30	view edit delete

Incidents included in the 2012 annual report can not be edited or deleted.



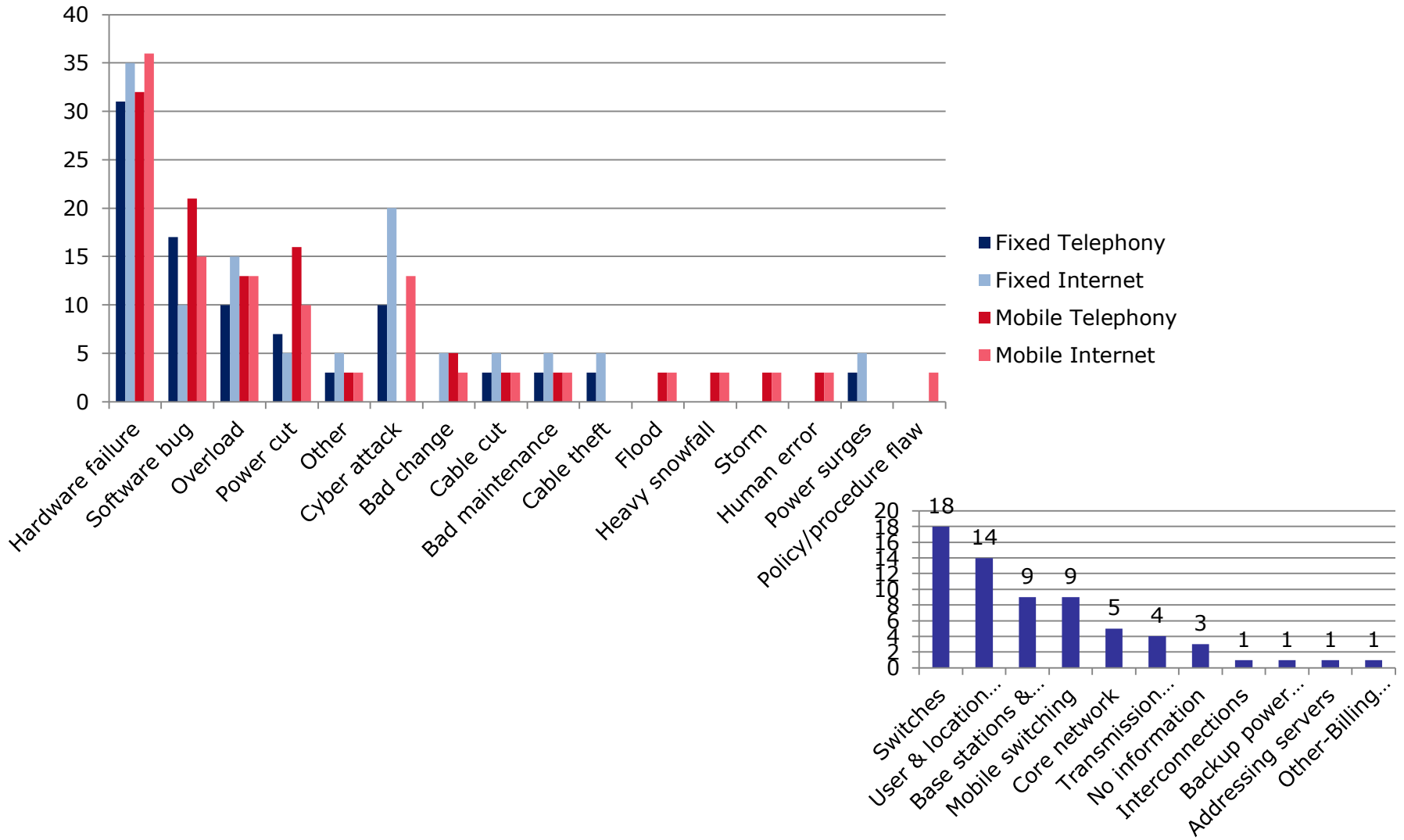
Article 13a: Annual EU wide security breach reports

