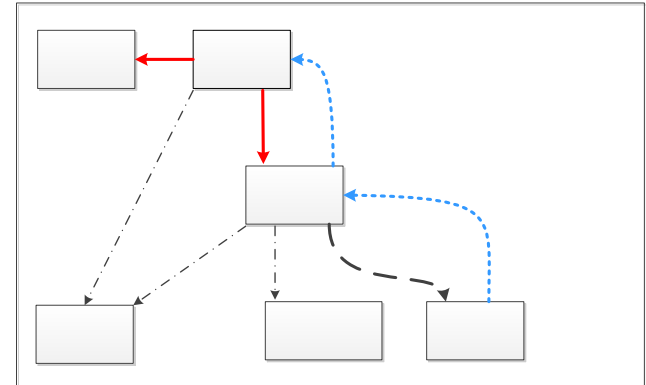




Network and Information Security Legislation in the EU



Dr. Marnix Dekker

Security expert, Information security officer
ENISA

@RSA Europe, SPER-R07 Security perspectives
Amsterdam, October 31, 2013



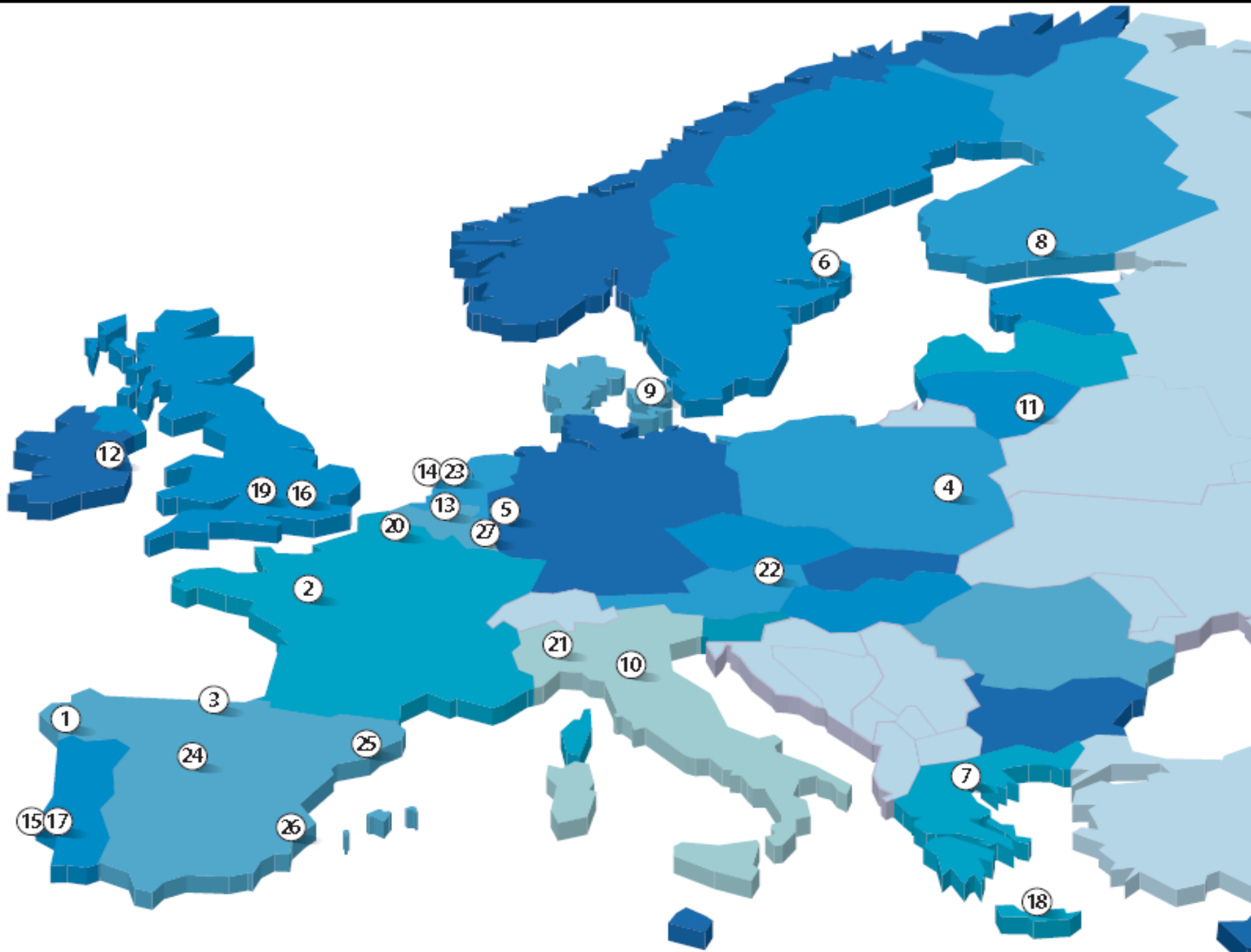


About ENISA



- European Union Network and Information Security Agency
 - gives advice on information security issues
 - to national authorities, EU institutions, citizens, businesses
 - acts as a forum for sharing good NIS practices
 - facilitates information exchange and collaboration
- Set up in 2004, new mandate in 2013 for 7 more years.
- Seat in Heraklion and office in Athens.
- Around 35 security experts and 25 staff.
- ENISA has an advisory role (not operational) and the focus is on prevention and preparedness.








Network and Information Security Legislation in the EU



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 a field of grass or other foliage. The lighting is bright, highlighting the texture of the petals.

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



Background: HTTPS is not working

- Public key cryptography is great – but PKI is cumbersome.
 - The most widely used form of PKI (HTTPS) is not user-friendly and insecure (600 single points of failure).
 - Scale of exploitation?
 - Matt Blaze <http://www.crypto.com/blog/spycerts> : “Products appear sophisticated, mature, and mass-produced... an active vendor community”
 - About CA’s: “a surprisingly large number of root authorities, from tiny, obscure businesses to various national governments”
 - Moxie Marlinspike <http://blog.thoughtcrime.org/ssl-and-the-future-of-authenticity> : Repeated hacks of CAs, and do you even need to hack?



A world map with a dark blue background and white outlines of continents and countries. Iran is highlighted in a bright red color. 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





Impact timeline

July 2011

Security breach at Diginotar

August 2011

Privacy breach in Iran

September 2011

Outage in the Netherlands





DigiNotar®

A  VASCO COMPANY

- Bankruptcy for Diginotar
- Vasco estimates losses at around 4 million euros
 - Vasco acquired Diginotar for 12 million euros

DigiD

Digitale
Identificatie



- Dutch e-Gov offline for millions of users for several weeks
- Dutch state claims 9 million euros in damages

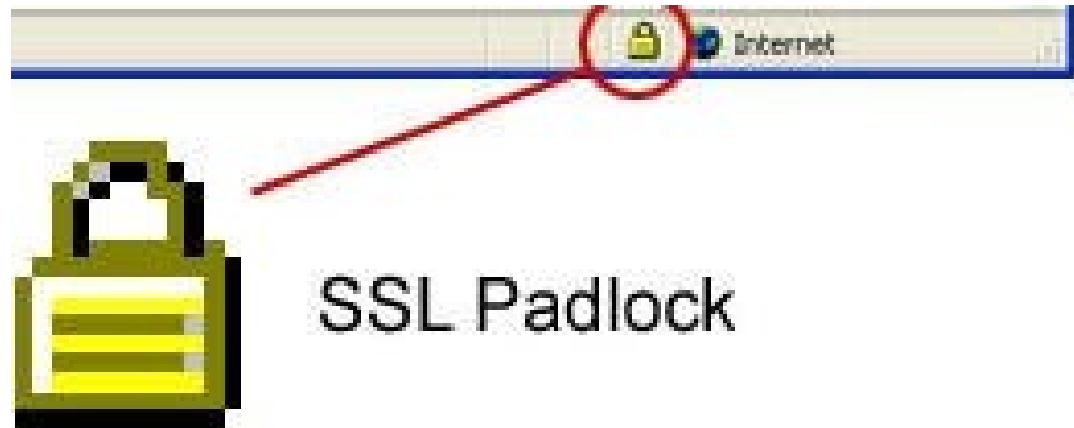
Mikko Hyppönen: “It is plausible that people died.”

... after the incident response?

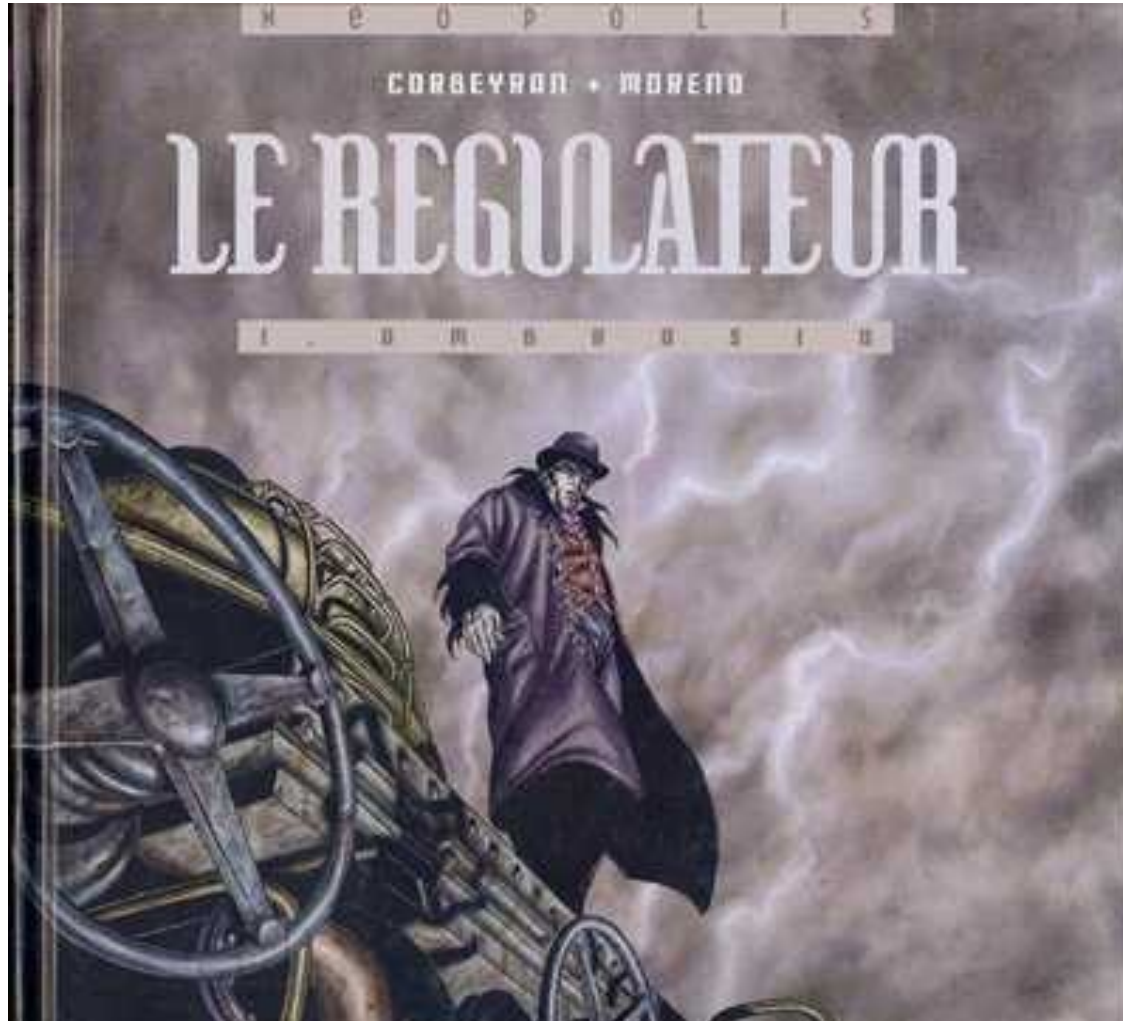


Technical discussions about PKI/HTTPS

- Google removes OCSP from Chrome (snapping seatbelt)
- Discussion about revising PKI, the role of CAs, and HTTPS?
 - DNSSEC, DANE, Convergence, TACK
 - ENISA criticises HTTPS and CAs
- And a strong push for security legislation ...



... fearsome information security legislation





The Frog & The Scorpion.

Political reaction on Diginotar

- CERT network worked well in the incident response phase
- Aart Jochem (NCSC): "PKI crisis is still ongoing".
- No incident notification/reporting obligations for Diginotar
- Weak legal grounds for the government to intervene
 - Only because Diginotar was also a CA for qualified electronic signatures (a government scheme)
- Breach at a small firm had severe impact abroad.
- New regulation
 - Extending Article 13a to etrust/esig providers
 - Extending also to other critical sectors



SBN Regulation

- Vulnerabilities of HTTPS
- Surveillance by CAs
- CAs get breached
- No incentive for security
- Security breach regulation (SBN)

Security Economics in the HTTPS Value Chain

Hadi Asghari*, Michel J.G. van Eeten*, Axel M. Ambak⁺ & Nico A.N.M. van Eijk⁺¹

* h.asghari@tudelft.nl, m.j.g.vaneeten@tudelft.nl
Delft University of Technology, Faculty of m.j.g.vaneeten@tudelft.nl and Management

⁺ a.m.arnbak@uva.nl, vaneijk@uva.nl
University van Amsterdam, Faculty of Law, Institute for Information Law

Abstract. Even though we increasingly rely on HTTPS to secure Internet communications, several landmark incidents in recent years have illustrated that its security is deeply flawed. We present an extensive multi-disciplinary analysis that examines how the systemic vulnerabilities of the HTTPS authentication model could be addressed. We conceptualize the security issues





Proposed NIS directive



EUROPEAN
COMMISSION

Brussels, 7.2.2013
COM(2013) 48 final

2013/0027 (COD)

Proposal for a

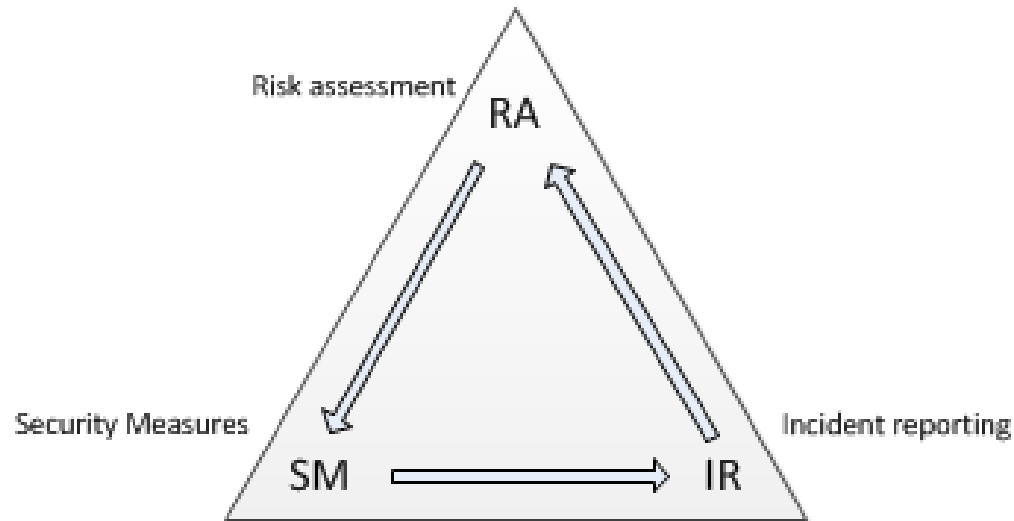
DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

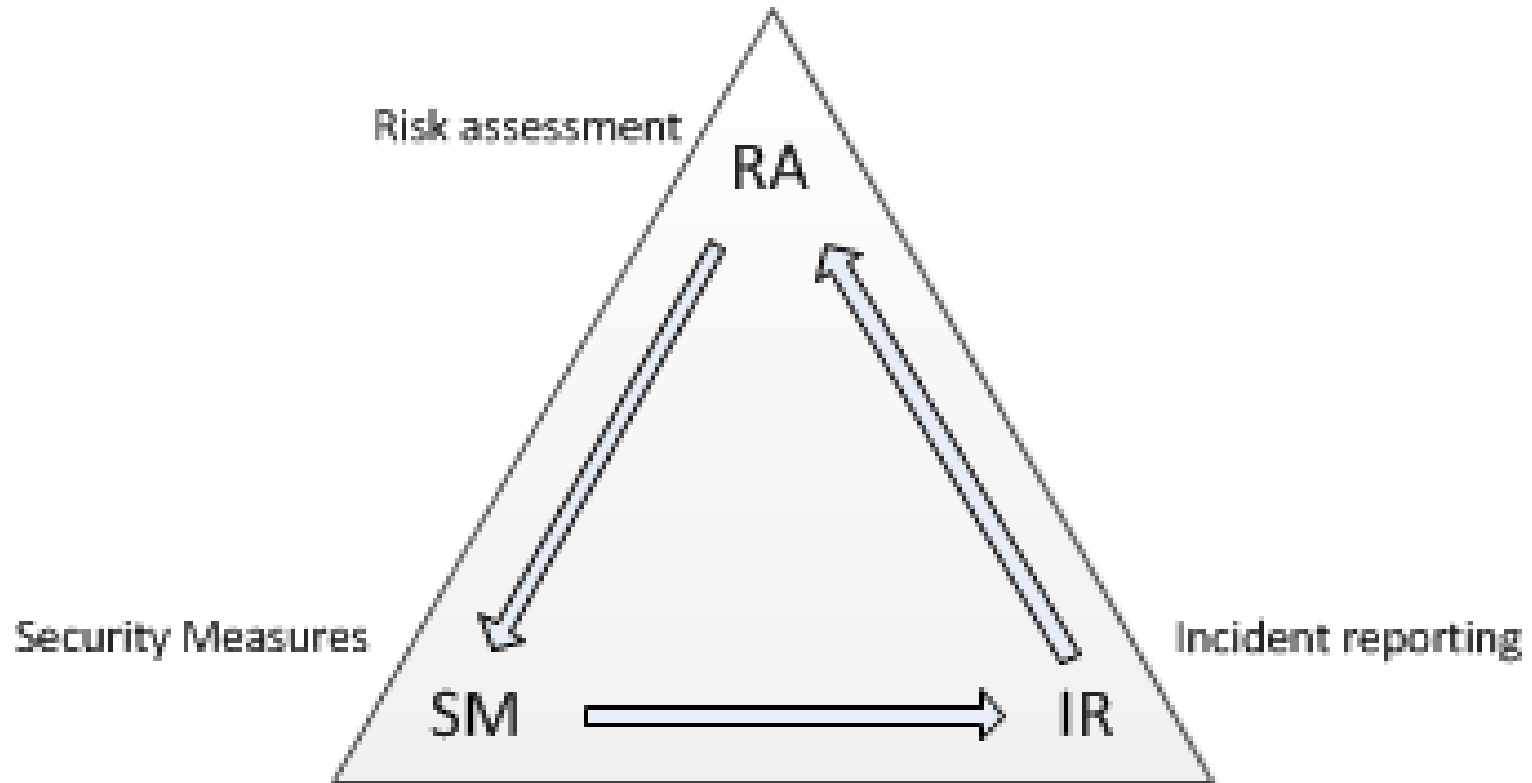


Part is based on Article 13a

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

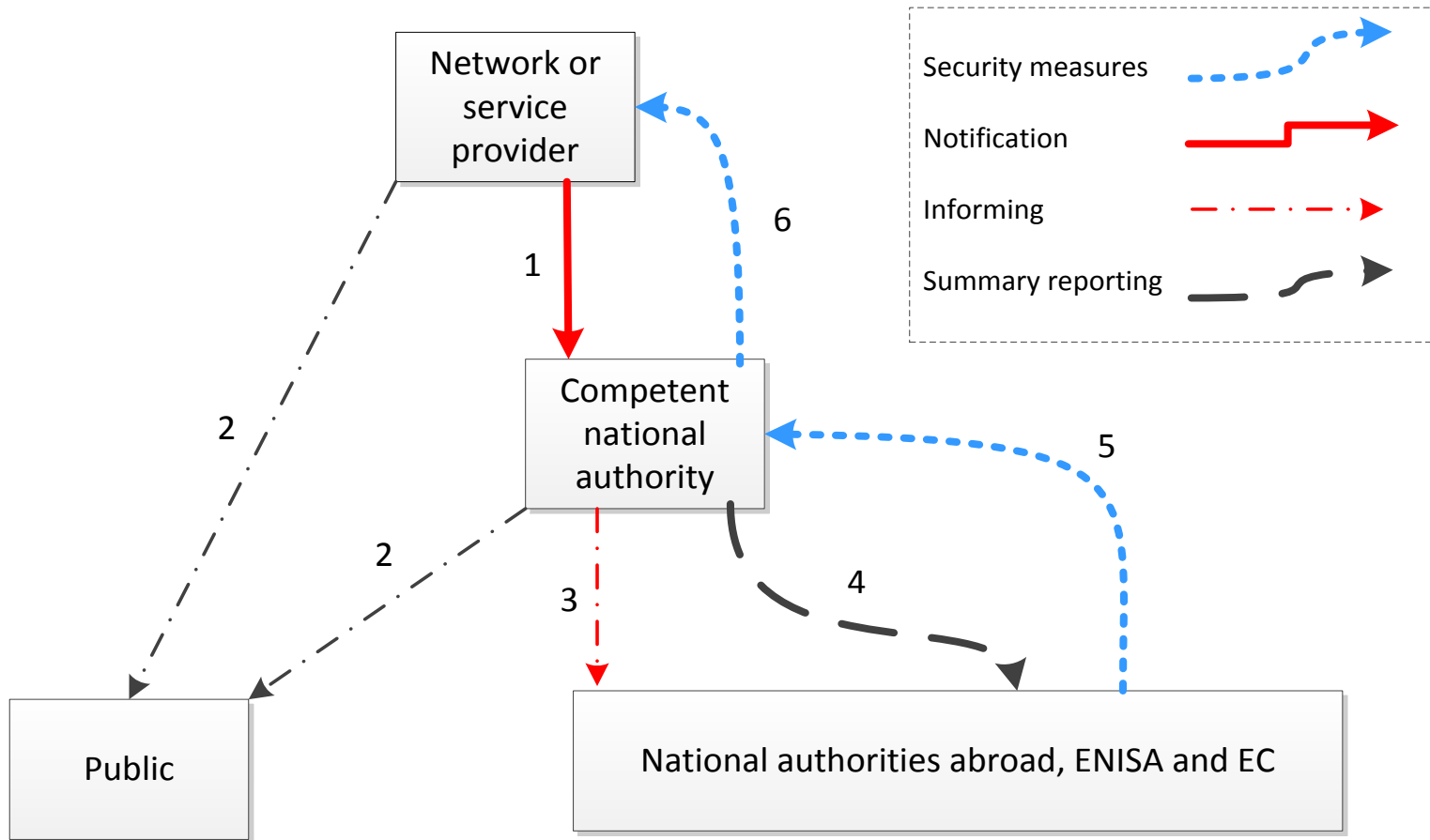


Security processes in the regulations

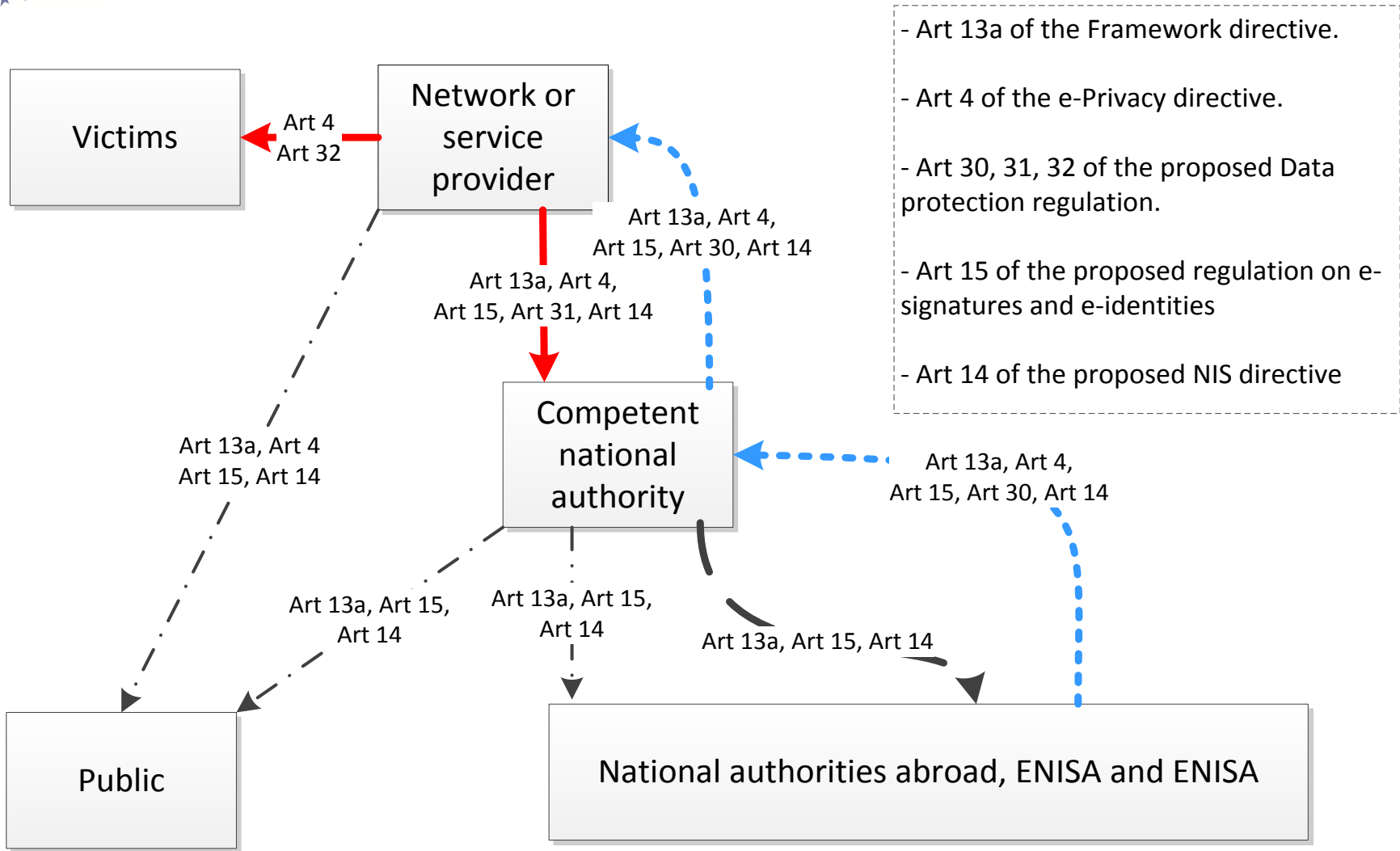


- Supervised by a national authority (regulator, DPA, etc.) in collaboration with regulators abroad (single market)

Information flows in the regulations



Security breach articles in EU legislation

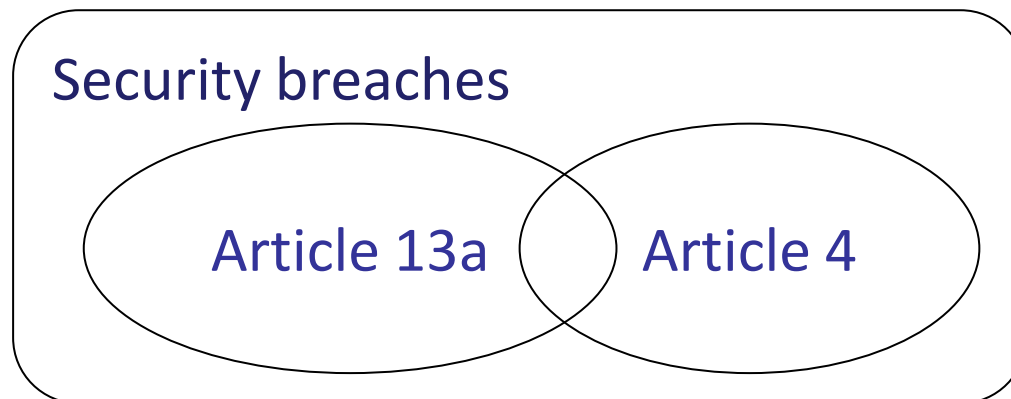




Overlapping regulation

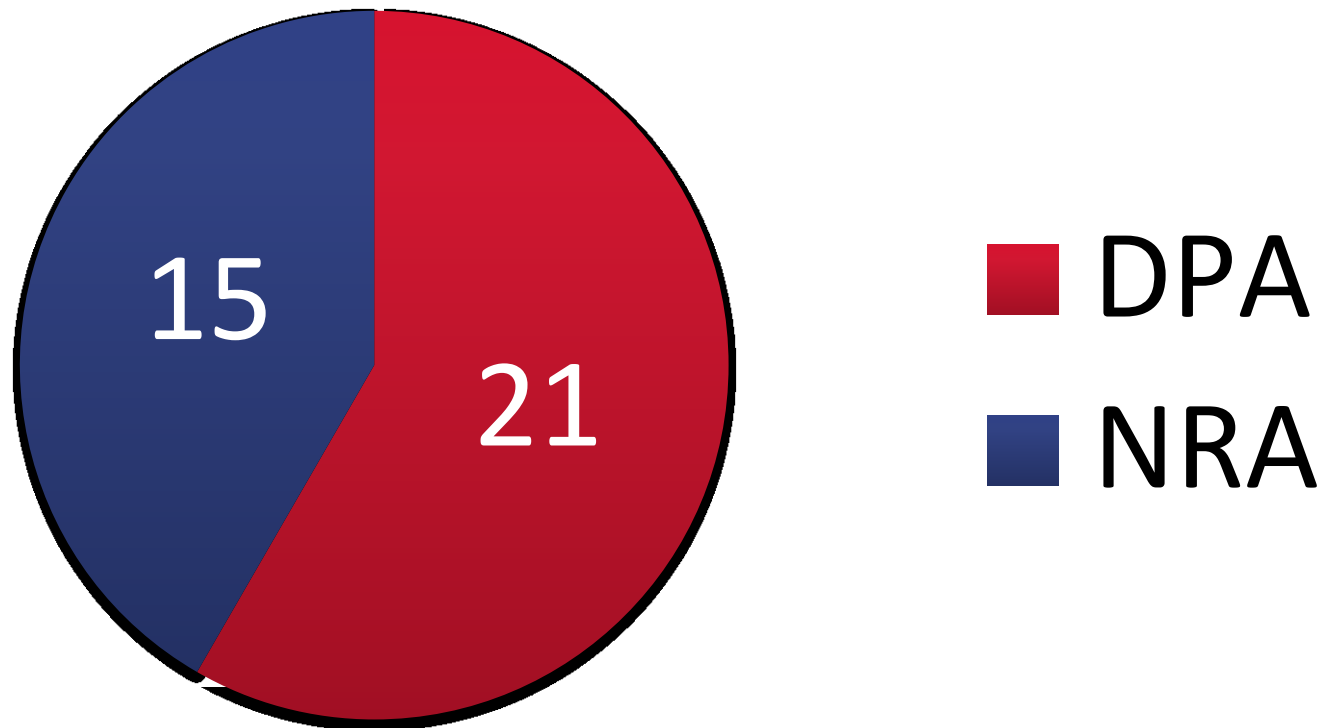
(f) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.

- Personal data breach = **Security breach** with impact on personal data



Article 4 – a joint responsibility

Authorities on personal data breaches in the telecom sector (Article 4 of the e-Privacy directive) across the EU



*) DPA – Data protection authority, NRA - telecom regulator

***) In some countries NRAs and DPAs share or split responsibility



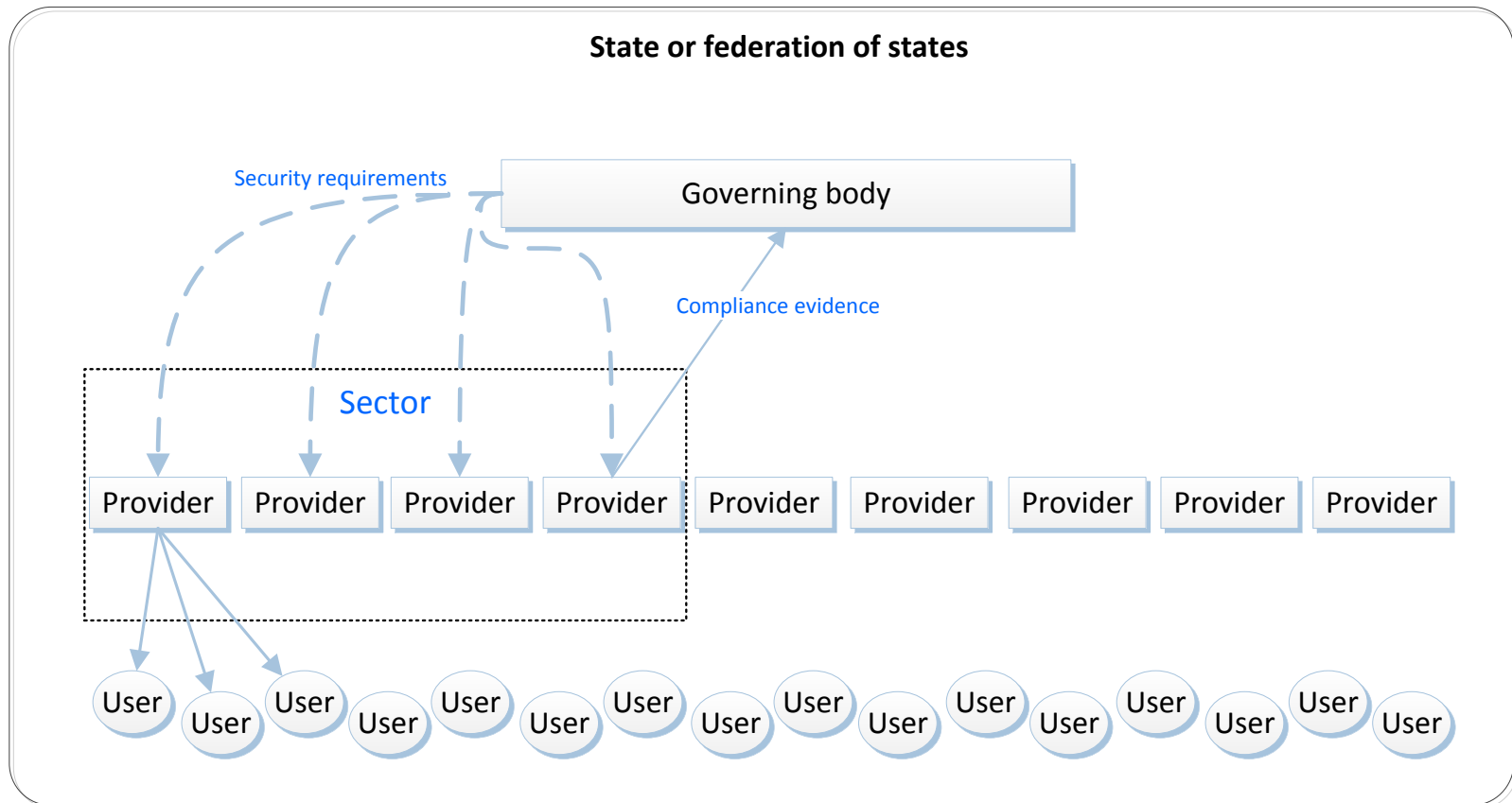
One security breach framework

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

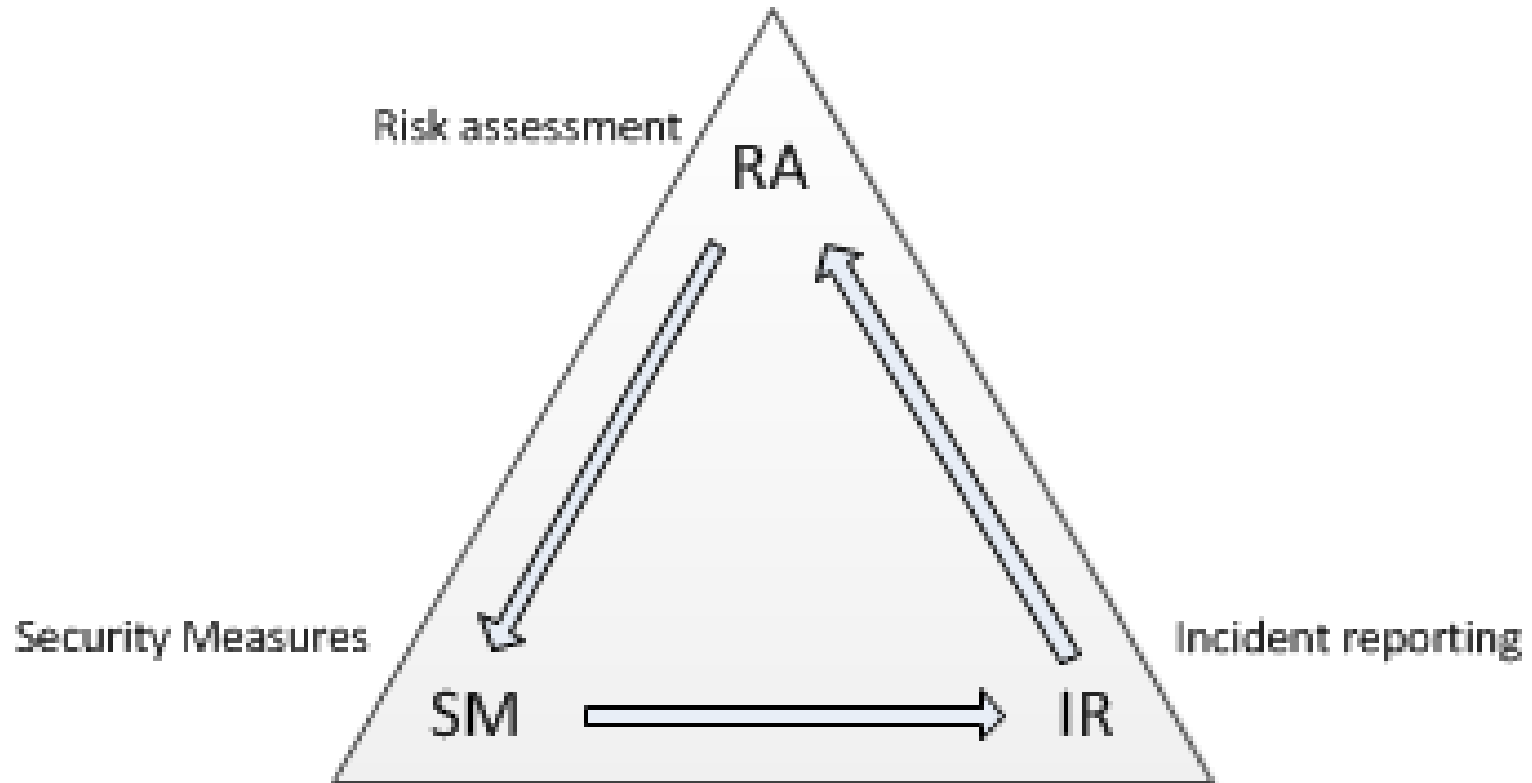
Liaising with the competent authorities and the data protection authorities, ENISA could assist by developing information exchange mechanisms and templates avoiding the need for two notification templates. This single notification template would facilitate the reporting of incidents compromising personal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

How to supervise security measures?



Security processes in the regulations



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



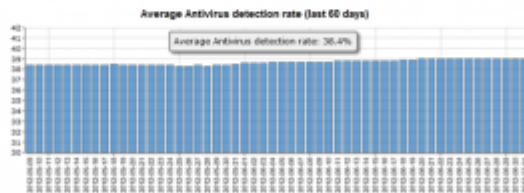
BLOG ADVERTISING

12 EU to Banks: Assume All PCs Are Infected

JUL 12

An agency of the European Union created to improve network and data security is offering some blunt, timely and refreshing advice for financial institutions as they try to secure the online banking channel: “Assume all PCs are infected.”

The unusually frank perspective comes from the **European Network and Information Security Agency**, in response to a recent “High Roller” report (PDF) by **McAfee** and **Guardian Analytics** on sophisticated, automated malicious software strains that are increasingly targeting high-balance bank accounts. The report detailed how thieves using custom versions of the **Zeus** and **SpyEye** Trojans have built automated, cloud-based systems capable of defeating multiple layers of



Statistics on Zeus: Only about 40% of Zeus malware is detected.

Source: zeustracker.abuse.ch

- Recent Pos
- Adobe Breach
- 38 Million U
- Senator Dem
- Experian
- Experian Sol
- ID Theft Serv
- Breach at PR
- Adobe Hack
- Critical Java
- Security Hol

Subscribe to



Which are appropriate security measures

- Proportionate to the risks
- Primarily the risks for the users, customers, et cetera
 - Enterprise risk mgmt frameworks are not fully applicable
- Hard: to define a-priori what is appropriate
- Feasible: Trying to move the sector faster forward
 - Use the example and best-practices of frontrunners
 - Exchange information and establish best practices
 - Flexible supervision for a diverse sector
- And analyse incident reports
 - Follow-up after major incidents

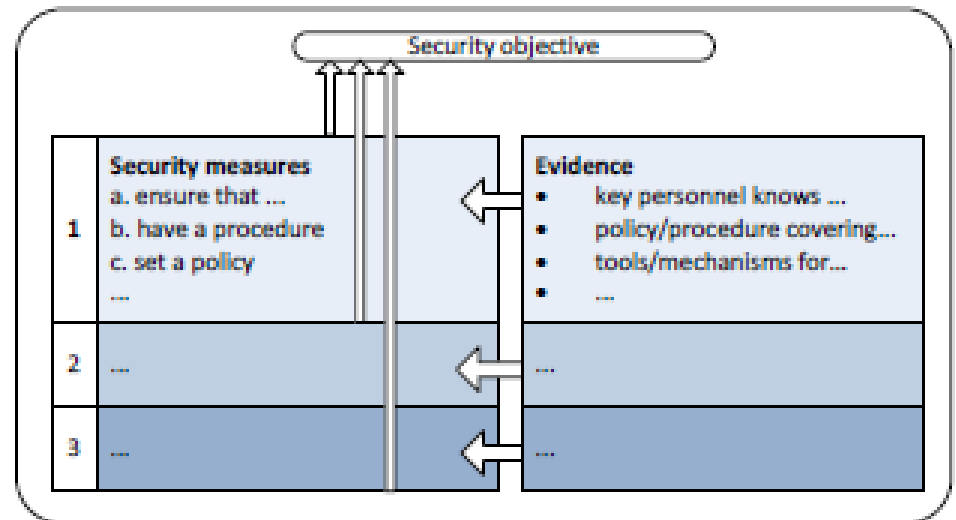
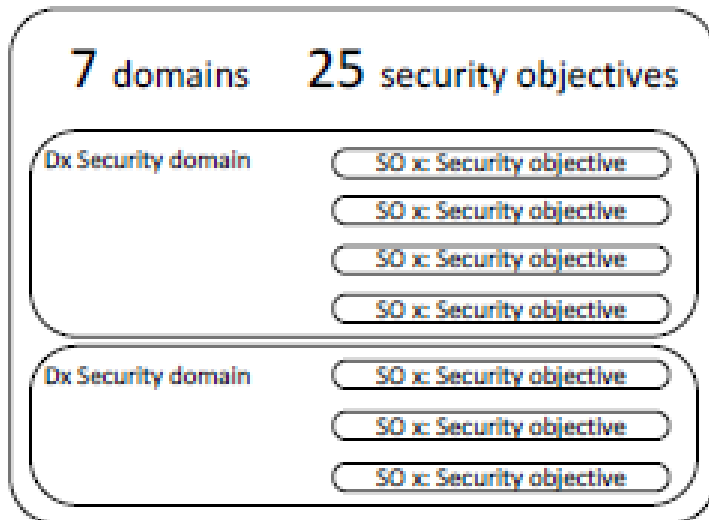


A bit like curling



Tool for supervising Security Measures

- Neutral standard/structure
- Adopted by many national authorities
- Structure for supervision
 - Interviews, questionnaires, guidance
 - Mapped to international standards



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

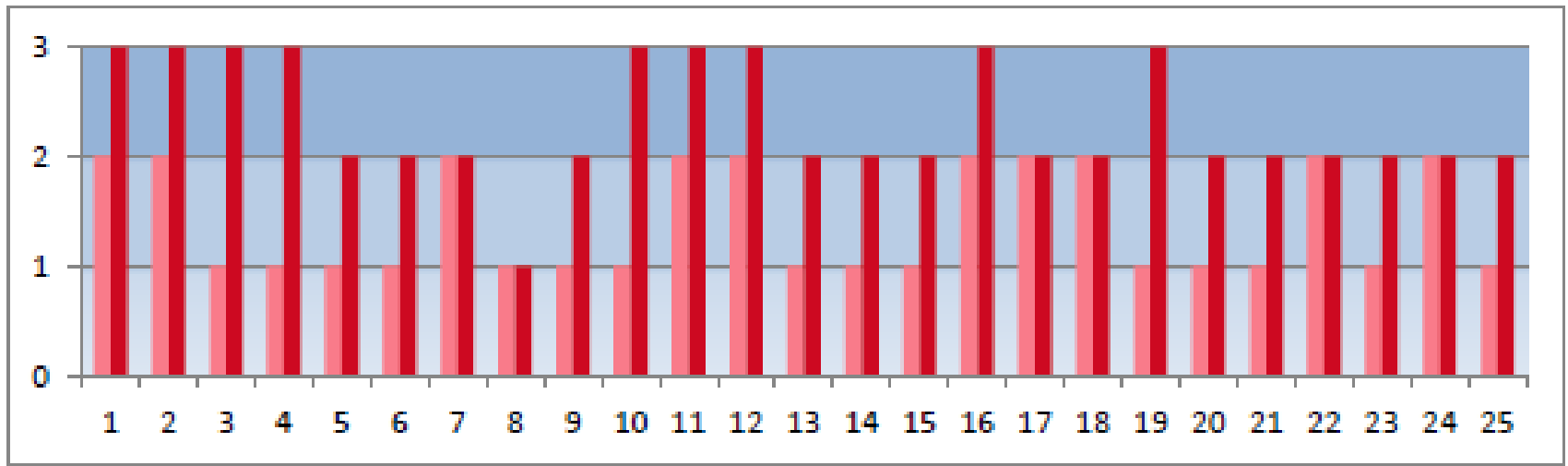
Establish and maintain an appropriate information security policy.

	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

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

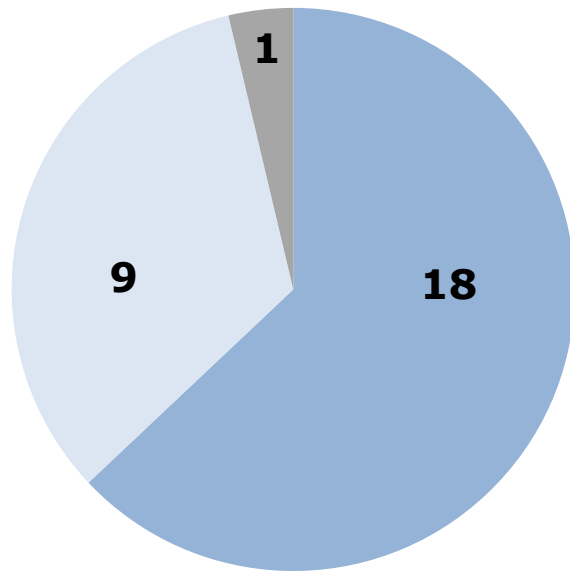
368 The sophistication levels can be used by providers to indicate, per security objective, what kind of
 369 security measures are in place. The sophistication levels could be used to make a profile per provider,
 370 which would allow for a quick comparison between providers.



371
 372 Figure 1: Two different profiles with varying sophistication for different security measures.

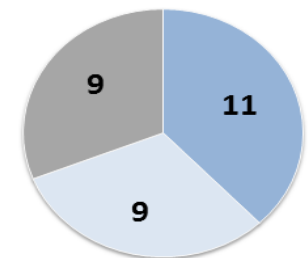
Incident reporting: annual reporting 2013

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



- Number of countries reporting significant incidents
- Number of countries reporting no significant incidents
- Number of countries without Article 13a implementation

In 2012:



One of the few tangible outcomes of Article 13a

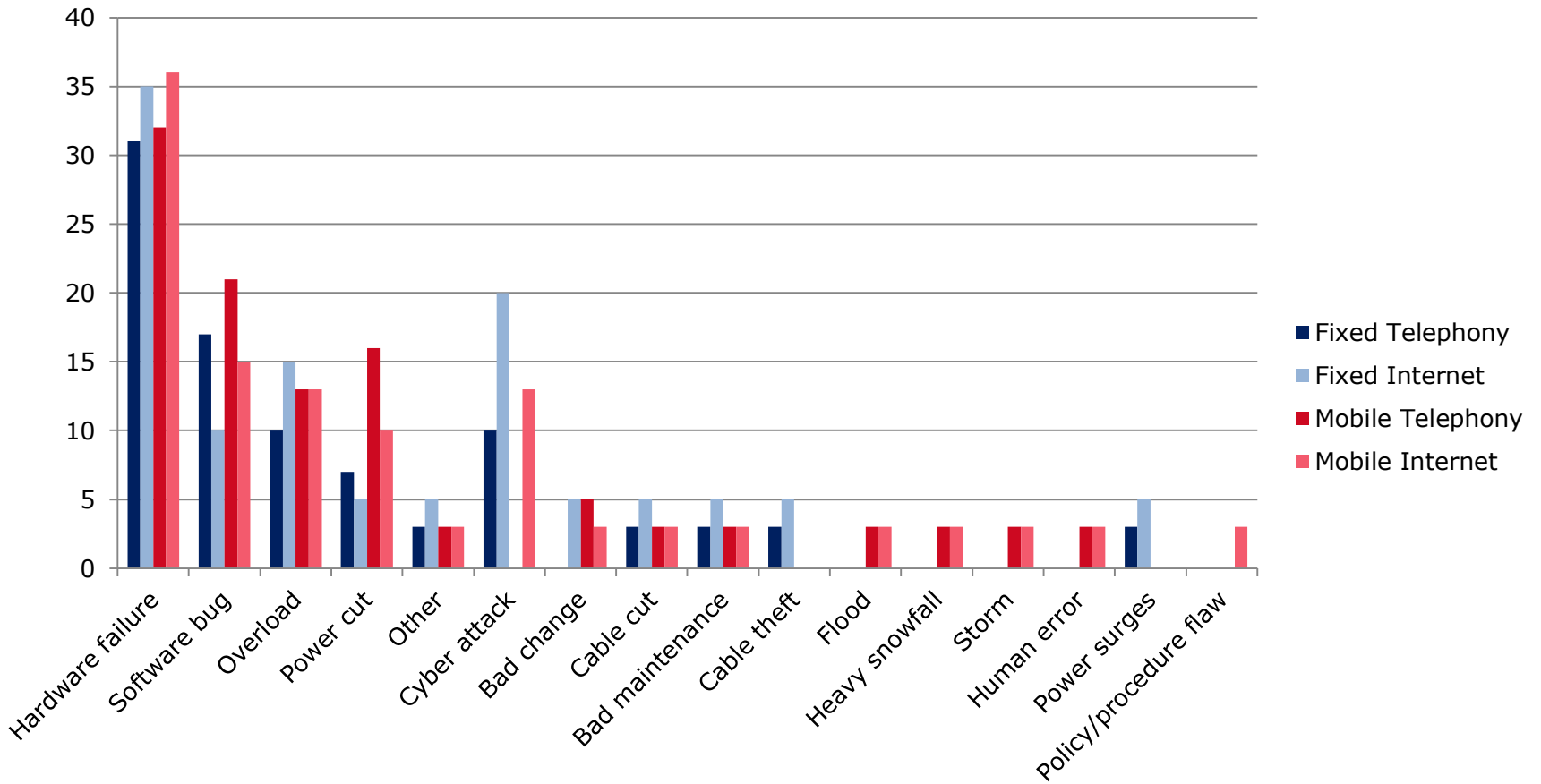
79 major outages reported

- Annual report **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

Examples of major outages (2012)

- **Overload caused VoIP outages (hours, thousands, system failure)**
 - Change t network solution, voice over IP service were lost for 400 000 users. Basically the IMS became overloaded as a result of too many simultaneous registrations of customer devices. The provider had to limit registrations and was handling full traffic again after 14 hours.
- **Faulty upgrade halted IP-base traffic (hours, millions, human error)**
 - An upgrade in a core router went seriously wrong, and caused a drop of all IP based traffic for the provider causing many services to go down, including the emergency number 112. This incident led to an outage of 17 hours affecting 3 million users.
- **DDoS attacks on DNS affected mobile Internet (hours, millions, malicious attack)**
 - A series of Distributed Denial of Service attacks targeted a provider's domain name service. Up to 2,5 million mobile Internet users were affected during 1-2 hours.
- **Big storm affecting power supply causing large scale outage (days, millions, natural disaster)**
 - A severe storm hit several countries. The storm had a major impact on the power grid infrastructure and to a limited extent also on mobile network equipment (like mobile base stations). As a result around a million users were without mobile communication services for 24 hours, and in some cases up to two weeks.

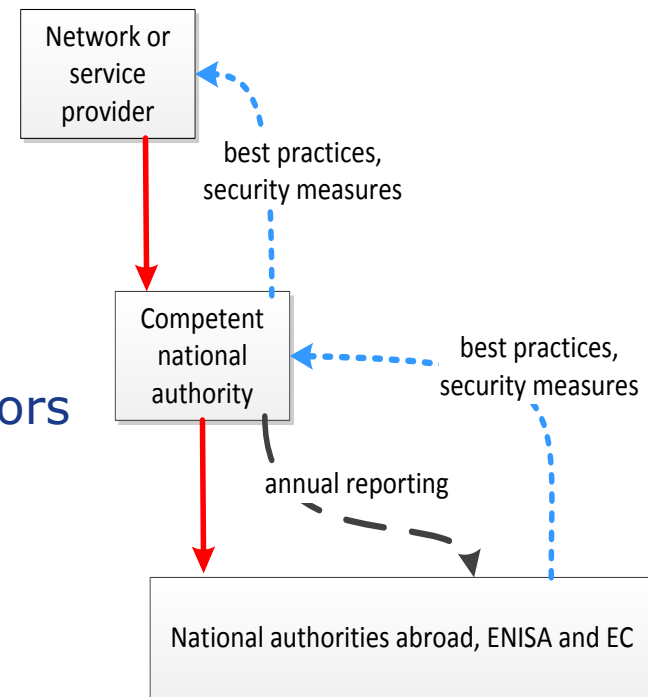
Hardware, software failures most common cause



Detailed causes (percentages per service)

From reporting to recommendations

- Update, issue recommendations on security measures together with Article 13a expert group and industry experts.
- In 2013 we are addressing two topics:
 - National roaming*
 - Power supply dependencies*
 - Resilience of interconnections
- In 2014 we plan to address
 - Dependencies on IT equipment/vendors
 - Audit training for regulators



*) these topics follow directly from the annual reporting



Proposed NIS 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



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

ENISA's activities on cloud security

- Supporting the EC
 - EU cloud strategy
 - EU cloud partnership
- Working with industry (CERT-SIG)
 - Transparency and trust
 - Role of cloud certification
 - Implementing legislation
- Listing cloud certification schemes
- Meta-model for cloud certification schemes and cloud security requirements
 - Facilitate cloud procurement



- 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? (anonymity/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?
 - IXPs, registries, registrars
 - Lower end of the cloud stack
- Role of certification and (external) audits
 - Soft, self-regulation?
 - Self-assessments?
 - Procurement guidelines/rules?
 - Impact on competition?



Contact us, work with us

Marnix Dekker marnix.dekker@enisa.europa.eu

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

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

