EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT A
ECONOMIC AND SCIENTIFIC POLICY

Economic and Monetary Affairs

Employment and Social Affairs

Environment, Public Health and Food Safety

Industry, Research and Energy

Internal Market and Consumer Protection

Data and Security Breaches and Cybersecurity Strategies in the EU and its international counterparts

NOTE

EN

2013

Data and Security Breaches and Cybersecurity Strategies in the EU and its international counterparts

EUROPEAN PARLIAMENT

DIRECTORATE GENERAL FOR INTERNAL POLICIES
POLICY DEPARTMENT A: ECONOMIC AND SCIENTIFIC POLICY
INDUSTRY, RESEARCH AND ENERGY

Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts

NOTE

Abstract

This long briefing provides an overview of the definition of security incidents and breaches and an analysis of their scale and trends. We summarise the current EU-level efforts to address network and information security, review some of the provisions of the Commission's 2013 proposals for a Network and Information Security Directive and offer recommendations. We have some potentially major concerns including the relationship of incident notification achieving the outcomes of the directive, potential for overlapping regulation and definitions of covered entities. We also suggest that it would be helpful to clarify what kind of incidents the Directive is aimed to address.

IP/A/ITRE/NT/2013-5 September 2013

PE 507.476 EN

This document was requested by the European Parliament's Committee on Industry, Research and Energy

AUTHORS

Mr Neil Robinson (RAND)
Ms. Veronika Horvath (RAND)
Prof Jonathan Cave (RAND)
Dr Arnold P. Roosendaal (TNO)
Dr Marieke Klaver (TNO) (as reviewer)

RESPONSIBLE ADMINISTRATOR

Balazs Mellar
Mariusz Maciejewski
Fabrizio Porrino
Policy Department Economic and Scientific Policy
European Parliament
B-1047 Brussels
E-mail: Poldep-Economy-Science@europarl.europa.eu

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

To contact the Policy Department or to subscribe to its newsletter please write to:
Poldep-Economy-Science@europarl.europa.eu

Manuscript completed in September 2013.

This document is available on the internet at: http://www.europarl.europa.eu/studies

DISCLAIMER

CONTENTS

LIST OF ABBREVIATIONS

ACDC	Advanced Cyber Defence Centre
ACLU	American Civil Liberties Union
APT	Advanced Persistent Threat
APWG	Anti-Phishing Working Group
CA	Competent Authority
CEPOL	European Police College
CERT	Computer Emergency Response Team
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CISPA	Cyber Intelligence Sharing and Protection Act
CLUSIF	Club de la Sécurité de l'Information Français
CSIRT	Computer Security Incident Response Team
CSOC	Cyber Security Operations Centre (AUS)
DDoS	Distributed Denial of Service
DPA	Data Protection Authority
EC	European Commission
EC3	European Cybercrime Centre
ECTEG	European Cybercrime Training and Education Group
EDPS	European Data Protection Supervisor
EFMS	European Forum for Member States
ENISA	European Network and Information Security Agency
EP3R	European Public–Private Partnership for Resilience

EuroSCSIE	European Supervisory Control and Data Acquisition and Control Systems Information Exchange
FTE	Full-time Equivalent
GCHQ	Government Communications Headquarters (UK)
GDP	Gross Domestic Product
HIPAA	Health Insurance Portability and Accountability Act
IAB	Impact Assessment Board
ICT	Information and Communication Technology
ISAC	Information Sharing and Analysis Centre
ISBS	Information Security Breach Survey
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITRE	Industry, Research and Energy
MS	Member State
NATO	North Atlantic Treaty Organization
NCSC	National Cyber Security Center (NL; SK)
NERC	National Electric Reliability Council (US)
NIS	Network and Information Security
NIST	National Institute for Standards and Technology (US)
OCSIA	Office of Cyber Security and Information Assurance (UK)
OECD	Organisation for Economic Co-operation and Development
OSCE	Organisation for Security and Co-operation in Europe (OSCE)
PII	Personally Identifiable Information
PPP	Public–Private Partnership

SEC Securities and Exchange Commission (US)

SIR Security and Intelligence Report

SME Small and Medium-sized Enterprise

TISN Trusted Information Sharing Network (AUS)

TLD Trust in Digital Life

UN United Nations

WARP Warning, Advice and Reporting Point

LIST OF TABLES

LIST OF FIGURES

EXECUTIVE SUMMARY

In February 2013 the European Commission presented its 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'[1] (hereafter: proposal for a NIS Directive), which accompanied the EU's cyber-security strategy. These proposals contain a number of measures to strengthen EU efforts in tackling cyber security. The measures include creating a system for the reporting of security incidents similar to that which currently applies to telecommunications providers under Article 13a of the 2009 Telecommunications Framework Directive. This incident reporting system would apply to other critical infrastructure sectors: energy, transportation, financial services, healthcare providers, but also market operators in the 'internet economy'. The proposal for a NIS Directive also requires that at the Member State level, each EU Member State should have competent authority (CA) and a national level computer emergency response team (CERT). Each CA should be part of a pan-European secure communications network to permit the sharing and exchange of cyber-security-related information (including incident reports).

What are security incidents and data breaches and how do they occur?

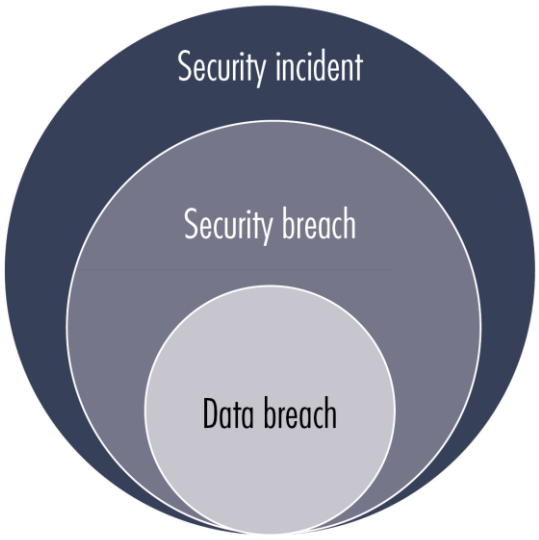
There are a range of definitions applying to categories of security incident, data breach and cyber attack. Some of these are based on definitions from the International Organization for Standardization (ISO), legislation in areas such as data protection and other guidance. Consistent and unambiguous legal definitions are often lacking, however.

Incidents can have a variety of root causes, including environmental conditions, such as: storms or floods, human error, malicious attacks, hardware or software failures, and third party failures. Security breaches are usually defined when there has been a demonstrated compromise of a security policy and are often associated with incidents of a malicious nature. A data breach takes place when there is an impact related to the data (in the sense of personal data), such as the data being lost or illegitimately accessed, and effects have repercussions not only on the security of the system but also on the right to the protection of personal data of the individual affected.

Figure 1 shows the relationship of security incidents to security and data breaches.