- Annual reports about large outages in EU's telecoms



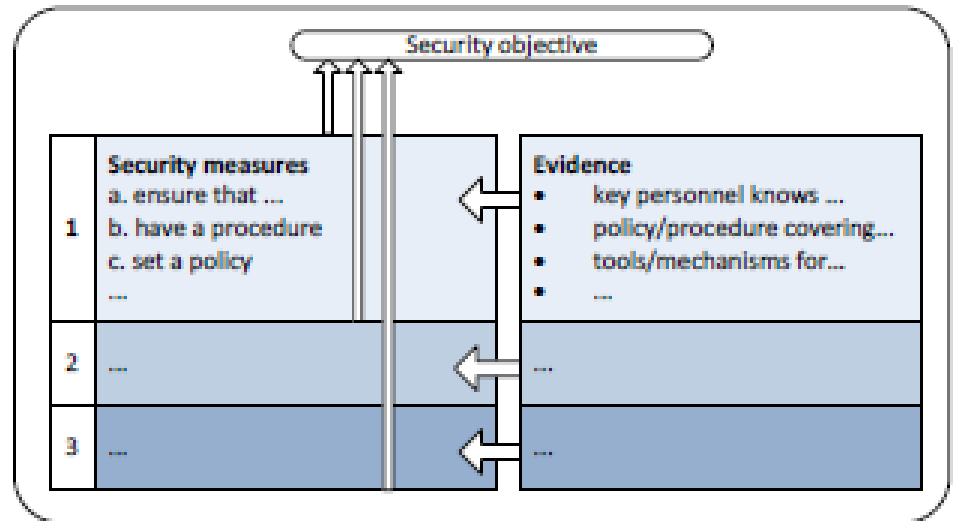
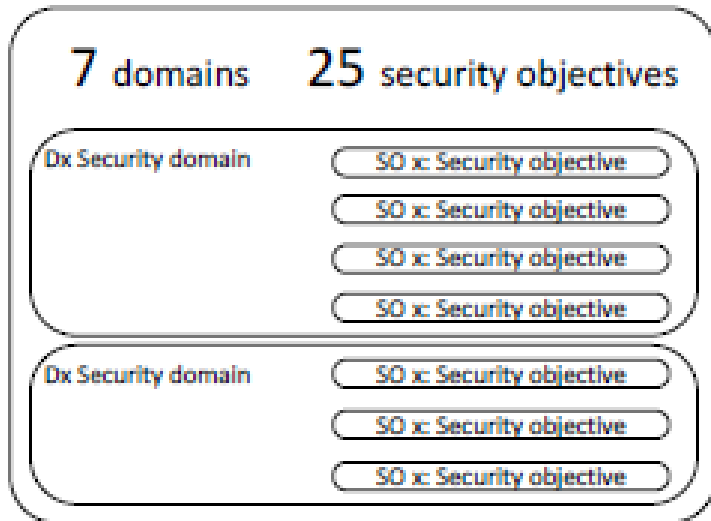
More information on <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting>

Article 13a: EU wide view on major outages



Tool for supervising security measures

- Standard neutral, technology neutral,
- No **a security how-to**, but a structure for supervision
- Adopted by many telecom regulators across the EU
- Provides basis for interviews, audits, questionnaires, nation wide benchmarking, guidance, etc.



Article 13a Security measures

D1: Governance and risk management

The domain “Governance and risk management” includes the security objectives related to governance and management of network and information security risks.

SO 1: Information security policy

Establish and maintain an appropriate information security policy.

	Security measures	Evidence
1	a) Set a high level security policy addressing the security and continuity of the communication networks and/or services provided. b) Make key personnel aware of the security policy.	<ul style="list-style-type: none"> • Documented security policy, including networks and services in scope, critical assets supporting them, and the security objectives. • Key personnel are aware of the security policy and its objectives (interview).
2	c) Set detailed information security policies for critical assets and business processes. d) Make all personnel aware of the security policy and what it implies for their work. e) Review the security policy following incidents.	<ul style="list-style-type: none"> • Documented information security policies, approved by management, including applicable law and regulations, accessible to personnel. • Personnel are aware of the information security policy and what it implies for their work (interview). • Review comments or change logs for the policy.
3	f) Review the information security policies periodically, and take into account violations, exceptions, past incidents, past tests/exercises, and incidents affecting other (similar) providers in the sector.	<ul style="list-style-type: none"> • Information security policies are up to date and approved by senior management. • Logs of policy exceptions, approved by the relevant roles. • Documentation of review process, taking into account changes and past incidents.

One size does not fit all

sophistication levels would yield a profile of a provider, allowing for a quick comparison between providers across the sector.

