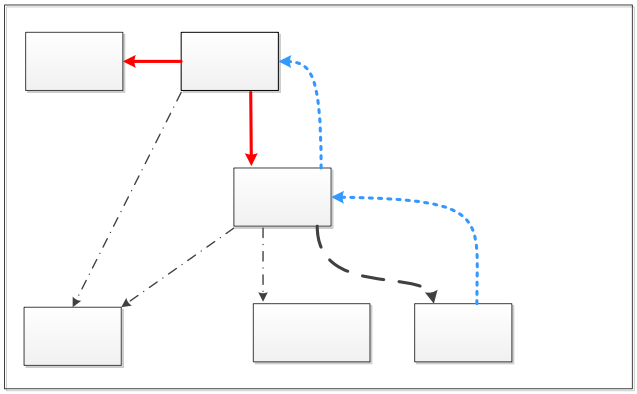
Cyber security incident reporting in the EU



Dr. Marnix Dekker
CIIP unit, ENISA

International Conference on Cyber Crisis Cooperation and Exercises
Athens, 24 September 2013

Incident response versus Incident reporting

Incident response

- Incident response teams
  - CISOs, IT dpts
  - Internal CERTs
  - National CERTs
  - Institutional CERTs
  - Vendor CERTs
  - Antivirus companies
  - Anyone who is around
  - Legal advisors ☺

- …like digital fire fighting

… beyond incident response?

Incident reporting

- Incident reporting
  - after the fact
  - total impact
  - root causes
  - actions taken
  - lessons learnt
- Share experiences with the rest of sector/other sectors
- Share experiences with other government bodies/abroad
- Exchange, discuss security measures and best practices
- Inform policy makers, the public and industry so they can assess the risks (i.e. frequency, impact)

Article 13a of the Telecom reform

Article 13a

Security and integrity

1. Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services. Having regard to the state of the art, these measures shall ensure a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of security incidents on users and interconnected networks.

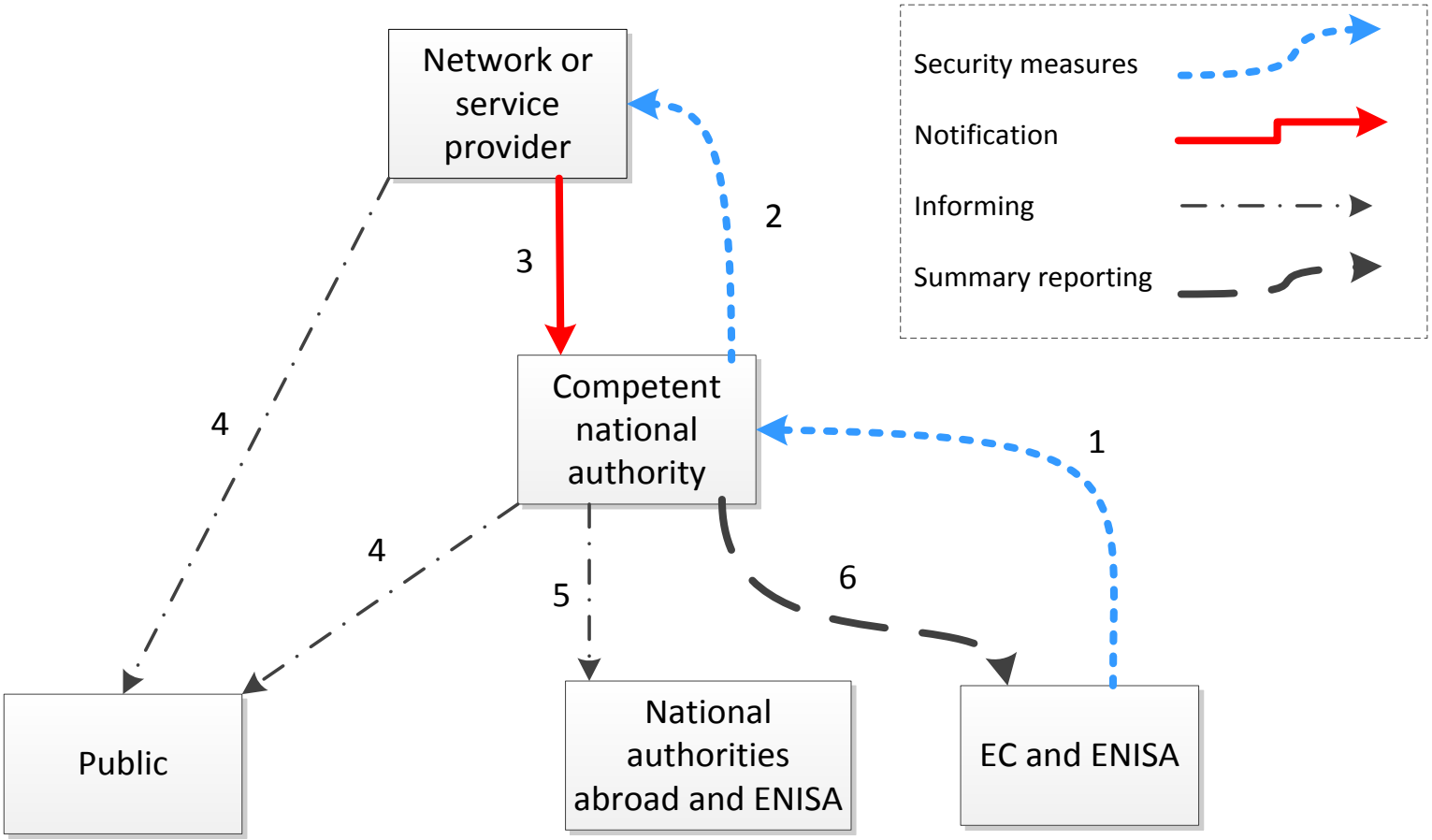
2. Member States shall ensure that undertakings providing public communications networks take all appropriate steps to guarantee the integrity of their networks, and thus ensure the continuity of supply of services provided over those networks.

3. Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services.

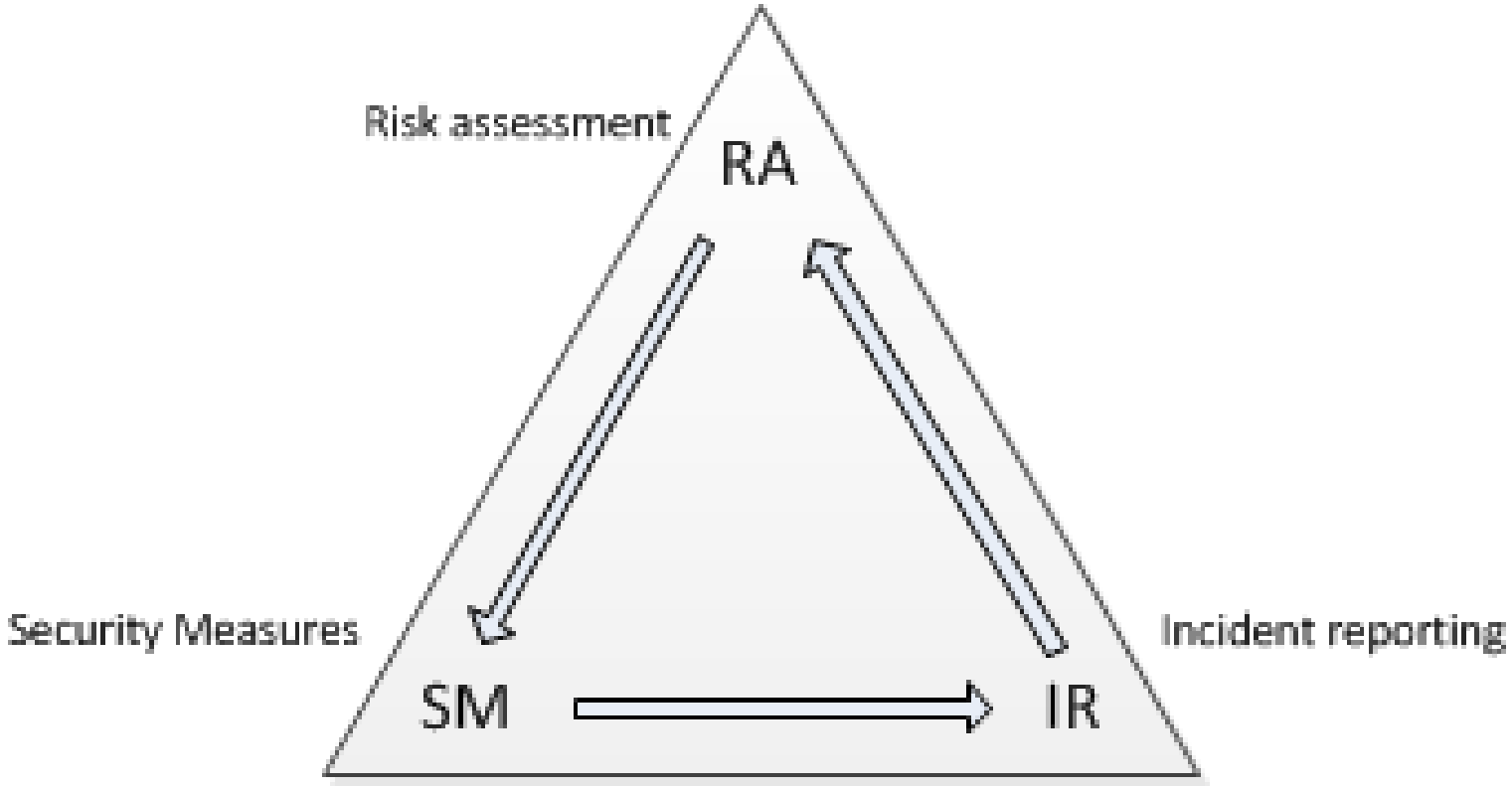
Where appropriate, the national regulatory authority concerned shall inform the national regulatory authorities in other Member States and the European Network and Information Security Agency (ENISA). The national regulatory authority concerned may inform the public or require the undertakings to do so, where it determines that disclosure of the breach is in the public interest.

Once a year, the national regulatory authority concerned shall submit a summary report to the Commission and ENISA on the notifications received and the action taken in accordance with this paragraph.

Information flows in Article 13a



Security processes in Article 13a



- Supervised by a national regulator

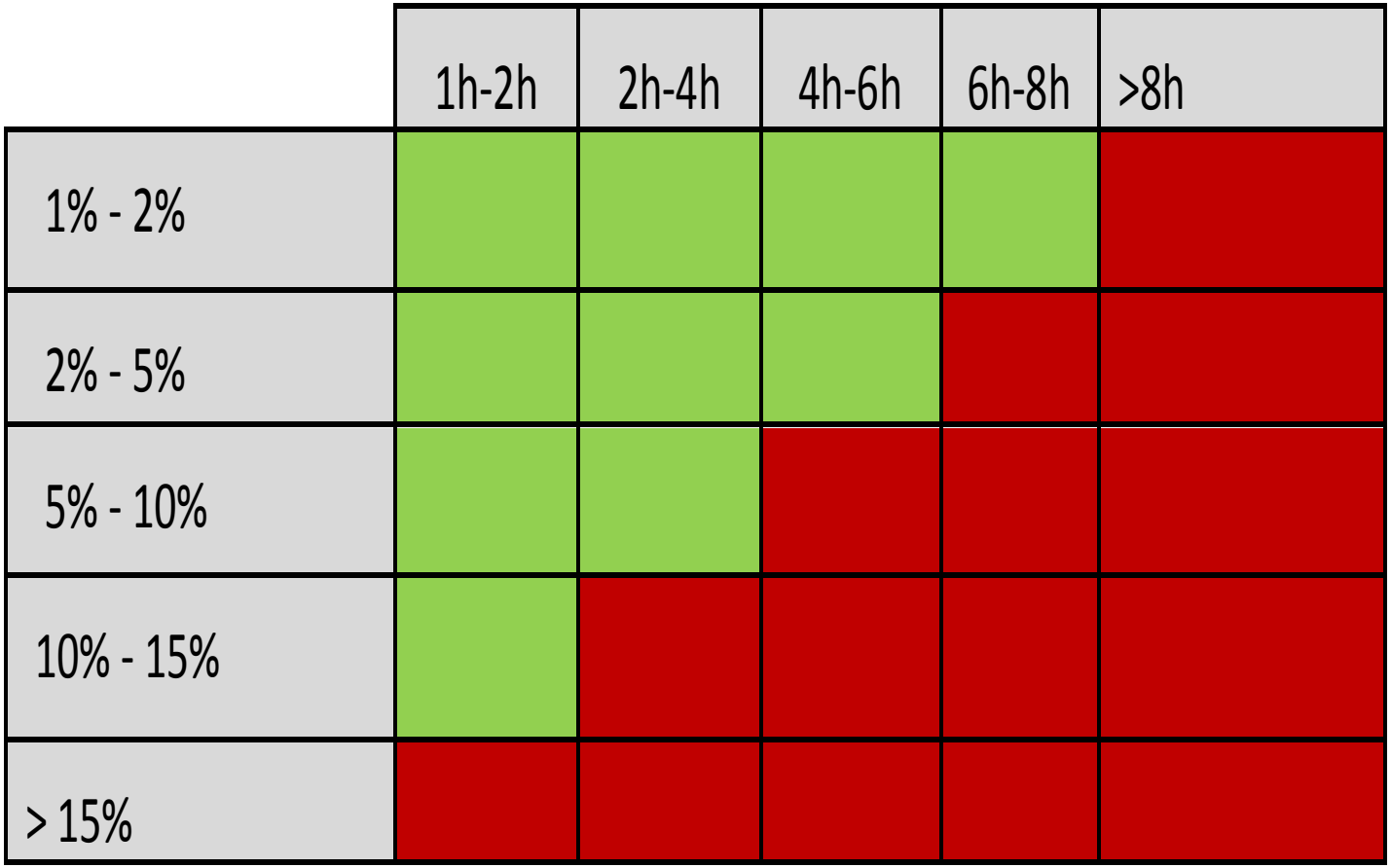
Article 13a Expert group

- Experts from NRAs from all EU countries

- F2F meetings to discuss
  - Implementation of the EU directive
  - Supervision
  - **Past incidents, stories**

- Guideline on incident reporting
- Guideline on security measures
- Mailinglist, portal, issue tracker
- Contact list for cross border notification
- State of play, issues per EU member state

Thresholds for annual reporting



Reporting tool: EU/ENISA view

CIRAS PILOT

- Home
- EU Cyber Exercises
- EU-US Exercise
- Article 13a
  - Workshops
  - MSM Working Group
  - Teleconferences
  - Reference material
  - State of Play
  - Contact List
  - Issue tracker
  - Guideline for Incident Reporting
  - Guideline for Minimum Security Measures
  - Annual summary reporting
  - CIRAS demo
  - CIRAS PILOT
    - Legoland
    - Pavland
    - Crymogaea
    - Green Europe
    - Wadiya
    - Takatuka
    - Laputa
    - Atlantis
    - Crystalia
    - Wonderland
    - Utopia
    - Narnia
    - Incident Search

Countries

Country	Incident reports	Annual reports
view Legoland	0	0
view Pavland	0	0
view Crymogaea	0	0
view Green Europe	0	0
view Wadiya	1	0
view Takatuka	0	0
view Laputa	0	0
view Atlantis	0	0
view Crystalia	0	0
view Wonderland	0	0
view Utopia	0	0
view Narnia	0	0

Search incident reports of all countries

Search incident reports

Update user permissions

Update permissions

Logs

Listing latest 50 log entries. View full log

Reporting tool: Country page

Wadiya

Country data

Fixed telephony users: 4000000
Mobile telephony users: 5000000
Fixed Internet users: 3000000
Mobile Internet users: 4000000
NRA Contact data: WTR, Wadiya's Telecom Regulators, Regulators street, +003123456789, Telecity, Wadiya

Edit country data

Authorized users

Plone user id	User name	Email address
efthyco	Costas Efthymiou	Costas.Efthymiou@ocecpr.org.cy

Annual Reports

No reports have yet been submitted.

Incident reports

Incident id	Impact	Date added	Date modified	
493748	Fixed telephony(12h, 500000) Fixed internet(10h, 300000)	21-12-2012 22:20:13	21-12-2012 22:20:14	view edit delete

Add incident | Send as annual report | Export to XML | Export to CSV | Export to HTML

Search incident reports of all countries

Search incident reports

Logs

Reporting tool: Incident form - impact

National ID

2013-14435245

Date

Year

2013

Service impact

	duration (hours)	number of users	
☐ **Fixed telephony**			☐ PSTN ☐ DSL ☐ Fiber ☐ Cable ☐ other
☑ **Fixed internet**	3	3.000.000	☐ DSL ☐ Fiber ☐ Cable ☐ other
☐ **Mobile telephony**			☐ GSM ☐ UMTS ☐ LTE ☐ other
☐ **Mobile internet**			☐ GPRS/EDGE ☐ UMTS ☐ LTE ☐ other
☐ Service	duration (hours)	number of users	

Other impact

☑ **Impact on emergency calls**

Check if availability of emergency services were impacted by the incident.

☐ **Impact on interconnections**

Check if there was impact on interconnections, affecting other operators in the same country or abroad.

Reporting tool: Incident form - causes

Root cause category

- [ ] System failures
- [ ] Human errors
- [ ] Malicious actions
- [x] Natural phenomena
- [ ] Third party failures

Initial cause

- [ ] Cable cut
- [ ] Cable theft
- [ ] Flood
- [x] Heavy snowfall
- [ ] Storm
- [ ] Power cut
- [ ] Power surges
- [ ] Physical attack
- [ ] Cyber attack
- [ ] Bad change
- [ ] Bad maintenance
- [ ] Overload
- [ ] Fuel exhaustion
- [ ] Policy/procedure flaw
- [ ] Hardware failure
- [ ] Software bug
- [ ] Human error
- [ ] None
- [ ] No information
- [ ] Other

Subsequent cause

- [ ] Cable cut
- [ ] Cable theft
- [ ] Flood
- [ ] Heavy snowfall
- [ ] Storm
- [x] Power cut
- [ ] Power surges
- [ ] Physical attack
- [ ] Cyber attack
- [ ] Bad change
- [ ] Bad maintenance
- [ ] Overload
- [x] Fuel exhaustion
- [ ] Policy/procedure flaw
- [ ] Hardware failure
- [ ] Software bug
- [ ] Human error
- [ ] None
- [ ] No information
- [ ] Other

Assets affected by initial cause

- [x] Base stations and controllers
  (e.g. BTS, NodeB, RNC)
- [x] Mobile switching
  (e.g. MSC, VLR, SGSN, GGSN)
- [ ] User and location registers
  (e.g. HLR, HSS, AuC)
- [ ] Switches
  (e.g. local exchanges, routers, DSLAM)
- [ ] Transmission nodes
  (e.g. SDH, WDM)
- [ ] Core network
  (e.g. fibre-core, cable-aggregation)
- [ ] Interconnections
  (e.g. IXPs, IP transit)
- [ ] Power supply system
  (e.g. transformers, power grid)
- [x] Backup power supply
  (e.g. diesel generators, batteries)
- [ ] Cooling system
- [ ] Street cabinets
- [ ] Messaging center
- [ ] Switching center
  (MSC, VLR, e.g.)
- [ ] International backbone
  (submarine cables, internet exchange points, international interconnections, e.g.)
- [ ] Addressing servers
  (DHCP, DNS)
- [ ] Operator backbone
  (fiber, cables, e.g.)
- [ ] Area network
  (fiber, cables, e.g.)

Article 13a Security measures

D1: Governance and risk management

This domain covers the security measures related to (network and information security) governance and risk management.

SD1.1 Information security policy

The Telco should establish and maintain an appropriate information security policy.

L	Practice	Evidence
1	a) Set a high level security policy addressing the key business processes of the organisation. b) Make key personnel aware of the security policy.	• Policy document exists, and describes primary assets in scope and security objectives. • Key personnel aware of the policy and its objectives (interview).
2	c) Set detailed security policies for key assets and business processes. d) Make all employees aware of the existence and what it implies for their work. e) Review the policy following incidents.	• Policy document or documents are approved by management. • They include applicable law and regulations is included. • They are accessible to personnel and contractors. • Most employees are aware of the security risks affecting their job and how the policy applies to their job (interview).
3	f) Review the information security policies periodically, and take into account past	• Security policies have been regularly updated and fine-tuned, and approved. • There are logs of policy exceptions

One size does not fit all

objectives. For example, an NRA could be interested in a domain like business continuity or specific security objectives around change management.

The sophistication levels can be used by providers to indicate, per security objective, what kind of security measures are in place. The sophistication levels could be used to make a profile per provider, which would allow for a quick comparison between providers.

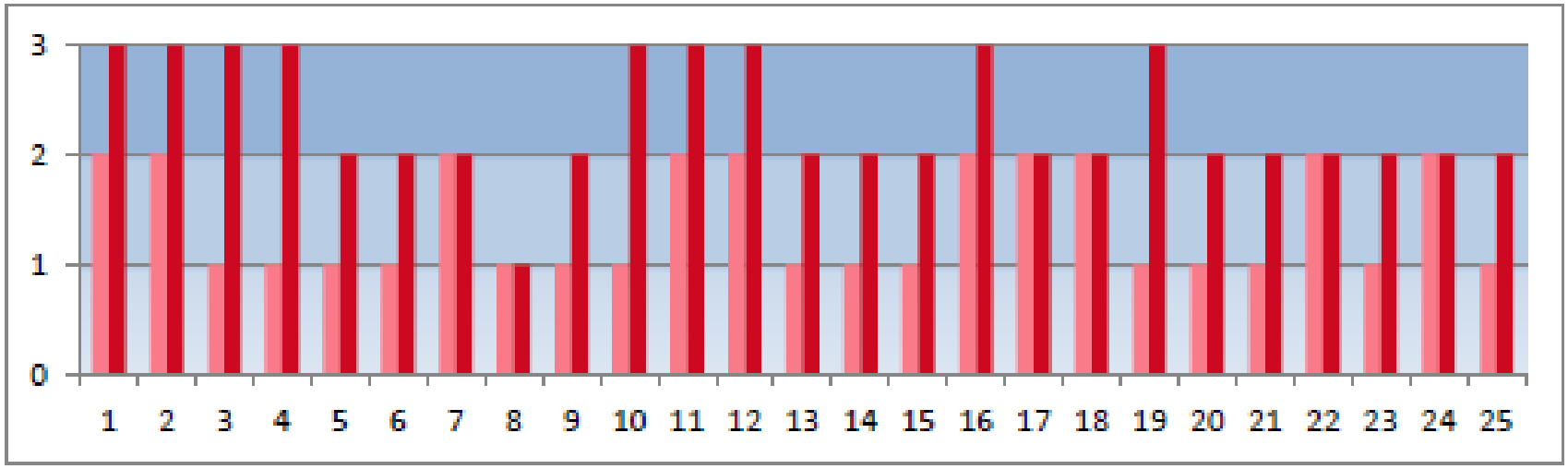


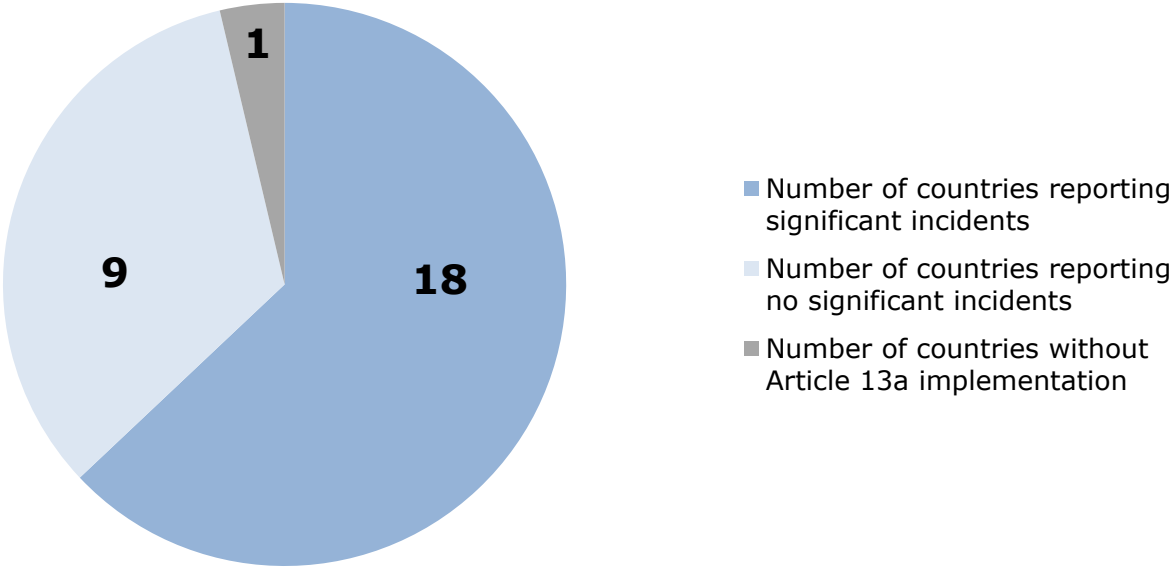
Figure 1: Two different profiles with varying sophistication for different security measures.

Mapping to existing international standards

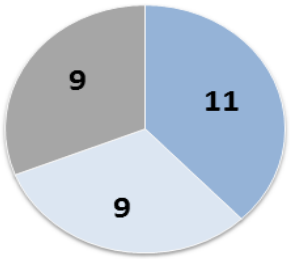
MSM	Telco	Compliance details
D1: Governance and risk management	ISO 27001/2 and ISO 27005	ISO27005 describes methods for setting the scope of information security risk management. ISO27002 Ch 5 covers information security policy, governance, risk management and controls for third parties (who deliver services, hardware or software), such as security requirements and procurement procedures for developed or acquired information systems.
D2: Human resources security	ISO 27001/2	ISO27001/2 Ch 8 covers security clearances, security roles and responsibilities, security knowledge and training, and personnel changes.
D3: Security of systems and facilities	ISO 27001/2	ISO27001 Ch 9 covers the physical security of facilities, IT equipment and environmental controls
D4: Operations management	ISO 27001/2	ISO27001 Ch 10 covers operational procedures, operational roles, classification, access control and change controls.
D5: Incident management	ISO 27001/2	ISO27002 Ch 13 covers incident management.
D6: Business continuity management	BS 25999-1/2	BS 25999 covers business continuity.
D7: Monitoring and	ISO 27001/2	Monitoring is covered in ISO27001/2 Ch 10: security testing

Annual reporting 2013 (2012 incidents)

- …for the second time, national authorities reported about **major outages** in the e-comms sector



In 2012:



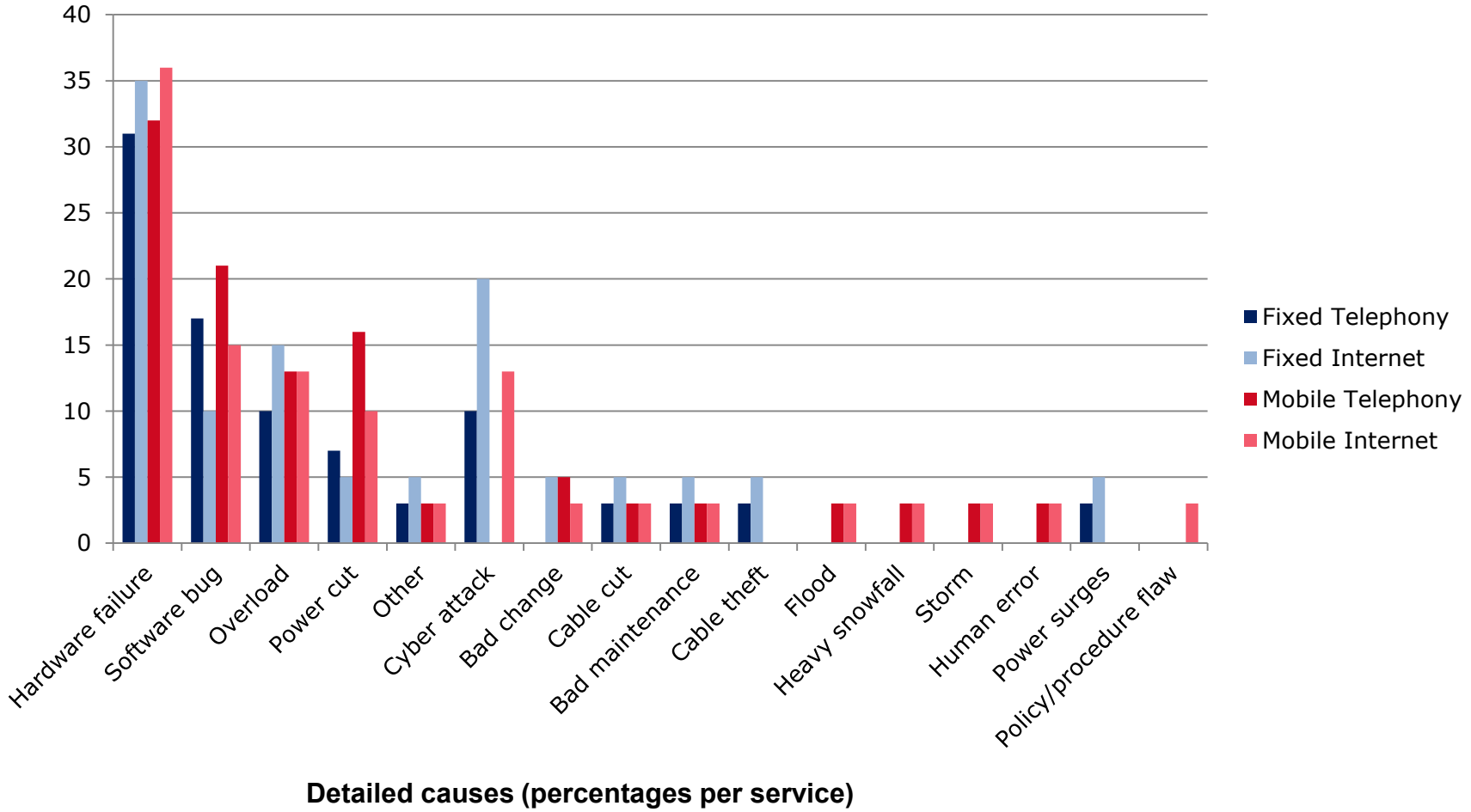
Examples of major outages reported

- Configuration error (hours, millions, configuration error)
  - An employee of a fixed telephony provider made a configuration error. The error prevented fixed telephony users to make outgoing international phone calls to Western European countries for 4 hours. The incident was resolved after a reconfiguration and a reboot.
- Vandalism by former employee affected DSL (days, thousands, malicious attack)
  - A former employee of a provider deliberately set fire to a switching system, which was used for providing fixed internet service to around 10.000 subscribers. The incident was resolved by replacing the switch. Around 36 hours later the fixed internet service was working again.
- Faulty software update affected mobile telephony (hours, thousands, software failure)
  - A provider applied a regular software update at a Home Location Register (HLR) which turned out to be faulty. The failure at the HLR impacted mobile telephony and internet services. The incident affected about half of the provider's customers and lasted around 8 hours.
- Submarine cable cut from anchorage (hours, thousands, third party)
  - A ship's anchoring damaged one of four submarine cables connecting two islands. Contingency plans were triggered quickly, which meant that only a smaller number of users were affected.

Annual report about 2012 incidents

- 40 pages with statistical data, diagrams and some* conclusions.
- No mentioning of single countries,
- No mentioning of single incidents or providers.
- Hardly any conclusions: it is a starting point for discussions with regulators

Hardware, software failures most common cause

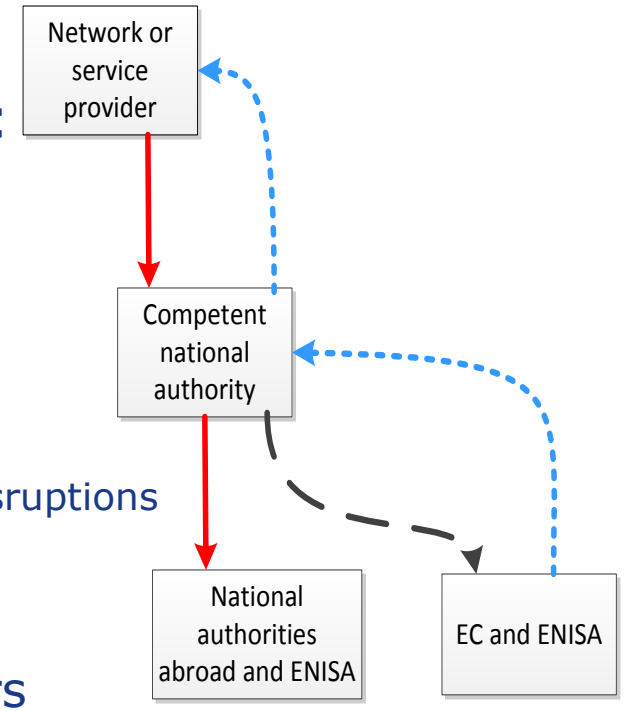


Detailed causes (percentages per service)

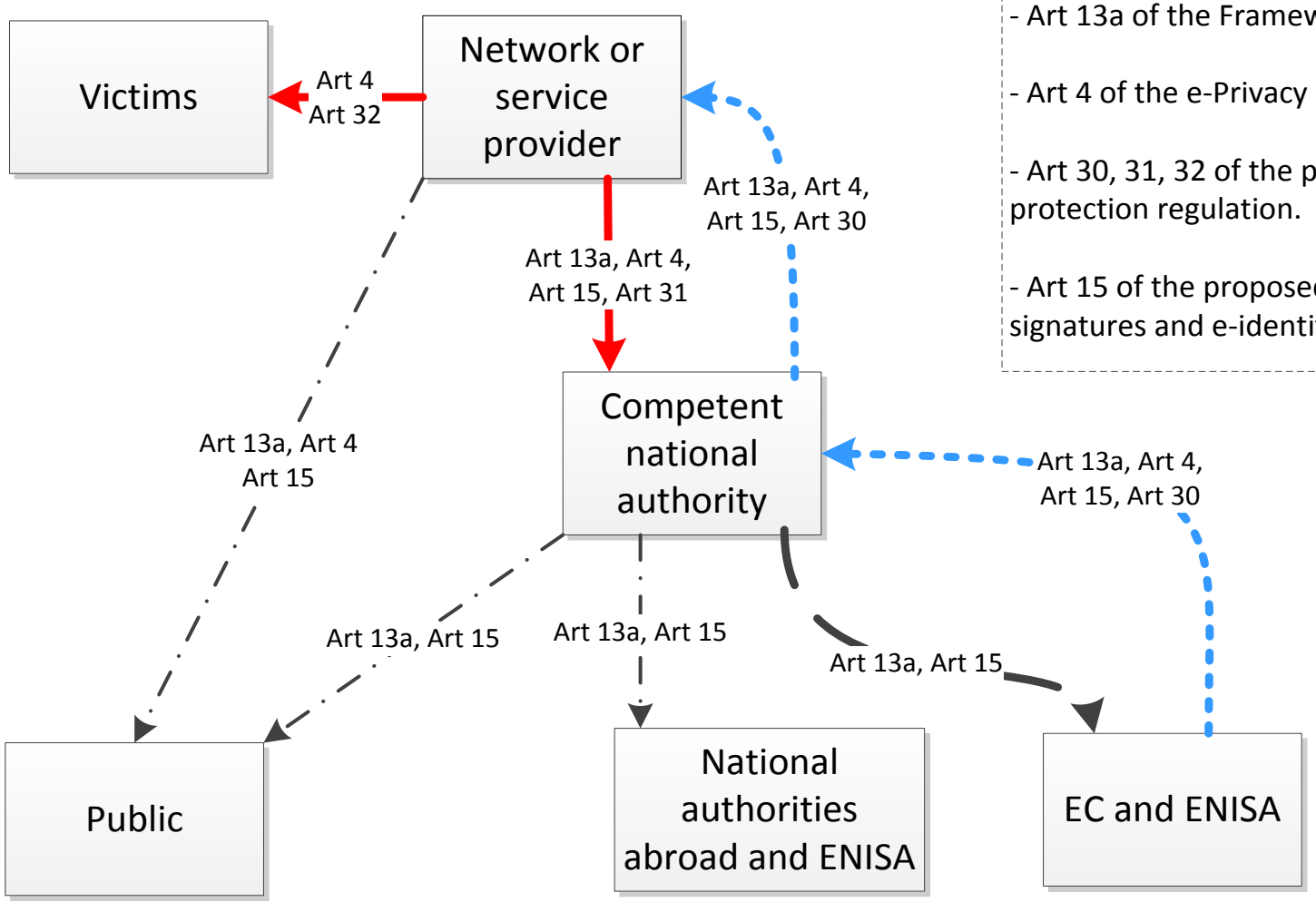
Article 13a: Full cycle supervision

- Update, issue recommendations on security measures together with Article 13a expert group and industry experts.

- In 2013 we are addressing two topics:
  - National roaming
    - To mitigate mobile network outages
    - Pros and cons per roaming setup
  - Power supply dependencies
    - Analysis of power dependencies in the sector
    - Reduce network outages caused by power disruptions
    - Improve handling of power disruptions
- In 2014 we plan to address
  - Dependencies on IT equipment/vendors



Other security articles in EU legislation



- Art 13a of the Framework directive.

- Art 4 of the e-Privacy directive.

- Art 30, 31, 32 of the proposed Data protection regulation.

- Art 15 of the proposed regulation on e-signatures and e-identities

EU Cyber security directive

EUROPEAN
COMMISSION

Brussels, 7.2.2013
COM(2013) 48 final

2013/0027 (COD)

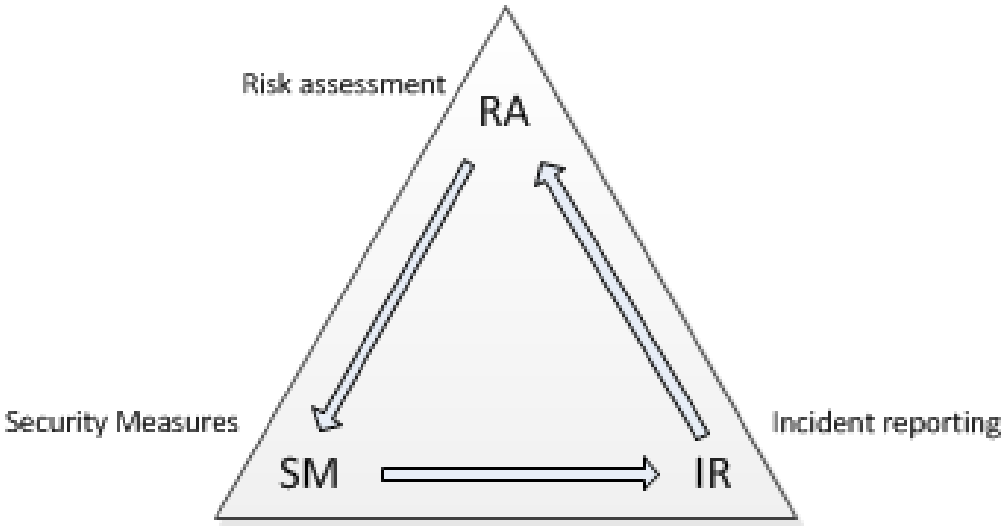
Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

concerning measures to ensure a high common level of network and information security across the Union

Part is based on Article 13a

Thirdly, based on the model of the Framework Directive for electronic communications, the proposal would aim to ensure that a culture of risk management develops and that sharing of



Article 14: Security and notifications

Article 14

Security requirements and incident notification

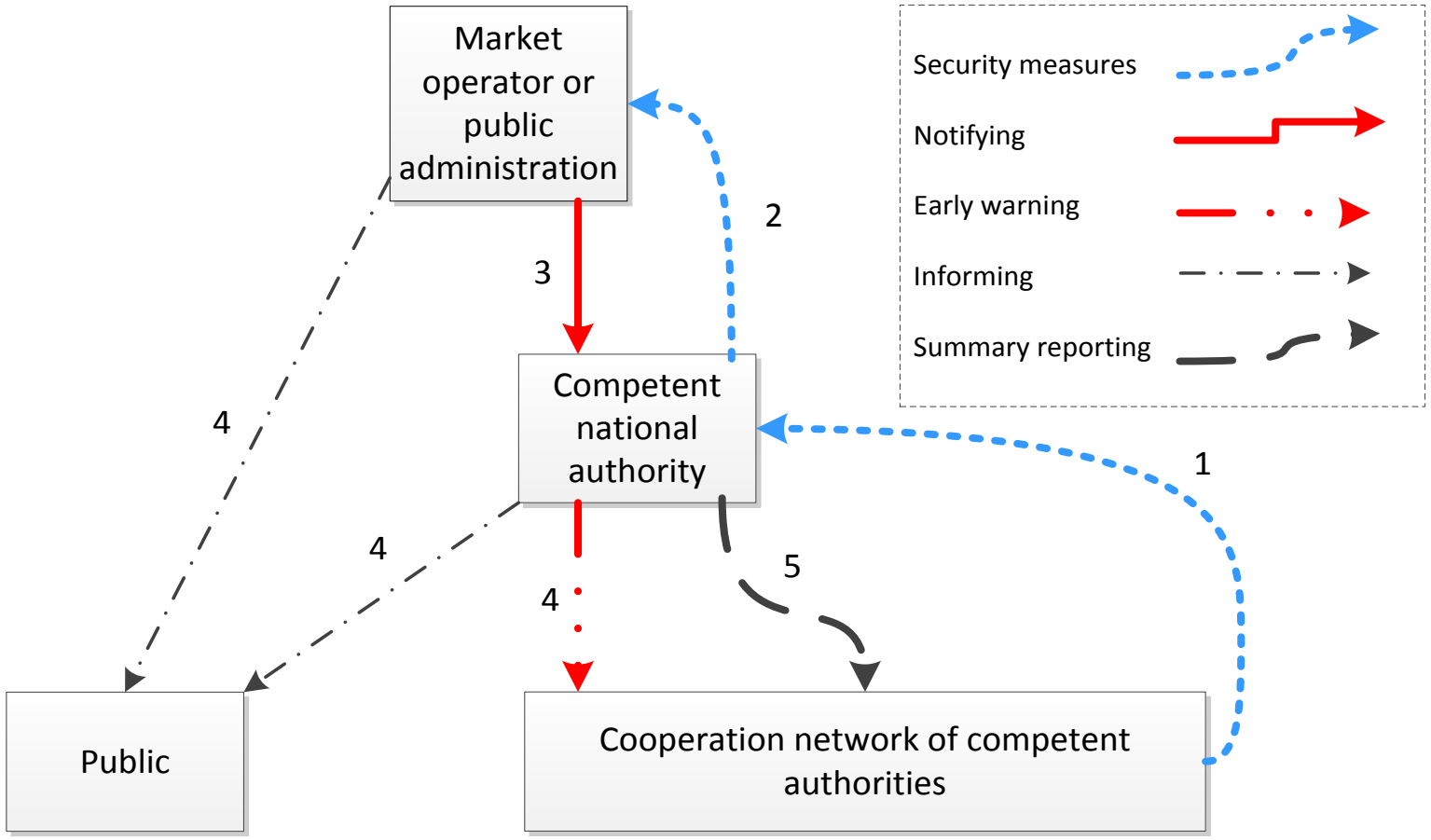
1. Member States shall ensure that public administrations and market operators take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations. Having regard to the state of the art, these measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems.

2. Member States shall ensure that public administrations and market operators notify to the competent authority incidents having a significant impact on the security of the core services they provide.

3. The requirements under paragraphs 1 and 2 apply to all market operators providing services within the European Union.

4. The competent authority may inform the public, or require the public administrations and market operators to do so, where it determines that disclosure of the incident is in the public interest. Once a year, the competent authority shall submit a summary report to the cooperation network on the notifications received and the action taken in accordance with this paragraph.

Information flows in Article 14



Operators and services in scope

(8) "market operator" means:

(a) provider of information society services which enable the provision of other information society services, a non exhaustive list of which is set out in Annex II;

(b) operator of critical infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health, a non exhaustive list of which is set out in Annex II.

Referred to in Article 3(8) a):

1. e-commerce platforms
2. Internet payment gateways
3. Social networks
4. Search engines
5. Cloud computing services
6. Application stores

Preambles: One reporting framework

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.

- ENISA should
  - Support Information exchange mechanisms
  - Bridge between DPAs and 'regulators'
  - Develop Single reporting template
    - Article 13a, Article 4, Article 30,31 of the proposed DB regulation, Article 15 of the

Article 8: Network of regulators

Article 8

Cooperation network

1. The competent authorities and the Commission shall form a network ("cooperation network") to cooperate against risks and incidents affecting network and information systems.

2. The cooperation network shall bring into permanent communication the Commission and the competent authorities. When requested, the European Network and Information Security Agency ("ENISA") shall assist the cooperation network by providing its expertise and advice.

3. Within the cooperation network the competent authorities shall:

   (a) circulate early warnings on risks and incidents in accordance with Article 10;

   (b) ensure a coordinated response in accordance with Article 11;

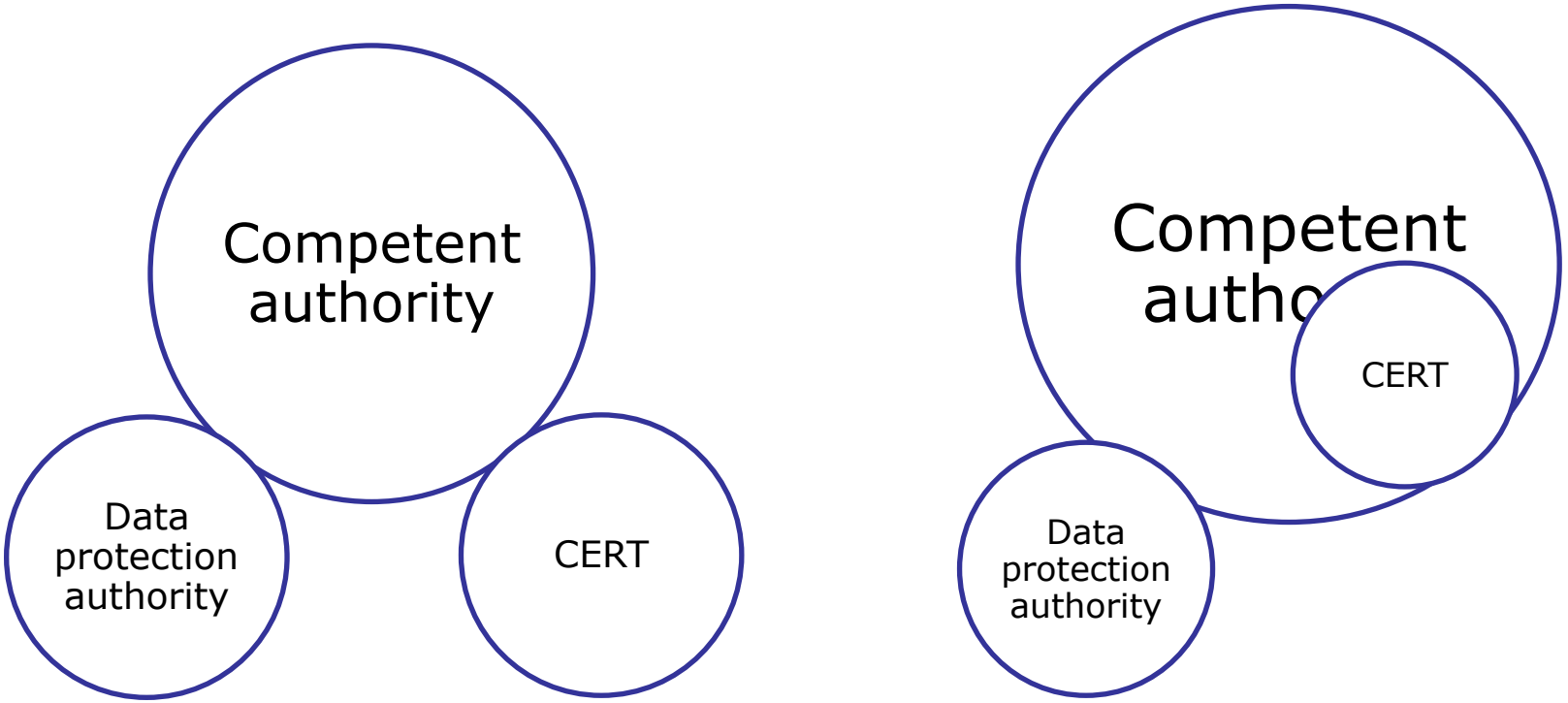
   (c) publish on a regular basis non-confidential information on on-going early warnings and coordinated response on a common website;

   (d) jointly discuss and assess, at the request of one Member State or of the Commission, one or more national NIS strategies and national NIS cooperation plans referred to in Article 5, within the scope of this Directive.

   (e) jointly discuss and assess, at the request of a Member State or the Commission, the effectiveness of the CERTs, in particular when NIS exercises are performed at Union level;

   (f) cooperate and exchange information on all relevant matters with the EuropeanCybercrime Center within Europol, and with other relevant European

Regulators in the Cyber security directive



Our focus and goals

- **Technicalities of incident reporting and supervision of security**
  - Tools, technical guidance for supervisory authorities
  - Pan-EU exchange of best practices between NRAs
  - Bridge with private sector
  - Enable harmonization of national approaches
- Examples of technical issues
  - What services should be addressed (first)?
  - Which incidents/breaches are in scope?
  - How to use incident reporting to prevent incidents in the future?
  - How to supervise that ‘appropriate’ security measures are taken?
  - How to supervise across borders?
  - How to align national and provider risk assessments?
- **How to incentivize reporting?**

Discussion topics

- Sharing without scaring?
  - “Heavy fines and bureaucracy for every single breach!! That will teach them!!”
  - Increase transparency/knowledge about incidents/vulnerabilities.
  - How to incentivize reporting? (anonimity/immunity for reporters, fines/sanctions for not reporting –not for incidents, Corporate culture , return value)
  - Sharing lessons learnt! (look beyond competition?).
- From telegraphs/telephony, to PCs/smartphones?
  - Services in scope? Blackberry, Social media, Cloud computing? Skype? Whatsapp?
- National IT security roles?
  - Regulator vs CERT vs DPA vs civil contingency agency?
- National IT risk assessment?
  - Critical IT assets
  - only IT in critical infrastructures, or also outside?
  - How to set up a process for periodic risk assessment (actors, method, etc)

Contact us, work with us

Marnix Dekker marnix.dekker@enisa.europa.eu

Article 13a: http://resilience.enisa.europa.eu/article-13

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

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