[1] European Commission, 2013a.

Figure 1 The relationship of security incidents to security and data breaches (Source: RAND Europe)



Who is affected and where?

In the absence of reliable comparable data on the incidence and targets of information security incidents and breaches, we surveyed the available information sources. We found a general picture of an increase in visibility of different types of incidents. This may be due to actual increasing prevalence or to more truthful reporting or other biases.

Overall, the trend in both attacks (as captured by data from cyber-security companies) and incidents (as shown by surveys) appears to be on the rise across IT-related categories of intrusion. While a significant proportion of EU companies (12% overall) reported having suffered incidents involving the failure of hardware or software, this does not appear to translate to a similarly high incidence of data breaches for these reasons. Where available, the proportion of data breaches that occurred for environmental reasons or following physical disruption appears to be much less severe than breaches due to human error or malicious attacks.

As a general analysis, extrapolating from 2013 data, we estimate that, *at a minimum*, the direct costs to all enterprises (except micro-enterprises) of those types of security incident with malicious motivation (excluding accidents and failures) is at least €935m. Including hardware and software failure, this rises to €4.15bn.[2]

According to Eurostat, the level of preparedness for a security incident with malicious motivation of European companies (using the existence of an ICT security plan as proxy for preparedness) in sectors excluding the financial sector is much lower than in the financial sector, where up to 90% of companies has such a plan. However, in all sectors there are large discrepancies across countries regarding the extent of preparedness.

Where we have information of the incidence of information security breaches (e.g. in the UK), we see that larger companies tend to report larger numbers of breaches. This phenomenon could potentially be a result of these companies benefitting from better detection and reporting capabilities, e.g. larger IT security staff, or they experience a larger number of attacks to begin with.

[2] Based on Eurostat data.

At the same time, individual attacks could have important effects on small companies, in particular where they comport business disruption.

How is Europe currently managing these problems?

Understanding how co-ordination and co-operation is achieved in the European cyber-security policy puzzle is very complex. No-one currently has a clear understanding of how all the different pieces fit together. There are many institutions, each working on a specific part of the problem. The European Network and Information Security Agency (ENISA) has been strengthening its efforts with CERTs and formulation of practical guidance on implementing Article 13a but lacks links with the end-user community. The future of the European Public–Private Partnership for Resilience (EP3R) is uncertain, especially its potential interaction with the recently announced NIS platform. The European Forum for Member States (EFMS) has been instrumental in formulating guidance for Member States to operate the incident notification regime under Article 13a of the Framework Directive. The European Cybercrime Centre has been established since 2013 and will become fully operational in 2014. It is planning discussions with market players active in reporting cyber crime on the internet. A number of other organisations in the public and private sector (such as the CERT-EU, the European Cybercrime Training and Education Group (ECTEG), Trust in Digital Life public–private partnership, the Advanced Cyber Defence Centre (ACDC) initiatives and global CERT peer networks) have varying levels of capability and capacity with regard to responding and dealing with the consequences of incidents.

In addition to those organisations covered above, there are a number of other entities that somehow play a role in responding to and managing facets of the cyber-security incident problem. These include public–private partnerships (PPPs) such as the European Security of Control Systems Information Exchange (EuroSCSIE), the 2CENTRE network (which aims to facilitate research, training and education concerning tackling cyber crime) and numerous non-government initiatives such as training for computer incident emergency response teams (TRANSITs). Furthermore, our description above has focused on EU-level interactions but the EU both participates in and invites participation from relevant external organisations and initiatives formally and informally, including those of the UN, Organisation for Economic Co-operation and Development (OECD), the Group of Eight countries and NATO.

Are there relevant cyber-security practices elsewhere?

In Europe there are few relevant examples. In the Netherlands a public consultation[3] was opened on 22 July 2013 on a draft 'Breach Notification Bill' (*Wet melding inbreuken elektronische informatiesystemen*), which makes it mandatory to notify security breaches or losses of integrity of vital ICT systems.[4] On notification to the Minister of Security and Justice the incident is examined by the National Cyber Security Center (NCSC).

Looking at incident reporting mechanisms from further afield, we see that many countries have adopted voluntary incident reporting mechanisms in areas of critical infrastructure, with some mandatory systems only applying to public notification systems involving breaches of personal data. Most of the security incident reporting systems are closed (are just between critical infrastructure owner-operators and government) although not without controversy.

[3] http://www.internetconsultatie.nl/meldplicht_ict_inbreuken

[4] Wet houdende regels over het melden van een inbreuk op de veiligheid of een verlies van integriteit van elektronische informatiesystemen die van vitaal belang zijn voor de Nederlandse samenleving (Wet melding inbreuken elektronische informatiesystemen), Memorie van Toelichting, p. 1.

For example, the US Executive Order of 2013 sets up a system of voluntary information sharing of cyber-security data between government and critical infrastructure owners. The US NIST Cybersecurity Framework will create a set of tools that organisations can use to help meet the goals of the Executive Order. Data breach notification laws (specifically covering the notification of losses of personally identifiable information) are also becoming increasingly common.

After analysis of relevant cyber-security practices from other countries, we find that a cyber-security incident reporting regime in India is the closest comparator to that described in the proposal for an NIS Directive. The measures set out in the draft Indian National Cyber Security Policy are similar to those contained in the Commission proposal for a NIS Directive insofar as the Indian system is mandatory; it includes a broad range of internet intermediaries, is a closed reporting system (does not impose disclosure to affected persons), and covers a range of types of incident. Although we found many grassroots, operational and technical information exchange and information sharing mechanisms, there appear to be very few comparable mechanisms for security incident notification for sectors like 'enablers of information society services' as identified in the proposal for a NIS Directive. Among the systems already in place, the study has identified only the Indian example as comparable.

Within the context of the evidence in this report, the incident reporting mechanism described in the proposal for an NIS Directive is thus the only regime encompassing a broad security incident reporting mechanism except for that in India. There are four unique features to the proposal for an NIS Directive:

- its inclusion of internet enablers as a sector
- the extension of security incident reporting for cyber-security incidents to critical infrastructure sectors that so far remain generally unaffected by EU critical infrastructure legislation
- a broad understanding of a variety of security incidents as the types of phenomena to be reported
- its mandatory reporting nature compared with voluntary or informal systems covering critical infrastructure in other countries.

Given the unique institutional complexity of the EU, 'like for like' comparisons with national regimes are undoubtedly difficult and so care should be taken with these comparisons. The institutional mechanisms of EU policy making are somewhat unique, which makes it difficult to identify best practices from other national contexts that it might be fruitful to consider.

What are the potential pitfalls with the proposals for a NIS Directive?

The policy interventions in the proposal for a NIS Directive appear somewhat disproportionate in their interplay with other issues and their costs and benefits.

In some areas the proposal is unambitious and in others very ambitious. The proposals may also be regarded as somewhat unbalanced as they emphasise hard policy rather than private sector initiatives (for example they fail to acknowledge the role of managed security service providers in the collection of incident data). This possibly stems from a perception of the unwillingness of the private sector to address cyber security over the last few years of policy development.