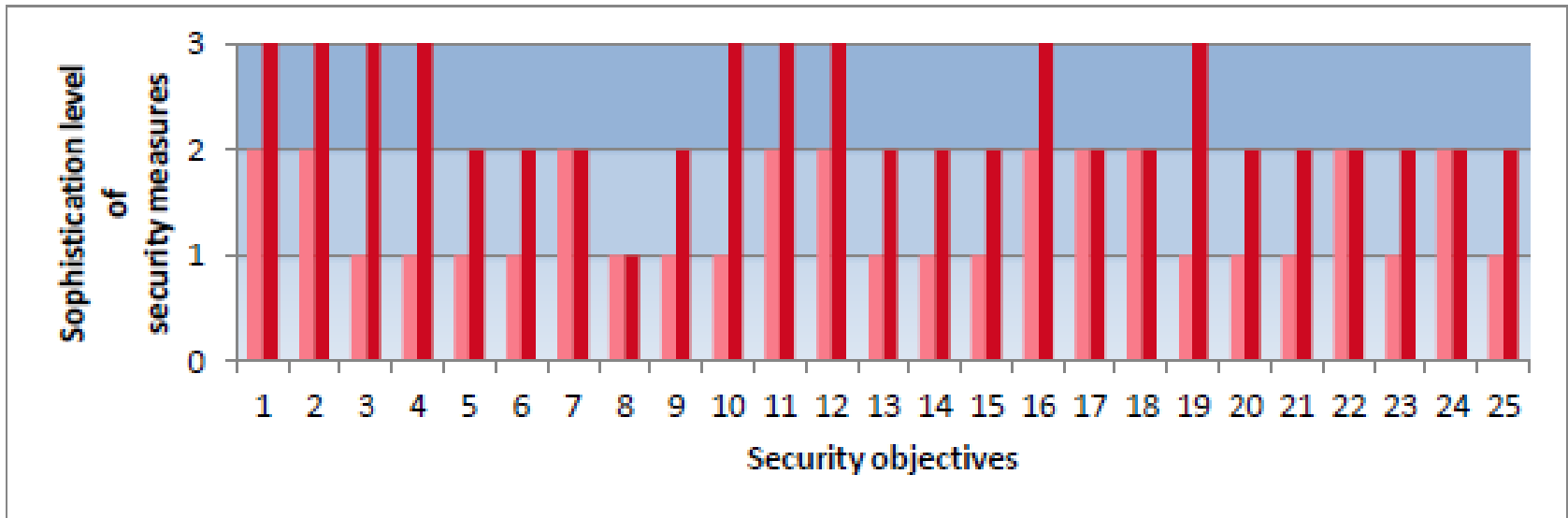


Figure 2: Two different profiles with different sophistication of measures for each security objective.

In figure 2 we show two example profiles in one diagram. The vertical axis spans the sophistication levels and the horizontal axis spans the security objectives. Dark red indicates a provider with more



A bit like curling



Challenge: Patchwork of legislation

Member states shall implement the obligation to notify security incidents in a way that minimises the administrative burden in case the security incident is also a personal data breach

Liaising with the competent authorities and the data protection authorities, ENISA could assist by developing information exchange mechanisms and templates avoiding the need for two notification templates. This single notification template would facilitate the reporting of incidents compromising personal data thereby easing the administrative burden on businesses and public administrations.

-> tired frog ... and two scorpions

Challenges: Sharing without scaring?

- Leverage incident reporting to increase knowledge and transparency
 - “Heavy fines and a lot of bureaucracy for every single breach!! That will teach them!!”
 - How to incentivize reporting?
 - Anonymity/immunity for reporters,
 - Fines/sanctions for not reporting –not for incidents,
 - Corporate culture, return value
 - Hotlines?
 - How to incentivize proactive incident detection?
 - How to incentivize sharing of lessons learnt!
 - When to look beyond competition?
 - Only incidents or also risks?

Amendment 97
Proposal for a directive
Article 14 – paragraph 2

competent

2. Member States shall ensure that market operators notify *without undue delay* to the competent authority *or to the single point of contact* incidents having a significant impact on the *continuity* of the core services they provide. *Notification shall not expose the notifying party to increased liability.*



Vision/outlook for ENISA Article 19 group

- Q2 - Q3 Draft and finalize a 'proposal' for a security incident reporting framework
 - Mainly focused on the notification/reporting between MS and ENISA
- Q3-Q4 Draft and finalize an overview of relevant security guides for TSPs – target audience: authorities.
- Learning while doing – hard to define a-priori
- Informal meetings, informal collaboration, consensus-based technical guidelines
- No incident reporting graveyard
 - Efficient and effective, for national authorities and for private sector
- Understand and discuss specific security incidents and issues
 - Share stories, experiences with supervision, trends, threats, etc.
 - Do not define or discuss 'security' in general at a high level
- Promote and support the EU's digital market!!!





Contact us

Kostas Moulinos Konstantinos.Moulinos@enisa.europa.eu

Marnix Dekker marnix.dekker@enisa.europa.eu (leaving ENISA per mid March)

ENISA website: <http://www.enisa.europa.eu>

Follow ENISA's twitter @enisa_eu feed: https://twitter.com/enisa_eu

For more information see ENISA's website: <http://enisa.europa.eu>

Follow ENISA's twitter feed: [@enisa_eu](https://twitter.com/enisa_eu)

Follow ENISA:

