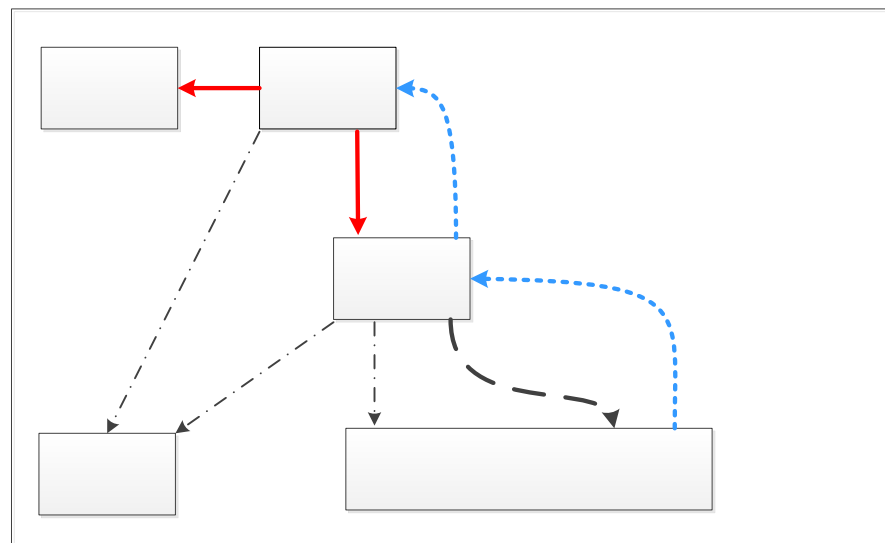




enisa Experiences from Article 13a

Dr. Marnix Dekker, ENISA

NIS Platform Plenary meeting
Brussels, December 11th, 2013



Structure of this talk

- Why NIS legislation?
- How did we support authorities in the implementation of Article 13a
 - Incident reporting framework
 - Security measures framework

Note: the ideas in this slide are based on discussions and consensus between regulators, using input from providers, over a period of several years of work.

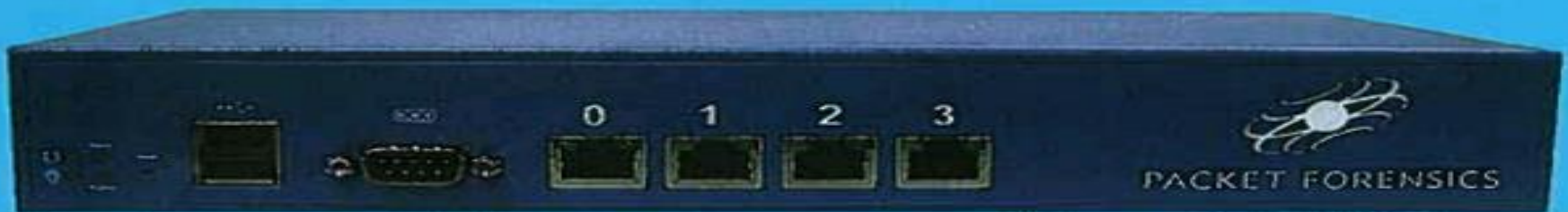
A close-up photograph of a field of dark purple tulips. The flowers are in various stages of bloom, with some showing deep purple petals and others more tightly closed. The green stems and leaves are visible, creating a vibrant contrast with the dark flowers. The background is a soft-focus green, suggesting a lush garden or field.

Summer 2011:
Diginotar aka Operation black tulip.



Background: HTTPS is it really working?

- Public key crypto is great! But PKI is poor.
 - The most widespread use of PKI is HTTPS.
 - HTTPS is neither user-friendly nor secure (600 SoFs).
 - 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 <http://blog.thoughtcrime.org/ssl-and-the-future-of-authenticity>: Do you even need to hack?
- Security failure and a market failure





For several weeks in August 20

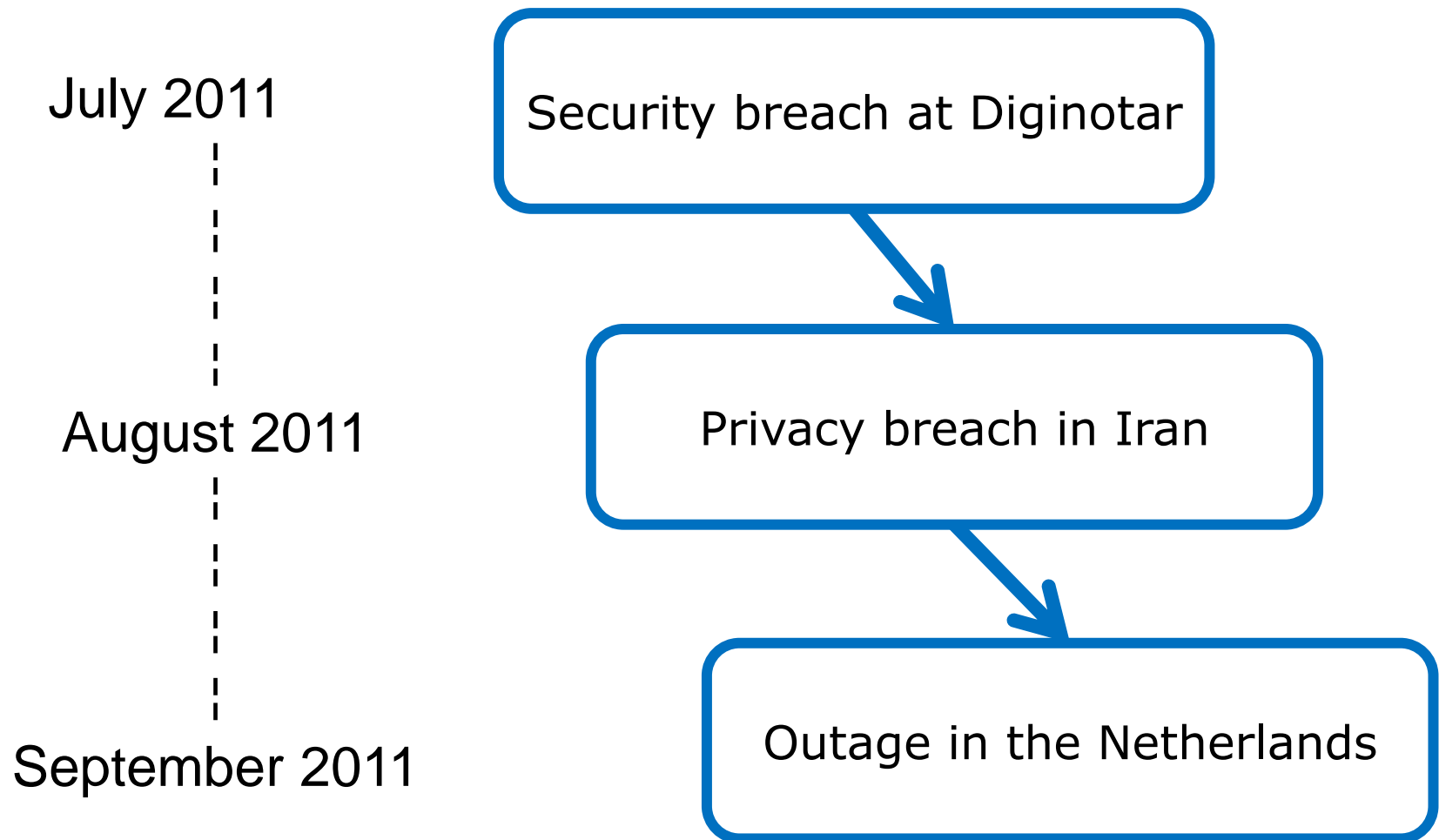
MitM on 300.000 Ira

For several weeks in September 2011

Dutch e-Government offline



Black tulip – impact timeline



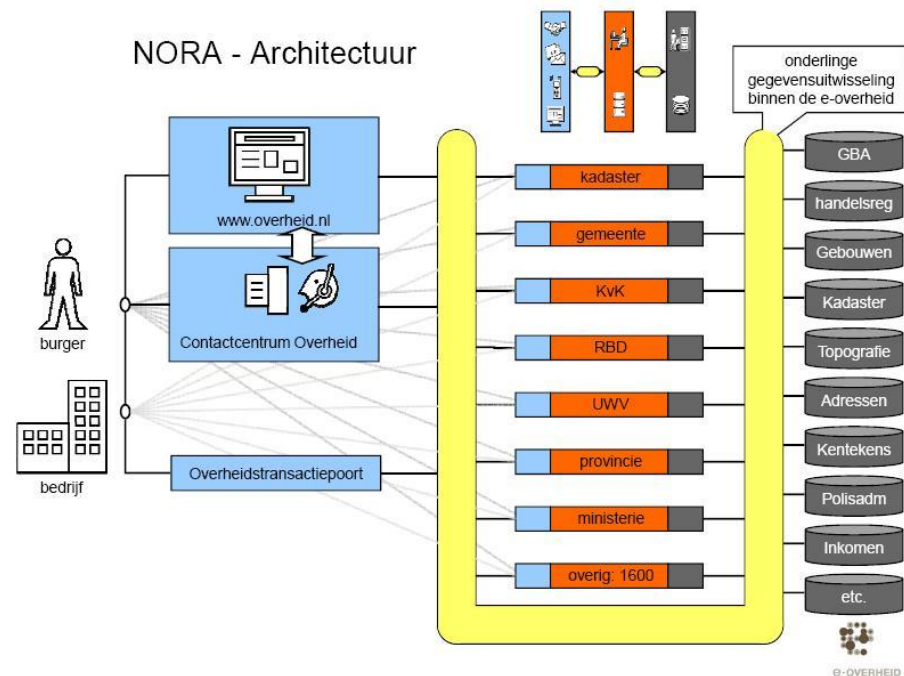


- Diginotar bankrupt, Vasco estimates losses at 4M euros

(Vasco acquired Diginotar for 12M,
Turn over certificate business of Diginotar is about 1M euros)

DigiD

Digitale
Identificatie



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

“It is plausible that people died.”

(Mikko Hyppönen, F-Secure)

... after the incident response?



Technical discussions following Diginotar

- CERT network worked well in the incident response phase
 - Aart Jochem (NCSC): “But PKI crisis is still ongoing”.
- Google removes OCSP from Chrome (‘snapping seatbelt’)
- More discussion about PKI and HTTPS
 - DNSSEC, DANE, Convergence, TACK, CA pinning
- ENISA criticises HTTPS and CAs
 - ☺ or rather “the implementation of HTTPS”



WILD WILD

- Vulnerabilities in the implementation of HTTPS.
- CAs can track internet usage of citizens.
- CAs get breached.
- CAs have no market incentive for improving security.
- Academics: "Security breach legislation (SBN) could help."

WEST

Political discussions following Diginotar

- No incident reporting obligations for Diginotar?
- Weak legal grounds for the government to intervene
 - Only because Diginotar was also a CA for qualified e-sig
- Case for international/EU action: Breach at a small firm in one country, had a severe impact abroad.
- Strong push for **legislation on information security**

CORBEYRON • MORENO

LE REGULATEUR

I - M - B - R - O - S - I - O



... fearsome legislation

... our "customers"



The Frog & The Scorpion.

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**

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 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.

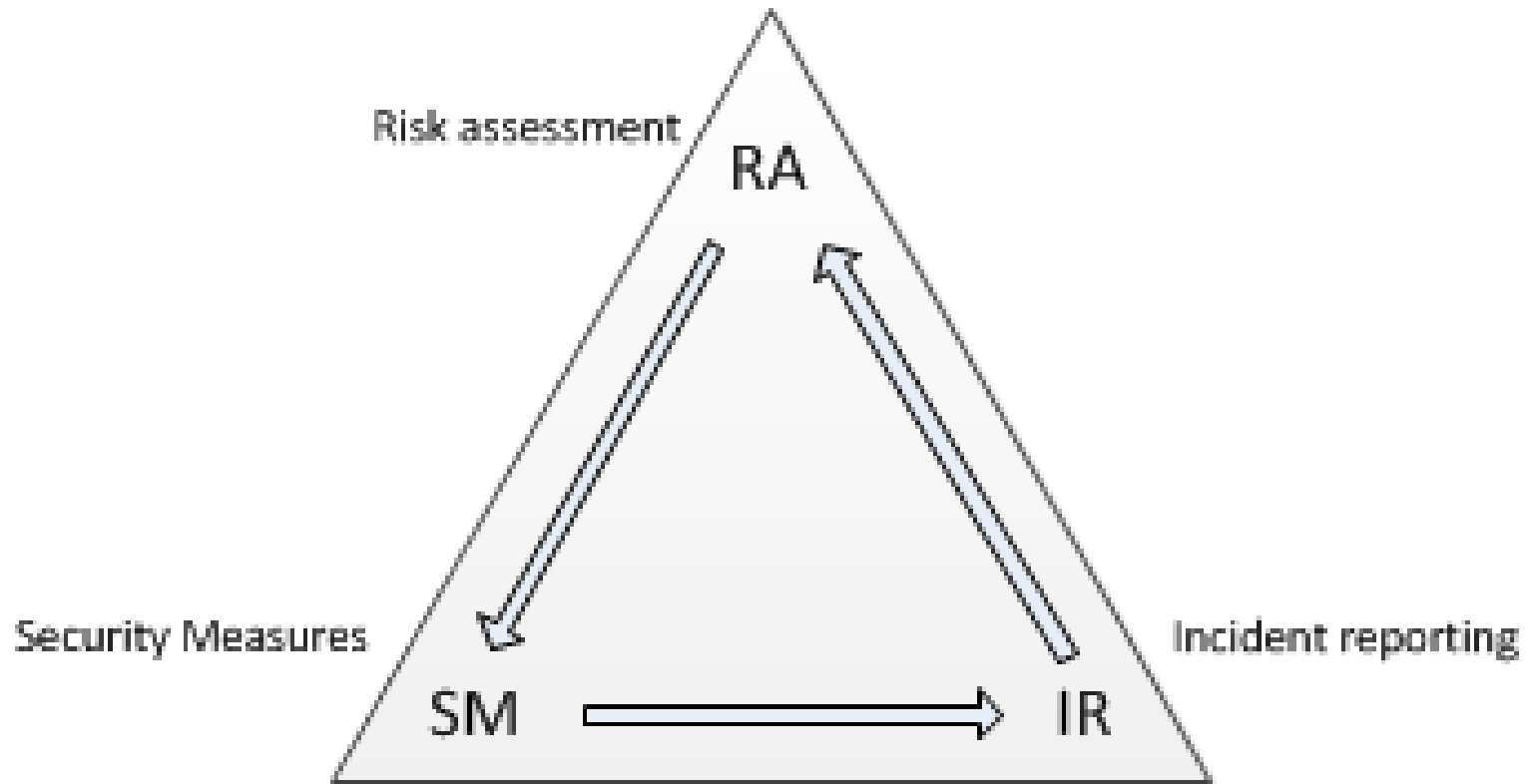
2. Member States shall ensure that undertakings providing public communications networks take all appropriate steps to guarantee the integrity of their networks, and thus ensure the continuity of supply of services provided over those networks.

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.

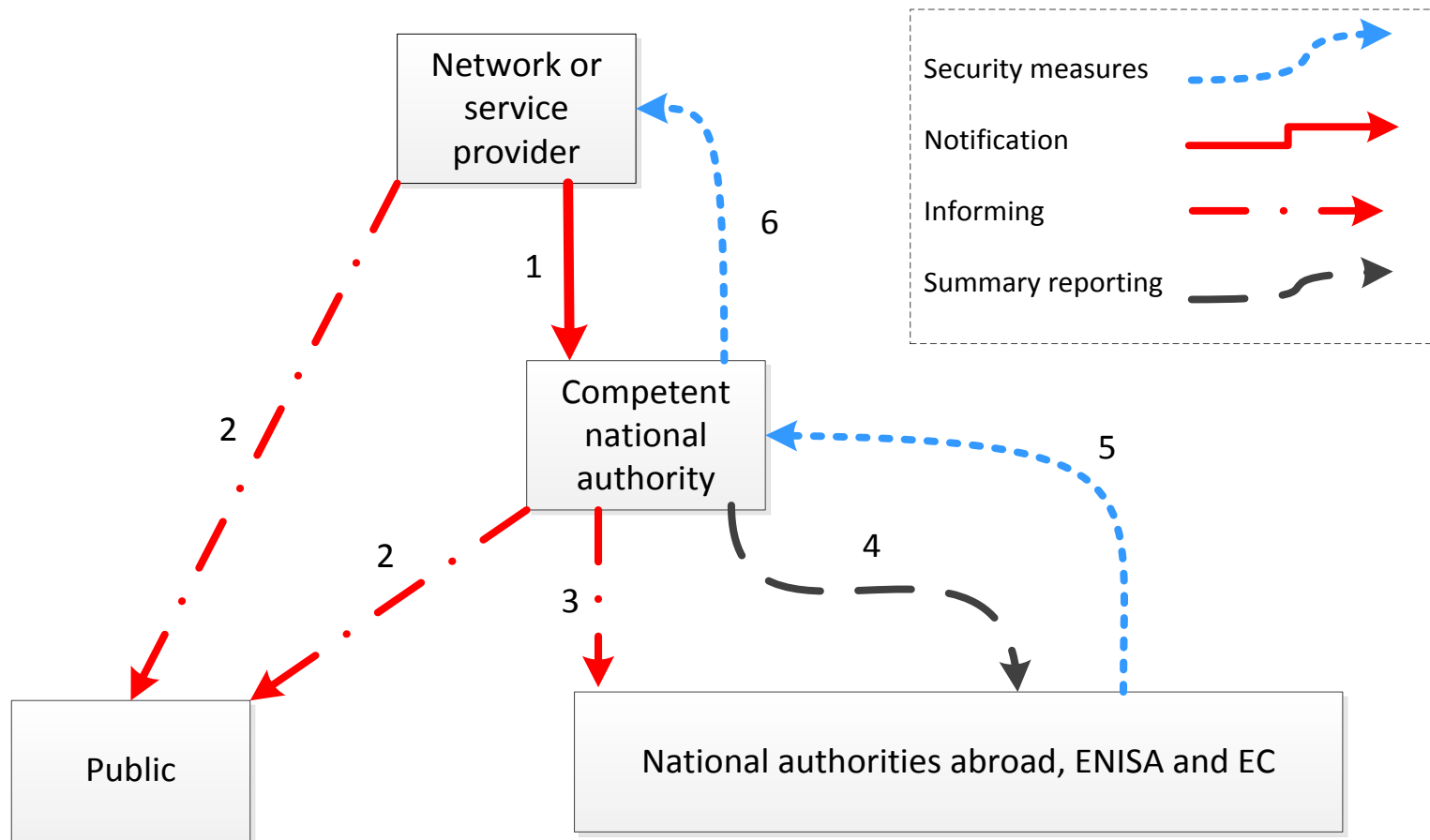
Once a year, the national regulatory authority concerned shall submit a summary report to the Commission and ENISA on the notifications received and the action taken in accordance with this paragraph.

Security processes mandated by Art13a



- Goal: Security of e-communication networks and services
- Supervised by a national regulator
(in collaboration with regulators abroad – the 'single market')

Information flows in Article 13a





-
- A word cloud visualization of the top 25 terms from the 2013-2014 Freedom of Information Act requests. The words are arranged in a circular pattern, with 'networks' and 'communications' being the most prominent. Other significant words include 'regulatory', 'security', 'measures', 'national', 'under', 'technical', 'information', 'breach', 'order', 'action', 'states', 'member', 'ensure', 'integrity', 'providing', 'take', 'appropriate', 'public', 'services', 'regulator', 'authorities', 'implementing', 'requirements', 'prevent', 'publicity', 'network', 'approach', 'european', 'taker', 'direct', 'available', 'concerned', 'article', 'taking', 'operation', 'advice', 'trinit', 'order', 'action', 'breach', 'order', 'operation', 'including', 'organisation', 'inquiry', 'may', 'regime', 'technical', 'information', 'national', 'under', 'measures', 'ensure', 'integrity', 'providing', 'take', 'appropriate', 'public', 'services', 'regulator', 'authorities', 'implementing', 'requirements', 'prevent', 'publicity', 'network', 'approach', 'european', 'taker', 'direct', 'available', 'concerned', 'article', 'taking', 'operation', 'advice', 'trinit'.

Article 13a Expert group members

Country	Art13a Incident Reporting	Art13a Security Measures	Art 4 Incident Reporting	Art4 Security Measures
Austria	RTR	RTR	DPC	DPC/RTR
Belgium	BIPT	BIPT	BIPT	BIPT
Bulgaria	CRC	CRC	PDP	PDP
Croatia	HAKOM	HAKOM	HAKOM	HAKOM
Cyprus	OCEPR	OCEPR	OCEPR	OCEPR/CPDP
Czech republic	CTO	CTO	OPDP/CTO	OPDP/CTO
Denmark	MINDEF	MINDEF	ERST	ERST
Estonia	TJA	TJA	AKI	AKI
Finland	FICORA	FICORA	FICORA	FICORA
France	MinFin	MinFin	CNIL	CNIL
Germany	BNetzA	Bnetza	Bnetza/BfDI	Bnetza/BfDI
Greece	ADAE	ADAE	ADAE/DPA	ADAE/DPA
Hungary	NMHH	NMHH	NMHH	NMHH
Ireland	COMREG	COMREG	DPC	DPC
Italy	MISE	MISE	GPDP	GPDP
Latvia	CERT.LV	CERT.LV	Data Inspector	Data Inspector
Lithuania	RRT	RRT	ADA	ADA
Luxembourg	ILR	ILR	CNPD	CNPD
Malta	MCA	MCA	OIDPC	OIDPC
Netherlands	Ag Telecom/ACM	Ag Telecom/ACM	ACM/CPB	ACM
Poland	UKE	UKE	GIODO	GIODO
Portugal	ANACOM	ANACOM	CNPD	ANACOM
Romania	ANCOM	ANCOM	ANSPDCP	ANSPDCP
Slovakia	TELEOFF	TELEOFF	TELEOFF	TELEOFF
Slovenia	APEK	APEK	APEK/IP-SR	APEK/IP-SR
Spain	Minetur	Minetur	AGPD	AGPD
Sweden	PTS	PTS	PTS	PTS
UK	OFCOM	OFCOM	ICO	ICO

Thresholds for annual summary reporting

- NRAs are gauging what are useful national thresholds.
 - Don't try to agree on what is significant impact (nationally)!
- Common thresholds for sharing with other NRAs
- Baseline + whatever else is 'interesting'

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



CIRAS: EC/ENISA view

CIRAS PILOT

Countries			
Country	Incident reports	Annual reports	Empty reports
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	1
view Atlantis	3	1	0
view Utopia	4	1	0
view Wonderland	11	1	0
view Fuego	2	0	0
view Crystalia	4	1	0
view Narnia	8	1	0
view Takatuka	7	1	0
view Tthaka	2	1	0

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
efthyco	Costas El

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.



CIRAS: Incident report form - impact

National ID

2013-14435245

Date

Year

2013 ▼

Service impact

<input type="checkbox"/> Fixed telephony	duration (hours) <input type="text"/>	number of users <input type="text"/>	<input type="checkbox"/> PSTN <input type="checkbox"/> DSL <input type="checkbox"/> Fiber <input type="checkbox"/> Cable <input type="checkbox"/> other
<input checked="" type="checkbox"/> Fixed internet	duration (hours) <input type="text" value="3"/>	number of users <input type="text" value="3.000.000"/>	<input type="checkbox"/> DSL <input checked="" type="checkbox"/> Fiber <input checked="" type="checkbox"/> Cable <input checked="" type="checkbox"/> other
<input type="checkbox"/> Mobile telephony	duration (hours) <input type="text"/>	number of users <input type="text"/>	<input type="checkbox"/> GSM <input type="checkbox"/> UMTS <input type="checkbox"/> LTE <input type="checkbox"/> other
<input type="checkbox"/> Mobile internet	duration (hours) <input type="text"/>	number of users <input type="text"/>	<input type="checkbox"/> GPRS/EDGE <input type="checkbox"/> UMTS <input type="checkbox"/> LTE <input type="checkbox"/> other
Service <input type="checkbox"/> <input type="text"/>	duration (hours) <input type="text"/>	number of users <input type="text"/>	

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.



CIRAS: Incident report form - causes

Root cause category

- ☐ System failures
- ☐ Human errors
- ☐ Malicious actions
- ☒ Natural phenomena
- ☐ Third party failures

Initial cause

- ☐ Cable cut
- ☐ Cable theft
- ☐ Flood
- ☒ 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

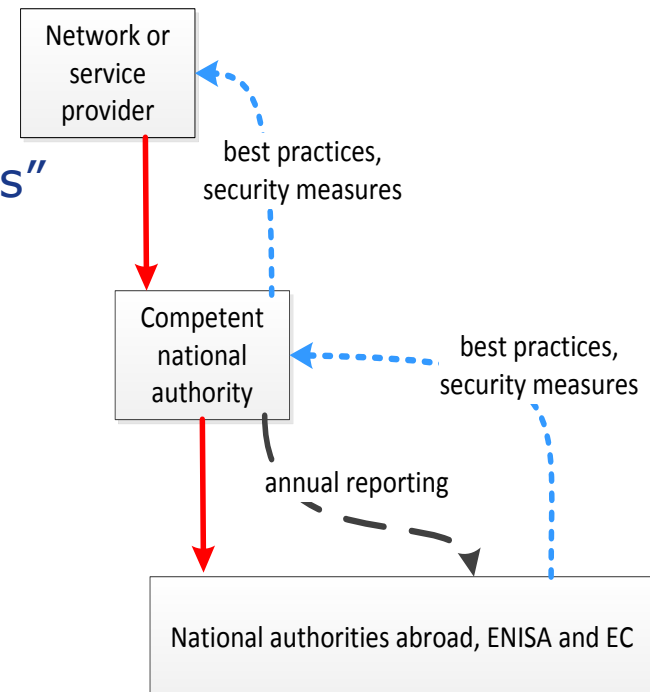
- ☐ Cable cut
- ☐ Cable theft
- ☐ Flood
- ☐ Heavy snowfall
- ☐ Storm
- ☒ Power cut
- ☐ Power surges
- ☐ Physical attack
- ☐ Cyber attack
- ☐ Bad change
- ☐ Bad maintenance
- ☐ Overload
- ☒ Fuel exhaustion
- ☐ Policy/procedure flaw
- ☐ Hardware failure
- ☐ Software bug
- ☐ Human error
- ☐ None
- ☐ No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

Assets affected by initial cause

- ☒ Base stations and controllers
(e.g. BTS, NodeB, RNC)
- ☒ 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)
- ☒ 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.)

Incident reporting as a means to an end

- Understand and discuss security issues
- Update and issue recommendations about security measures
- In 2013 two specific topics:
 - “National roaming for mobile outages”
 - “Power supply dependencies”
- In 2014 we plan to address
 - “Telecoms meet ICT vendors”

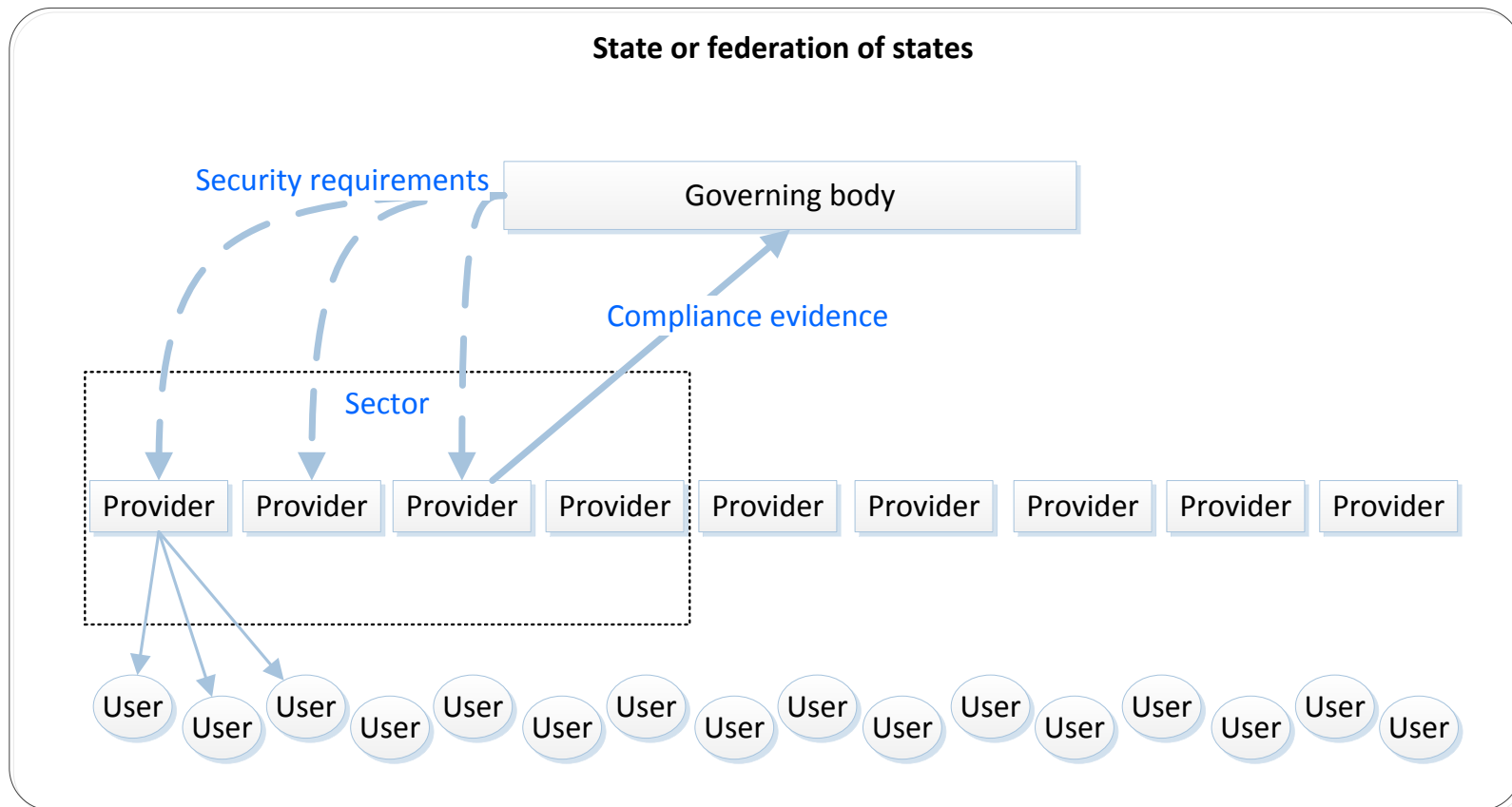


From one thing comes another

- Agreement about incident reporting template leads to agreement about
 - Which services are in scope (for now)
 - Which security incidents are in scope (for now)
 - Common terminology/vocabulary/metrics
 - Quantify/qualify impact of incidents
 - Categories of root causes (human error, natural disaster, etc)
 - Detailed causes (snow fall, power cut, overload, etc)
 - Assets (basestations, interconnections, MSC, HLR, etc)



*) These are all the main ingredients for a risk assessment (assets, threats)

Supervising security measures



Security is a dynamic field

- Rapidly changing technology and attacker capabilities
- Examples:
 - EU Carbon emissions trading scheme (30M euro)
 - High roller (80M euro)
 - Twitter account of Associated Press (143 Dow Jones pts)

In-depth security news and investigation


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



Average Antivirus detection rate (last 60 days)
Average Antivirus detection rate: 38.4%

Source: zeustracker.abuse.ch

Recent Posts

- Adobe Breach
- 38 Million Users
- Senator Dem Experian
- Experian Sol ID Theft Service
- Breach at PR
- Adobe Hack
- Critical Java Security Hole

Subscribe to

Appropriate security measures

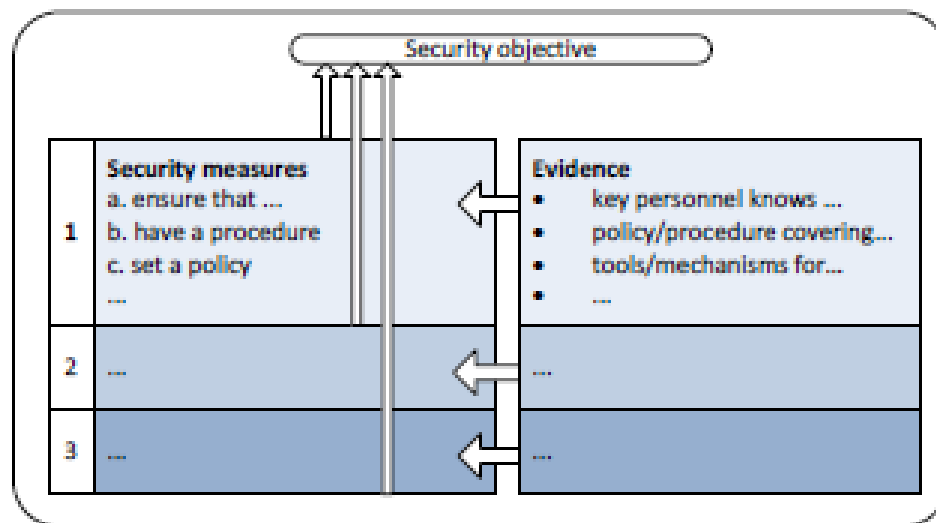
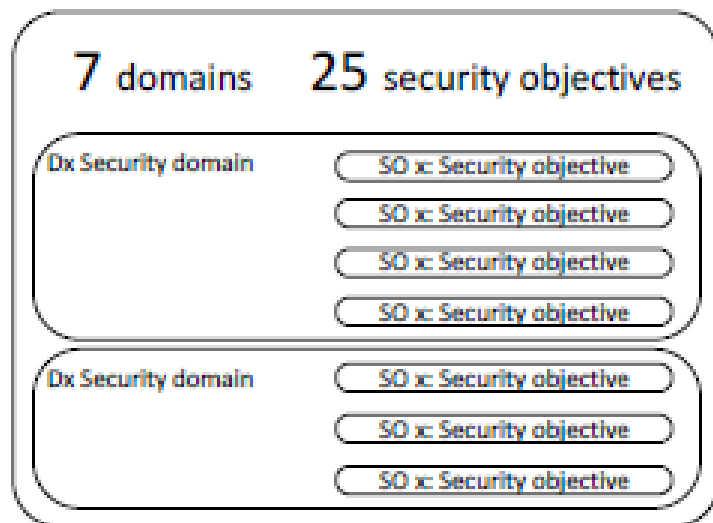
- Appropriate, proportionate, commensurate to the risks
 - Risks for customers, society, et cetera (so enterprise risk mgmt frameworks are not fully applicable)
 - NRA is not the asset owner and cannot do the risk assessment
 - Technology changes rapidly (IP etc)
 - The sector is very diverse (per country 100s of providers)
- Hard: NRA defines up front which are the appropriate security measures.
- Feasible: Try to move the sector **faster forward**
 - Use examples and best-practices from industry frontrunners
 - Assess, compare, analyse and support best practices
 - Analyse incident reports and follow-up



... like curling

Guideline on Security Measures

- Neutral standard/structure
- Adopted by most national authorities
- Structure for supervision, not a security manual
 - For self-assessments, interviews, questionnaires
 - Mapped to international standards



Guideline on 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

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.

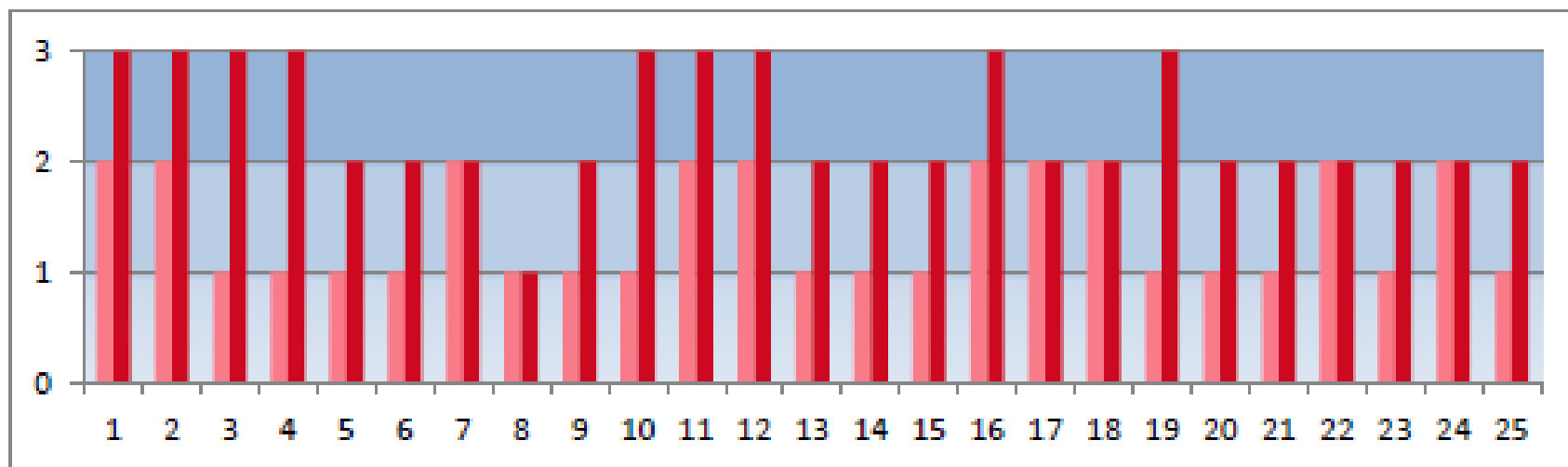
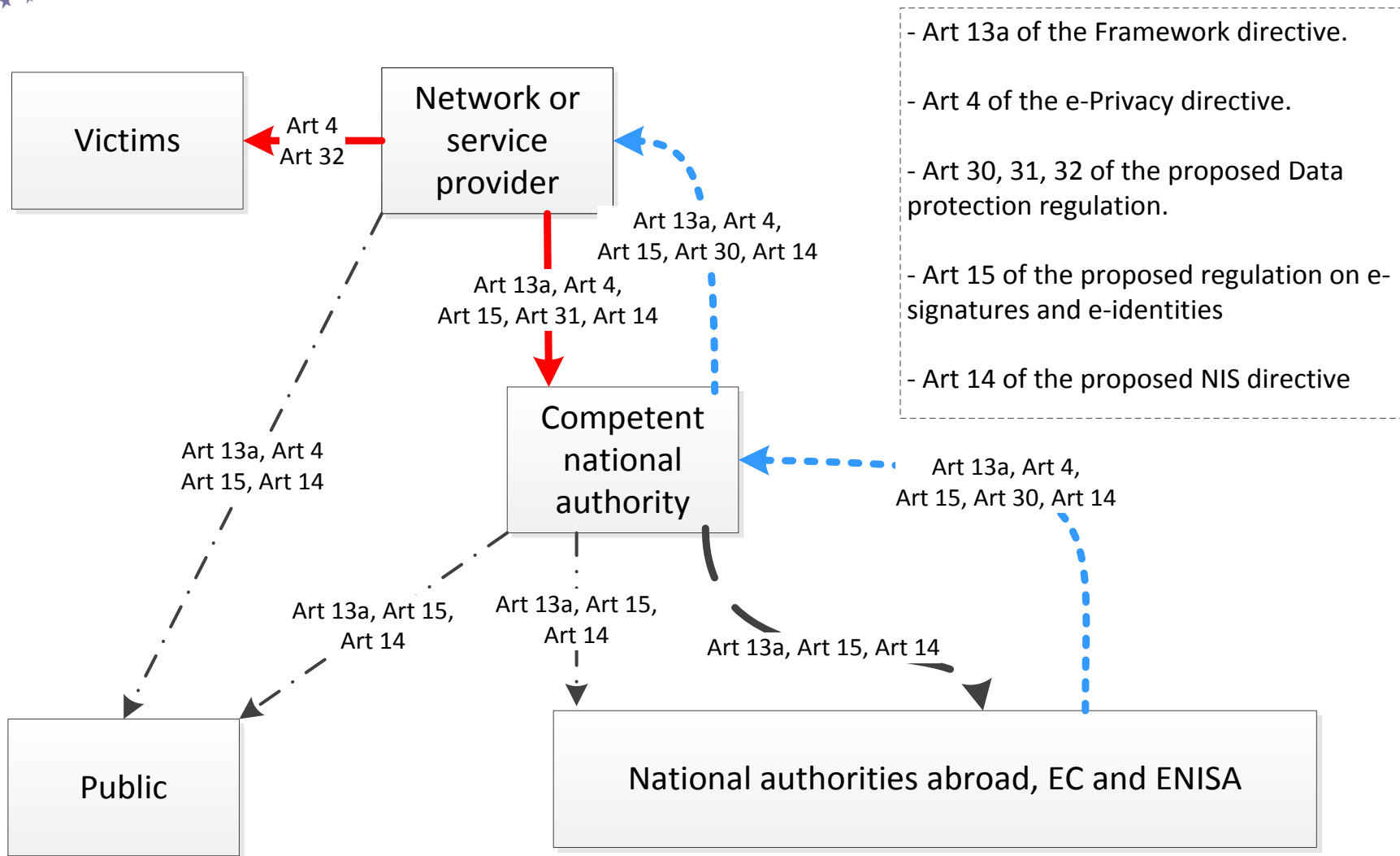


Figure 1: Two different profiles with varying sophistication for different security measures.

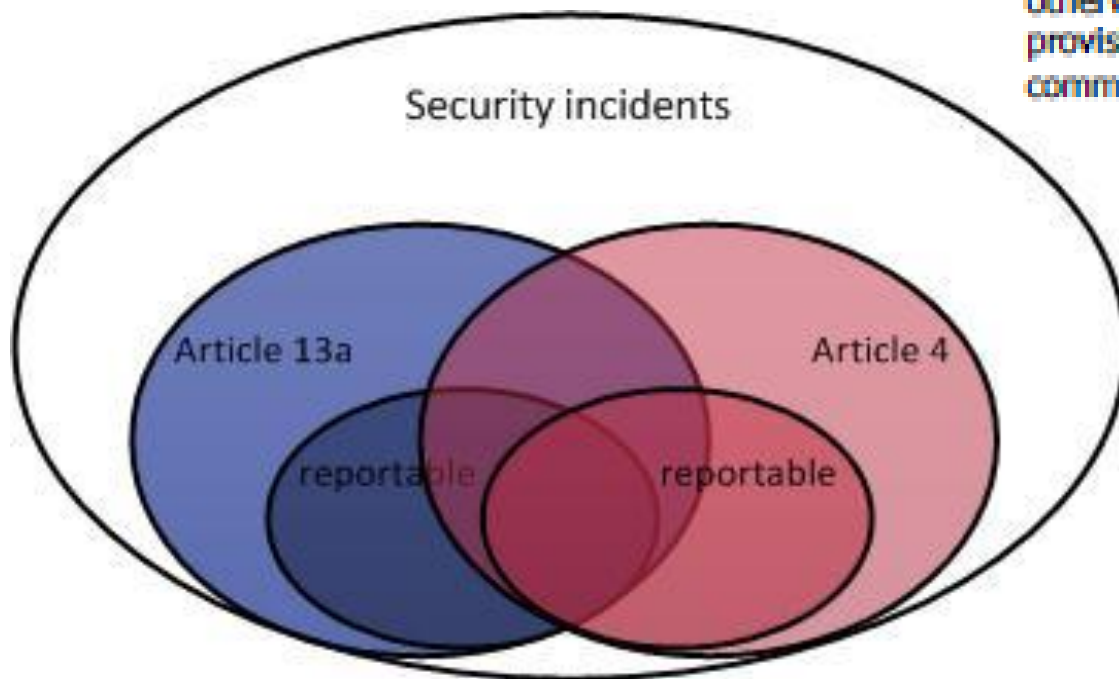
Security breach articles in EU legislation



Security and personal data

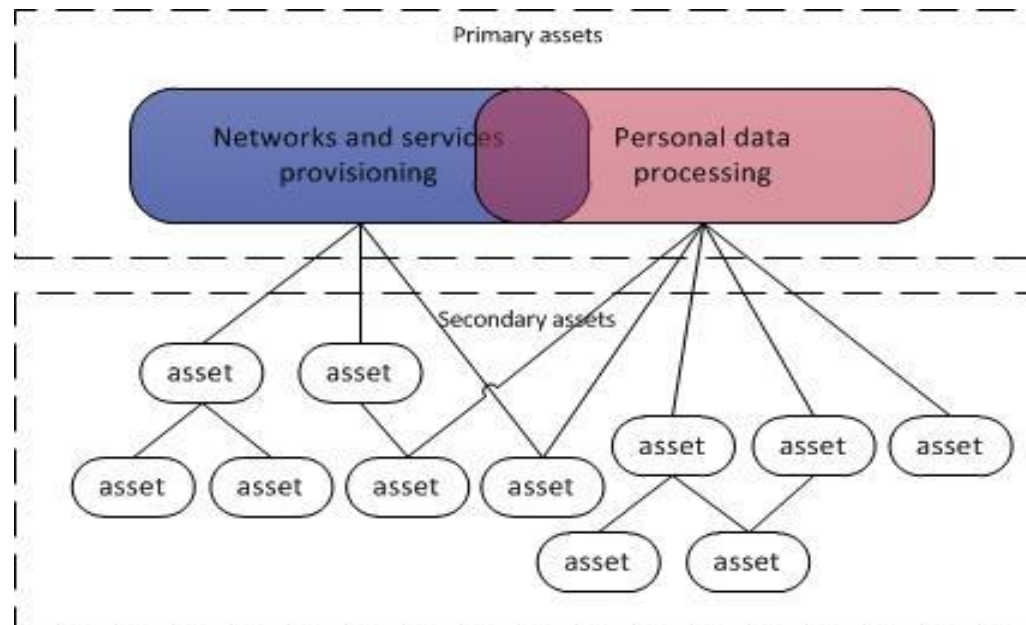
- Article 13a: Security of services and networks
- Article 4: Security of personal data processing

'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.



Proposal for One security framework

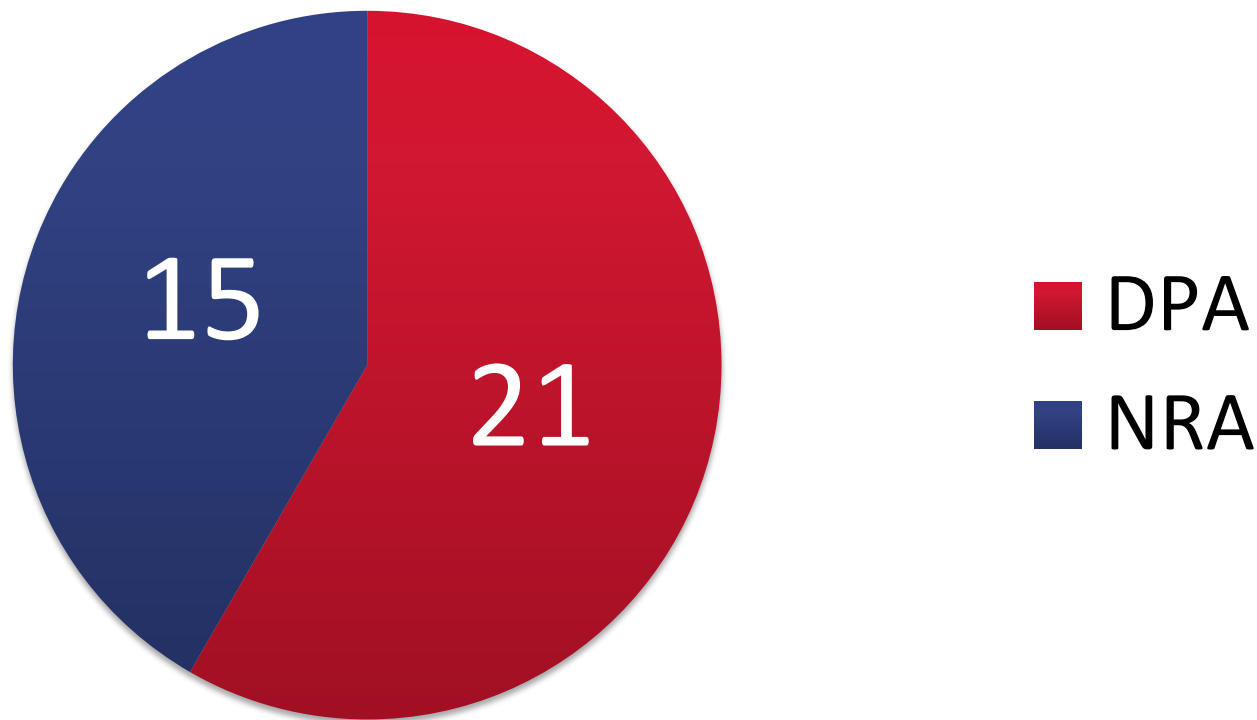
- “probably 80% overlap in measures”
- Merged Art4 and Art13a: “Security of networks, services and personal data processing”
- Easier for providers
- Easier cooperation between authorities nationally
- Easier cooperation between authorities across borders





Personal data breaches: a joint responsibility

Authorities on 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

Harmonization across regulators

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 ... two scorpions

Article 13a Rules of thumb



- Regulator is not the asset owner
 - NRA cannot do a detailed risk assessment
- Countries, markets and regulators are different
 - No single definition of 'significant' incidents
- One size does not fit all
 - Accommodate for the diversity in the sector
- Collection of incident reports drives the supervision (nationally)
- Security measures are voluntary
 - Provide guidance for small providers but avoid setting a minimum.
- Pan-EU sharing (summaries of) incident reports drives collaboration and harmonization.
 - Exchanging experiences and learning from other countries.
 - Agreement on common terminology/vocabulary and approach.
- Start pan-EU collaboration with an reduced/imperfect scope
 - a short list of services, a shortlist of types of incidents
- Identify and reap added value for the job at hand (security)

Article 13a Open 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? (anonymity/immunity for reporters, fines/sanctions for not reporting –not for incidents, Corporate culture , return value)
 - Sharing lessons learnt! (or when to look beyond competition?).
- Times of change
 - From telegraphs and telephony to PCs and smartphones?
 - Services in scope? Blackberry, social media, cloud computing, Skype, Whatsapp?
 - IXPs, registries (DNS, BGP), registrars, et cetera.
 - Lower end of the cloud stack (IaaS)
- Role of standards, certification and (external) audits
 - Soft, self-regulation?
 - Self-assessments?
 - Procurement guidelines/rules?
 - Impact on competition?



Contact us, work with us

Article 13a material

- Article 13a EG portal and draft guidelines: <http://resilience.enisa.europa.eu/article-13>
- Article 13a video: <http://www.enisa.europa.eu/media/multimedia/reporting-of-cybersecurity-incidents>
- Article 13a annual reports: <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2012>

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