Establishing mandatory reporting while encouraging firms to take up risk analysis seems paradoxical because risk analysis for cyber security is highly context dependent and what may be a significant risk for one organisation (thus passing a threshold for notification) could be trivial for another. Table 1 lists the major potential pitfalls associated with the proposal for a NIS Directive.

Table 1 The major potential pitfalls associated with the proposal for a NIS Directive

	Potential pitfalls
1.	Uncertainty over the benefits of public disclosure versus private notification with regards to security incidents and data breaches
2.	Vague understanding of public–private partnership
3.	Centralising effects may cause divergence in implementation
4.	Regulatory duplication
5.	Proposed mandates of CAs and CERTs encourage a reactive and technical focus to incidents
6.	Additional reporting requirements might lead to fragmentation of consideration of risk and poor outcomes for cyber security
7.	Conservative understanding of current approaches to implementing cyber security in SMEs would cause inefficiencies
8.	Little attention given to other stakeholders that collect and process incident information on behalf of customers
9.	Multiple reporting mechanisms create additional burdens
10.	Obligations fall on those most likely to be doing something
11.	Regulation of internet economy enablers is without precedent

What recommendations might improve the proposals?

In Table 2 we present several recommendations aimed at addressing the challenges with the proposal for a NIS Directive as it stands, in order of importance.

Table 2 The main recommendations of the study

	Recommendations	Responsible
1.	Strive for transparency in the EU policy framework for cyber security.	
2.	Make reporting voluntary not mandatory.	European Commission; European Parliament; European Council
3.	Exploit and strengthen existing information sharing channels.	European Commission (DG CNECT and ENISA)
4.	Elaborate and expand a role for sector-specific regulators with a particular focus on building and exploiting existing information sharing channels, especially for the highly regulated sectors of critical infrastructure.	European Commission (DG CNECT and relevant other DGs, e.g. DG HOME; DG MOVE); European Parliament; Member States
5.	Formulate use of guidance as part of stock market listings to encourage good security behaviour by publicly listed firms.	European Commission (DG MARKT; DG CNECT); European Central Bank
6.	Create a suitable trusted information sharing mechanism for internet enablers.	ENISA
7.	Modify the Article 13a regime to cover critical infrastructure only and broaden its scope (not only covering include security incidents that result in outages).	European Commission (DG MARKT; DG CNECT)
8.	Create an informal trusted information sharing mechanism for public administrations.	European Commission; European Council; Member States
9.	Engage SMEs though chambers of commerce and grassroots cyber-security initiatives such as warning, advice and reporting points (WARPs).	ENISA; EuroChambres
10.	Leverage international practice in implementation guidance.	ENISA; European Commission (DG CNECT)

1 INTRODUCTION

In February 2013 the European Commission presented a proposal for a directive of the European Parliament and the Council concerning measures to ensure a high common level of network and information security across the Union[5] (hereafter: proposal for a NIS Directive), in tandem with the EU's cyber-security strategy. The proposal for a NIS Directive contains a number of proposals to strengthen EU efforts to tackle cyber security. These include extending the provisions of reporting security incidents currently limited to telecommunications providers under Article 13a of the 2009 Framework Directive (FWD) to other critical infrastructure sectors: energy, transport, finance, health and the 'internet economy'. The proposal for a NIS Directive also requires that at the Member State level each EU Member State should have a national or governmental computer emergency response team (CERT) and competent authority (CA). Each CA should be part of a secure pan-European electronic data interchange network to permit the sharing and exchange of cyber-security-related information (including incident reports).

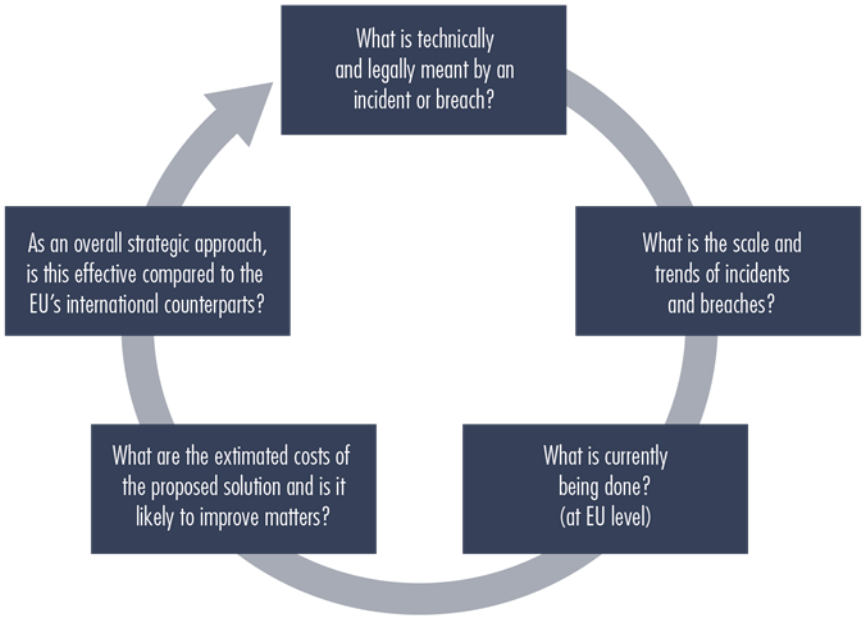
Scrutiny and interest in the proposals has understandably been very high since they were released. The Industry, Research and Energy (ITRE) Committee of the European Parliament asked for:

- a definition of terms like incident, breach etc
- a definition of the entities covered in the proposals, including an assessment of market operators
- an analysis of facts and figures relating to breaches and incidents across Europe and selected international counterparts
- a list of the achievements and results of the main EU-level institutions relevant to cyber security
- an assessment of the overall costs of the proposal for a NIS Directive, including the establishment of a CERT and a pan-European co-ordinated NIS national authority (CA) network and taking into account compliance costs for public and private actors
- identification of the most cost effective, innovative and competitive cyber-security practices.

These questions can be related to the steps in a cycle outlined in Figure 2.

[5] Ibid.

Figure 2 Framework for the study



1.1 Our methodology

The sources used included available scholarly and 'grey' (policy, industry) documents and quantitative evidence, supplemented by the expertise of the study team.

We have taken a very straightforward research approach: general desk research; analysis of data on security incidents from a number of sources; and broad assessment of costs from readily available open-source data. We emphasise security incidents[6] and breaches over personal data breaches (although the two are related). We have also undertaken general background desk research into incidents via sources collectively known to the study team and through hand searching of two databases: Google Scholar[7] and the Digital Library of the Association of Computing Machinery[8] using the terms: 'security incident', 'security breach' and 'data breach'. We reviewed the abstracts of the first 20 hits to determine relevance of articles.

1.2 Structure of this report

Chapter 2, the next chapter, reflects our understanding of the terminology and its legal basis. Chapter 3 presents data on trends: incidents, breaches, levels of security and costs of incidents. Chapter 4 discusses how the current response is established at European level. Chapter 5 sets out the proposed improvements to the set up encapsulated in the NIS Directive with a specific focus on incidents and breaches. Chapter 6 discusses best practice with reference from practice overseas, while Chapter 7 critically analyses the proposal for a NIS Directive. Finally, Chapter 8 presents recommendations.

[6] We are aware that incident reports are not the same as incidents. First, they may be subject to temporal clustering caused by the attacker or defender 'arms race' (new exploit -> many incidents -> effective response -> hiatus; repeat cycle). Second, reports alone cannot capture all important characteristics such as motivations, methods used, different probabilities of detection, incentives to report and the effectiveness of passive, active and specific countermeasures, all of which should be taken into account when drawing inferences from these data about the true incidence, prevalence and impacts of cyber threats.

[7] Google Scholar: http://scholar.google.com

[8] ACM Digital Library: http://dl.acm.org/

2 WHAT ARE SECURITY INCIDENTS AND DATA BREACHES AND HOW DO THEY OCCUR?

KEY FINDINGS

- Understanding what constitutes an incident or breach can be technically challenging; therefore the available definitions used by different actors overlap only in part.
- Internationally recognised standards such as ISO27005:2008 define security events and incidents. For example, the ISO definition of security incident is: 'a single or a series of unwanted information security events that have a significant probability of compromising business operations and threatening information security'.
- Article 13a of the EU's 2009 Framework Directive and ENISA's 2011 Guidance on Technical Incident Reporting currently defines what should be reported as a breach. ENISA defines security breach as a 'breach of security or a loss of integrity that has a significant impact on the operation of electronic telecommunications networks and services'.
- Adversaries with malicious intent can use different approaches to target the integrity, availability and/or confidentiality of the data. However, incidents and breaches do not always need to be a result of malicious intent – they can be driven by human, organisational or natural phenomena.

The preamble to the proposal for a NIS Directive makes reference to security incidents as 'deliberate or accidental security incidents'[9] and in the definition in Article 3(4) refers to: 'any circumstance or event having an actual adverse effect on security' in the context of, according to Article 3(2)m an 'accident or malicious action that compromise the availability; authenticity, integrity or confidentiality of stored or transmitted data or the related services'.

We analyse this definition further in this chapter.

2.1 Background

The conceptual understanding of online security incidents (or data breaches) is undoubtedly extremely complex, for various reasons, not least those of a technical nature.[10] Definitions discussed in different communities are not standardised and may overlap – for example a single breach from the perspective of one community may be considered to be several security incidents by another community (for example malware variants are delimited according to different standards with regards to the difference needed to exist between two variants in order to be registered as separate malwares). For instance, parts of the zero-day vulnerability in Stuxnet have been re-used in other examples of malware, but do not count as Stuxnet attacks themselves.[11]

[9] Ibid.
[10] Howard et al., 1998
[11] A 'zero-day vulnerability' is a security gap in a software that is unknown to the vendor, and is exploited by hackers before the vendor is aware of the gap and can patch the software. The name refers to the fact that there are zero days between the vulnerability becoming known and the first attack(Source: PC Tools, Definition of zero-day vulnerability, http://www.pctools.com/security-news/zero-day-vulnerability/

It is also highly important to understand that security incidents with a malicious motivation resulting in breaches may exploit socio-technical (behavioural, organisational or procedural) vulnerabilities instead of or together with vulnerabilities expressed in technical terms (for example, 'product x having bug y').[12]

Various types of guidance are available to define incidents, and some are encapsulated in internationally recognised standards (sets of agreed practice concerning security). These include:

- ISO/IEC 27001:2005 – Information technology – security techniques – information security management systems – requirements[13]
- SO/IEC 27035:2011 (revising ISO/IEC TR 18044:2004) Information technology – security techniques – information security incident management
- Standards of individual Member States (for instance BSI)
- NIST SP 800-61 Computer security incident handling guide recommendations of the US Department of Commerce, National Institute of Standards and Technology
- CMU/SEI-2004-TR-015 Report on defining incident management processes for computer security incident response teams (CSIRTs).[14]

2.2 Security incidents

A security incident may be understood as something that arises the interest or flags a particular warning or alert with regards to a desired or attained security posture.

ISO/IEC Standard No. 27005:2008 (revised by ISO/IEC 27005:2011) is an international standard for security techniques and information security risk management, to which several Member State standards are aligned.[15] Effectively, it constitutes a set of broadly accepted practice relating to security and contains commonly understood terms. This standard defines an information security event as:

> *an identified occurrence of a system, service or network state indicating a possible breach of IS policy or failure of safeguards, or a previously unknown situation that may be security relevant*[16]

and an information security incident:

> *is indicated by a single or a series of unwanted information security events that have a significant probability of compromising business operations and threatening information security.*[17]

[12] Breaches may also occur as a result of accident, at system boundaries or through failure of communications and co-ordination (especially where disposal or loss of physical devices are concerned).
[13] The ISO/IEC 27001:2005 standard is going to be replaced by ISO 27001:2013 in the course of 2013.
[14] Alberts at al., 2004.
[15] E.g. BSI IT-Grundschutz standards on Information Security Management Systems; BSI BS 7799-3:2006 on Information Security Management Systems standards package, first established in 1995; was a precursor to ISO 27001. See http://www.bsi.de/english/gshb/; Susanto et al., 2010.
[16] ISO definitions: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=56742
[17] Ibid.

Examples of incidents include an alarm being triggered on an intrusion detection system, analysis of security incident event monitoring data resulting in flagged patterns; certain kinds of suspicious behaviour being logged (port scanning,[18] for example) by specialised network security personnel or a report from an end-user about odd behaviour occurring on their computer. Consider a 'distributed denial of service' (DDoS)[19] attack, for example. Technically, this may be legitimate traffic, but the sheer scale and speed of the requests to a server (in other words a pattern) alerts administrators and security personnel that this is something unusual and to be considered as a security incident.

The US-CERT defines an 'incident' as 'the act of violating an explicit or implied security policy',[20] but this is a very 'security orientated' understanding of the word. A practical example of an incident may also be sudden slow or loss of internet connectivity, caused by problems upstream in the network (for example an outage in an electricity power station). The complex dependency on energy provision of internet infrastructures makes it difficult to determine exactly how incidents in one infrastructure relate to consequences in another.

The RFC 2350 guide, laying down expectations for the future functioning of CSIRTs, defines security incidents as: 'any adverse event which compromises some aspect of computer or network security'. However, the guide emphasises that these are very general categories and emphasises that attacks, even if they failed because of proper protection, can be regarded as incidents, and often it is the task of the entities performing the response to make a distinction between the two.[21]

The US Committee on National Systems Security Instruction No. 4009 defines an 'incident' as: 'assessed occurrence having actual or potentially adverse effects on an Information System'.[22]

Operational definitions proposed by NIST might be thought of as the most comparable to those from ENISA.

The non-binding US computer security incident response teams (NIST) Computer Security Incident Handling Guide (NIST SP 800-61 rev 2 from 2012)[23] discusses events, adverse events and incidents. It does so from the perspective of those that are computer security related, not those caused by probabilistic events such as natural disasters, power failures and so on.

---

[18] As described in Lee et al., 2001, port scanning is a method that can be used as a part of an attacker's strategy searching for susceptible vulnerable hosts. The activity involves sending a message to a port and listening for an answer. The received response indicates the port status and can be helpful in determining a host's operating system and other information relevant to launching a future attack.

[19] As outlined by the US Computer Emergency Readiness Team (US-CERT), 2009, a denial of service attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting a computer and the network connection of the user, attackers may be able to prevent you from accessing e-mail, websites, online accounts (banking, etc.) or other services that rely on the affected computer. With a distributed denial of service attack, attackers take over other computers and use them, for instance, to send huge amounts of data to a website or send spam to particular e-mail addresses. The attack is 'distributed' because the attacker is using multiple computers to launch the denial of service attack.

[20] US-CERT incident definition: http://www.us-cert.gov/government-users/compliance-and-reporting/incident-definition

[21] The purpose of this 1998 document was to express the general internet community's expectations of computer security incident response teams. It was not possible to define a set of requirements that would be appropriate for all teams, but was considered helpful to list and describe the general set of topics and issues which are of concern and interest to constituent communities. http://www.ietf.org/rfc/rfc2350.txt

[22] Committee on National Security Systems, 2010.

[23] National Institute of Standards and Technology, 2012.

Events might include any observable occurrence in a system or network, such as a server responding to a request for a web page, a user sending an e-mail or a firewall blocking a connection attempt.

NIST's Computer Security Incident Handling Guide defines adverse events as:

> *events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data. This guide addresses only adverse events that are computer security-related, not those caused by natural disasters, power failures, etc.*

It further defines a computer security incident as:

> *a violation or imminent threat of violation of computer security policies; acceptable use policies or standard security practices.*[24]

A proposed US bill from 2013 on Co-ordination of Federal Information Security Policy proposes a definition of an incident in Section 332 of Title 44 of the US Code as

> *An occurrence that:*
>
> - *actually or imminently jeopardises without lawful authority the integrity, confidentiality or availability of an information system or the information that system controls, process, stores or transmits or:*
> - *constitutes a violation or imminent threat of violation of law, security.*[25]

Finally, as an example of a definition from a critical infrastructure provider, the US National Electric Reliability Council (NERC) defines a security incident as:

> *Any malicious act or suspicious event that: Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset.*[26]

Despite this, under the US regulatory system, each critical infrastructure has a sector-specific plan that outlines definitions applicable to that particular sector. For example, the US Defense Industrial Base pilot, in its interim rule[27] (hereinafter 'Interim Rule') from 2012 defined a cyber incident as:

> *actions taken through the use of a network that result in an actual or potentially adverse effect on an information system and /or the information residing therein.*

[24] Ibid.
[25] Federal Information Security Amendments Act, 2013, pp. H2037–H2042.
[26] North American Electric Reliability Corporation, 2013.
[27] US Department of Defense, 2012.

The Defense Industrial Base (DIB) pilot rule also defined threats as:

> *any circumstance or event with the potential to adversely impact organization operations (including mission, functions, image, or reputation), organization assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service.*

The Japanese CERT JP-CERT defines an incident as:

- *Human Manipulation related to computer security*
- *Abuse of resources, denial of service breaking data information leakage*[28]

A security breach, by contrast, may be considered to occur when an incident breaches or causes a state where certain perimeter based security controls are compromised. The term 'breach' implies the penetration of a barrier or some other form of protection mechanism.

At the same time, the definition of 'data breach' has received the common understanding (and an understanding which the legal framework aims at) that intends data breaches to mean those incidents resulting in the compromise of the confidentiality, integrity or availability of *personal* data (as defined by the Data Protection Directive 95/46/EC), although technically the term might cover a range of data types beyond personal data (e.g. intellectual property, classified information). EU Member States largely conform to this legislation in defining the conceptual and legal frameworks of their relevant systems.[29] Therefore, there is little evidence of courts or competent authorities utilising definitions not aligned with the ones laid down by the Directives.

The US Health Information Technology for Economic and Clinical Health (HITECH) rule in the Health Insurance Portability and Accountability Act (HIPAA)[30] defines a breach as:

> *an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.*

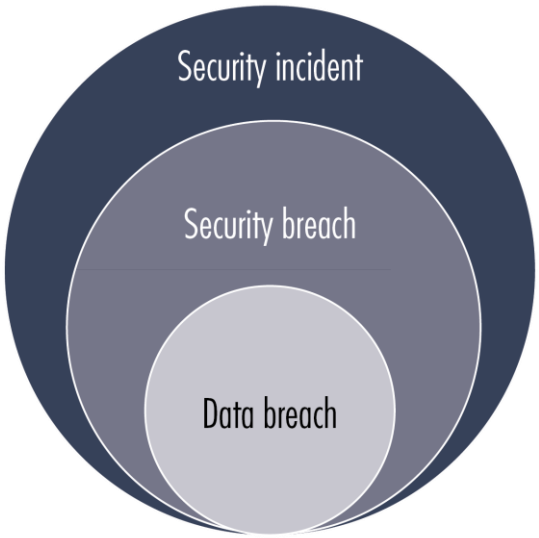
In January 2013 the Breach Notification Rule was amended.[31] The US Department of Health and Human Services defined breach as: 'the acquisition, access, use or disclosure of Personal health information (PHI) in violation of the Privacy Rule that compromises the security or privacy of the PHI'. The amendments modified the phrase from significant risk of financial, reputational or other harm to the model that, notwithstanding exceptions, an impermissible use or disclosure of personally identifiable information is presumed to constitute a breach unless the covered entity can demonstrate that there was a low probability that personal health information had been compromised based on, at a minimum, a four part risk assessment.

[28] JP CERT, 2008.
[29] Article 29 Working Party, 2011, p. 32
[30] Interim final breach notification regulations, issued in August 2009, implement section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act by requiring HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.
[31] Final omnibus rule amending the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in accordance with the HITECH Act of 2009.

The multidisciplinary character of vulnerabilities, incidents and breaches can become complex to understand. For example, the loss of unencrypted laptops can be seen as a failure of policy and procedure where those using the laptops expected them to be encrypted (yet they weren't) and therefore behaved more recklessly in their use. Such challenges become even more acute with regard to individual owned devices (under the bring your own device – BYoD) model.

Figure 3 presents a broad classification of how these terms are sub-sets of one another.

Figure 3 The relationship of security incidents to security breaches and data breaches (Source: RAND Europe)



However, this is a somewhat (and necessarily) simple and abstracted picture. A security incident may result in a data breach where an adversary targets personal data to obtain or copy illegitimately. A security incident also may not involve personal data – such as a DDoS, for example, which does not target personal data but aims to take the target offline.

Regulators may also choose to include certain types of incidents and not others. The proposed legislation on information security breaches under consultation in the Netherlands, for instance, only covers the breaches that are considered to affect the security or integrity of electronic information systems most severely. In the Explanatory Memorandum to this draft bill, DDoS attacks are not considered to have this effect and are, thus, not covered by the notification duty. It is argued that DDoS attacks result in the temporary unavailability of certain systems, but does not affect the systems that are used in this respect.[32]

To complicate matters, a breach of personal data might not necessarily precede a security incident (although, if discovered, it may become an incident after the fact). A careless data controller might, through lack of oversight or poor practices, lose or misplace personal data, as occurred in the UK at the UK's HM Revenues & Customs (HMRC) in 2005 when two CDs with the personal data of 25m UK citizens went missing in the post.

[32] Ibid, p. 3.

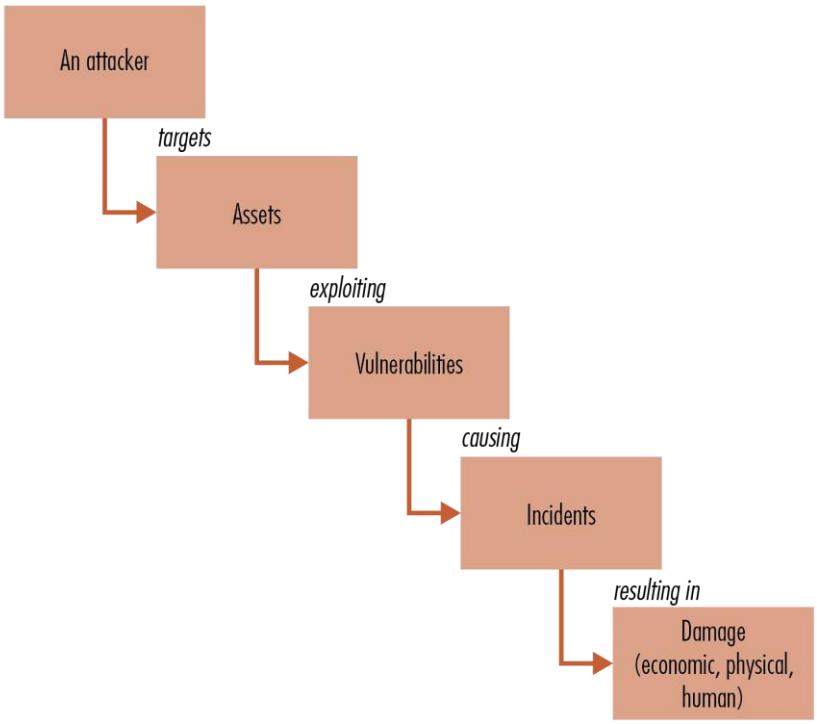
By the time such an incident becomes known it is undoubtedly a security incident (in that the management controls aiming to meet security objectives regarding the protection of personal data failed).

2.2.1 Malicious incidents

The type of security incident that is perhaps most focused on is one where it is thought a malicious actor ('adversary') may be involved. Adversaries may cause incidents in order to effect some kind of consequence: either extracting information,[33] or denying use of a service to others.

Focusing on the motivation of malicious actors in perpetrating incidents, Figure 4 presents an overview of the logic behind adversaries exploiting different kinds of vulnerability.

Figure 4 The logic of adversary-driven incidents (Source: RAND Europe)



It is difficult to determine absolutely whether an adversary is part of an organised crime network;[34] a disgruntled former employee or a nation-state.[35] Furthermore, even the definition of attack is far from straightforward. Some security incidents may not necessarily breach defences to be useful from an attacker's perspective, for example a port scan where an attacker can remotely check to see what kind of services are running on a particular machine.[36] Armed with this information, which may sometimes include technical details about the computer offering such services, the attacker can then select which methods to use and might try to target:

[33] It is difficult to define 'information theft' since by copying it, its use is not denied to others; therefore the term often used is 'data exfiltration'.
[34] E.g. the Russian Business Network.
[35] Mandiant Intelligence Center Report, 2012.
[36] See footnote 18 above.

- the integrity of information, by breaking into networks (e.g. by exploiting known vulnerabilities to software versions running on the targeted computer) to modify data to cause damage or disruption
- the availability of information or information systems by undertaking attacks such as DDoS attacks
- the confidentiality of information, for example by downloading it and exploiting it for criminal purposes, such as identity theft and accessing bank accounts; disclosing confidential information for political purposes etc.; the target can be either commercially or nationally sensitive data (such as business or military secrets) or personal data (such as usernames, passwords, bank account information or credit card details).

Cyber attacks may comprise more than one security incident such as in an advanced persistent threat like the Night Dragon series.[37] Furthermore, attacks affecting or exploiting cyber space do not necessarily need to be electronic. Many are multidisciplinary and can employ a variety of vectors.[38] We present below an overview based on analysis of some common types:[39]

- *DDoS*: in a DDoS attack, a denial of service, a number of computers send a barrage of legitimate requests (e.g. for web pages or other type of service) over an extremely short period of time, overloading the destination server. Normally, DDoS attacks are carried out using a botnet – a network of compromised computers usually unwittingly running software that allows them to become part of such a network. Botnets are controlled using command and control server software. An example of such software is Low Orbit Iron Cannon.[40] An adversary (either an individual or a group of individuals) behind a botnet is called a 'bot master'. A DDoS can be politically or ideologically motivated or, as part of a threat to extort, criminally driven.
- *Advanced persistent threat* (APT): this type of attack is characterised by multi-stage, multidisciplinary ('advanced') techniques over an extended ('persistent') period of time. Incidents usually include social engineering or spear phishing to gain access; network reconnaissance (mapping of the internal network to discover where services or assets are located); installation of backdoors or remote access tools) and then data exfiltration (unauthorised copying of data).
- *Web defacement*: in this type of cyber attack a website or other online service accessible through a web browser is defaced and the original content replaced (usually with a message intended to convey a particular point that the attackers wish to get across).
- *Insider attack*: this is a particularly complex form of attack as an insider attack may encompass any of types of incident listed below. For example, an insider might try to escalate his or her account privileges via their knowledge of the network layout in order to copy information. The defining characteristic of the insider attack is that the perpetrator is in some way trusted as being inside the organisation or having some level of trusted role within it.

[37] McAfee, 2011.
[38] Attack vectors (source: ENISA, 2012)
[39] For more detailed taxonomy, see ENISA, 2012b.
[40] For more information, see: GCN. Com, 2012, Hackers' New Superweapon adds Firepower to DDoS, 24 October 2012, GCN.com: http://gcn.com/articles/2012/10/24/hackers-new-super-weapon-adds-firepower-to-ddos.aspx

- *Social engineering*: although not strictly a type of cyber attack, given the huge quantities of information stored and accessed via cyber space, adversaries are wont to try and exploit as many possible routes to get to it to achieve their objectives. The human factor is usually the easiest route. Kevin Mitnick, the notable computer hacker, remarked that 80% of his success was down to social engineering,[41] a class of attack where an adversary tries to exploit different psychological, behavioural or social weakness in order to breach security controls. A simple example is where an adversary calls a user pretending to be someone from the IT department and asks the user for their password under the guise of performing system maintenance.
- *Undermining integrity of the supply chain*: a form of attack that is also non-specific to cyber but because of the complex interdependent globalised supply chains for information society products and services is particularly acute in cyber space. In this case, the entities in the supply chain may be coerced or bribed or acting against the wishes of business partners and others in the supply chain to deliberately modify or change products and services, installing backdoors or other code that is not part of what they were contractually asked to complete. This type of attack is relatively insidious to defend against and has similar characteristics to the insider threat (in that addressing it comes down to management, procedural and organisational measures).

The list above identifies incidents where attackers acting strategically might try to breach security controls by exploiting specific vulnerabilities to cause desired consequences. There are many other types of incident which might affect the security posture of an organisation, including accidents, incidents arising from natural causes and incidents caused by other phenomena.

Table 3 illustrates a list of prominent recent incidents of these types of attack, compiled by one of the online databases collecting data on these events.

Table 3 Examples of data breaches collected by Hackmageddon in the EU since October 2012 (Source: Timeline master index on Hackmageddon website[42])

Date	Event	Implication
26/05/2013	Monsanto website hacked	Whole database dumped,[43] including credentials of personnel managing the website
22/05/2013	XCount3r hacked Audi Switzerland	More than 2,000 accounts dumped
20/05/2013	UK Toyota blog hacked	Personal information of 5,000 individuals leaked
19/05/2013	Imperial College information system hacked	Staff and administrator accounts breached
11/05/2013	Website of the Romanian National Authority for qualifications hacked	Administrator and user accounts breached
08/05/2013	Dutch government websites suffered DDoS	10 million citizens unable to pay taxes and bills online

[41] Mitnick, 2000.

[42] http://www.hackmageddon.com

[43] The term data dumping (a technique usually used in the backing up of databases) usually refers to the publication of data and the structure of the database itself, usually in the form of SQL commands (for more information (see: definition of dump at MySQL Forum: http://dev.mysql.com/doc/refman/5.0/en/mysqldump.html). The term data leaks usually refers to the disclosure of sensitive information (see: Definition of data leaks, Mitre.org: http://capec.mitre.org/data/definitions/118.html).

03/05/2013	Anonymous Italia published 4.2 GB of e-mails by Movimento Cinque Stelle	Members of parliament and senators e-mail accounts breached
20/04/2013	Unknown hackers hack jewellery manufacturer bluebird.pt	4,316 member accounts and credentials dumped
15/04/2013	Website of the German Young liberals hacked	More than 10,000 e-mail addresses and contact details breached
06/04/2013	Lulzsecwiki hacked HPTH UK, a charity for a rare medical condition	User accounts leaked
05/04/2013	Polo Tecnico Giulianova hacked	Approximately 500 accounts and credentials dumped
02/04/2013	Website of UK branch of Commonwealth Bank of Australia hacked	1,900 encrypted passwords, accounts and full names dumped
14/03/2013	An unnamed hacker penetrated the computers of the Polish president's office and computers in the Ministry of Foreign Affairs	
14/03/2013	The careers website of a Lithuanian university hacked	Names and passwords of 14,000 students dumped
27/02/2013	Several European governments (including Czech Republic, Ireland, Portugal, Romania) and NATO were targeted by a malware in Adobe Systems software	Not disclosed
25/02/2013	The database of the Hungarian police breached	More than 5,000 records published
24/02/2013	EADS and Thyssenkrupp reported as victims of cyber espionage by Chinese firms	Not disclosed
19/02/2013	LulzES breached the database of the Spanish film academy	Personal details of members leaked
18/02/2013	Mandiant published a report exposing cyber-state-backed cyber espionage	Among the victims were UK, Belgian, French and Luxemburg-based companies
15/02/2013	Website muslim-ads.co.uk hacked	IP addresses and e-mails of more than 6,000 members leaked
13/02/2013	Website muslim-news.co.uk hacked	Personal data including phone numbers, addresses, e-mails and names of more than 1,600 users published
13/02/2013	Ruhr University Bochum made public that it was hacked	50,000 students potentially affected
02/02/2013	French Ministry of Sport breached	100 accounts breached
02/02/2013	French Ministry of Development breached	800 account details leaked
02/02/2013	Luxembourg British Chamber of Commerce website hacked	Login information of 900 individuals leaked
01/02/2013	Association des Anciens Eleves France hacked	Account information of 17,900 members leaked
17/01/2013	Database of Italian Democratic Party hacked	Information of 630 members leaked
15/01/2013	A sub-domain of the French Ministry of Defence hacked	Server details and 20+ account details
07/01/2013	Panasonic Europe Czech Republic and Slovakia websites hacked	Complete database dumped
06/01/2013	Association of Irish Festival associations hacked	15,000 records with full credentials dumped
04/01/2013	Anonymous release of files from German Chamber of commerce	2.66 GB (approx. 5,500 files) leaked

22/12/2012	Belgian railway company data breached	Internal error – inadvertently published 1.46 million sets of customer data online
26/12/2012	Renault Bulgaria hacked	7,000 accounts, including administrative accounts and passwords, leaked
24/12/2012	German Muslim website Ihya.org hacked	100,000 accounts leaked
21/12/2012	For the expected end of the world, several organisations hacked and data dumped, including e-commerce and online services websites from Europe	
16/12/2012	Anonymous Bulgaria took down the website of the Ministry of Finance	
11/12/2012	UK MP David Morris website hacked and defaced	
06/12/2012	Private document leaked from International Telecommunication Union meeting	Divulged confidential information on deep packet inspection measures
04/12/2012	IAEA database hacked	Data from nuclear data section leaked
04/12/2012	Swiss national security agency warned that large amounts of confidential antiterrorism data were leaked by employee	
03/12/2012	phisolophia.eu.org website hacked	1,700 e-mail addresses and other text dumped
28/11/2012	Phone numbers of several famous Spanish football players published	
28/11/2012	Websites of several large companies redirected to hacker websites.. including the Romanian websites of Google, Yahoo, Microsoft and Kaspersky	
27/11/2012	Several retail firms hacked	The largest leak was of more than 2,000 accounts each from Royals Quay, UK and Leaden Hall UK
27/11/2012	Piwik, the free web analytics tool for PHP/MySQL hacked, planting malicious code inside the latest version of the programme	
26/11/2012	Website of the Lithuanian police hacked	
25/11/2012	IAEA server hacked	160 e-mail addresses leaked
21/11/2012	Computers in the French presidential office reported to have been victims of a US-originated targeted attack	
20/11/2012	Man arrested over massive-scale ID theft in Greece	Theft of 9 million files including personal data, social security numbers, vehicle registration numbers etc of Greek citizens
19/11/2012	Complete database of Bulgarian torrent website arenabg leaked	
15/11/2012	Danish dating website sex.dk attacked via SQL injection	30,000 accounts and passwords published online
11/11/2012	Anonymous hacked the Organisation for Security and Co-operation in Europe (OSCE)	55 mbs of internal documents leaked
11/11/2012	Amazon.co.uk hacked (Amazon denies the attack)	600 account details, names etc and e-mail addresses dumped
10/11/2012	Far-right organisation English Defence League hacked	E-mails and list of donors hacked
08/11/2012	UNESCO website hacked	60 usernames and passwords leaked
08/11/2012	The laptops of two EU officials, Ryan Heath and	

	Camino Manjon apparently hacked in a hotel in Baku, Azerbaijan, during the Internet Governance Forum	
07/11/2012	LG Hungary's site hacked	1,300 user credentials, names, locations, e-mails and passwords leaked
06/11/2012	Anonymous claimed to have hacked Telecom Italia	Anonymous claimed to possess 300,000 credentials (several are dumped to substantiate the claim)
06/11/2012	Ministry of Defence UK hacked	3,600 user accounts and account information dumped
04/11/2012	Anonymous claimed to have released several documents from the OSCE	
29/10/2012	Anonymous leaked confidential documents from the Greek Ministry of Finance	
27/10/2012	International Professional Management Association UK website hacked	More than 2,400 user names and passwords released
24/10/2012	UK Police internal communication network hacked	More than 20 million accounts hijacked
23/10/2012	Italian Police database hacked	3,500 private documents leaked
15/10/2012	WHO website hacked	Part of the database dumped

2.2.2 Accidents

Given the complexity of cyber space and the sheer size of the infrastructure, it is perhaps unsurprising that human error is an important consideration. In fact, many argue that at the level of the core backbone of the infrastructure, human error is a more significant security issue than those listed above.[44] Human error may encompass misconfiguration of devices or routers[45] or other infrastructure causing either local or in extreme cases regional or international issues. Mistakes and misconfigurations may go unnoticed and result in vulnerabilities that attackers can then exploit if found, for instance by accessing the system and compromising information stored on it, or assuming control of the system and causing disruption of its functioning; or installing malicious software on its elements.

There is also the possibility of errors arising from the sheer complexity of cyber space, which may be compounded by mistakes in configurations or may occur 'naturally' as a result of systemic complexity.[46] For example, routers in the backbone infrastructure read tables to tell them where to send traffic for the next hop. If there are delays in updating the tables (for instance due to systemic glitches, general network latency, or unusually high quantities of transmitted data) then a condition called 'route-flap' occurs, which can reduce internet speed for end-users. A domain of research called 'internet weather' has developed, which investigates such issues.[47]

[44] These are discussed in several guidance documents, e.g. ENISA, 2012b; also the German Federal Ministry of the Interior's guidelines on critical infrastructure protection also stress the high potential damage and rapid dissemination of incidents caused by human error (see: Federal Ministry of the Interior, 2008).

[45] E.g. see Pakistan YouTube outage: in 2008, an attempt of the Pakistani government to block access to YouTube within the country for hosting content it perceived as anti-Islamic resulted in YouTube becoming inaccessible around the globe for more than an hour as a result of a mistake committed by Pakistan Telecom (see: Gannes, 2008).

[46] Incident leading to outage that occurred in France in July 2012, where a software glitch in France Telecom's software used to trace mobile phones accidentally multiplied signals and resulted in a flood of signalling traffic, eventually bringing down the network and resulting in 28 million customers unable to place calls or receive text messages (see: http://theneteconomy.wordpress.com/2012/07/11/france-seeks-influence-on-telcos-after-outage).

[47] For an explanation of this phenomenon, see: Connection Management, 2013.

2.2.3 Incidents arising from natural causes ('force majeure')

Events in the natural environment may affect the physical elements of the internet infrastructure resulting in security problems (e.g. loss of availability). Examples include tsunamis, which can affect submarine cables resulting in outages,[48] solar flares,[49] storms and other extreme weather conditions.

2.2.4 Other physical incidents of relevance

Major acts of terrorism, such as the attacks in the eastern seaboard in the US in 2001, may have security implications for the availability of internet infrastructures and hence cyber space.[50]

Physical accidents such as the accidental severing of undersea or underground fibre optic cables (known as 'backhoe failure'[51]) are more frequent than might be expected and, although the internet infrastructure is designed to be resilient, can have an effect.[52]

Serious large scale industrial accidents such as the Deepwater Horizon disaster or Buncefield Oil Refinery fire in the UK may result in knock-on effects on the internet infrastructure and consequently in cyber space.[53]

Theft of physical elements of the internet infrastructure are also relevant. The theft of copper wire is a major security issue for telecommunications companies – as prices of copper have risen on the market and there is extensive use of copper in telecommunications infrastructure, copper wire has become a target for criminals.[54]

[48] Carter et al., 2009.

[49] Sommer and Brown, 2011.

[50] There has been no public analysis of the implications of other major terrorist attacks on the internet infrastructure (such as Madrid; London or Mumbai). The report by the Committee on the Internet under Crisis Conditions noted that the attacks in New York in 2001 did not have a noticeable effect on the backbone routing infrastructure despite the collapse of an AT&T switching centre – rather that the high demands made on electronic communications networks by voice calls and SMS messages (of people calling each other to see where they were) and traffic to news websites were the more significant visible effects – see: National Research Council of the National Academies, 2003.

[51] Backhoe failure or backhoe induced fibre failure is where a tractor or digger accidentally cuts fibre optic cables when engaged in other work (e.g. laying new gas pipes).

[52] Accidental severing of submarine cables in Cairo.

[53] Deepwater Horizon oil spill: on 20 April 2010 and explosion killing 11 people and subsequent fire on the Deepwater Horizon oil rig operated by BP resulted in the largest oil spill recorded so far, leaking 4.1m barrels of oil in the Gulf of Mexico. In the more than 80 days that oil flew from the underwater oil well, five states were impacted, and rescue operations involved more than 47,000 staff and 6,870 vessels (see: National Response Team, 2011). In the Buncefield fire on 11 December 2005 a series of explosions took place at Buncefield Oil Storage Depot, Hemel Hempstead, Hertfordshire. 40 people were injured and significant damage occurred to commercial and residential properties in the vicinity. The fire burned for several days, destroying most of the site. According to the final report published by the investigation into the accident the overall cost amounted to approximately £1 billion comprising compensation for loss, costs to the aviation sector, the emergency response and the costs of the investigations. The incident ultimately led to redefining health and safety good practice applying to the storage of similar materials (see Buncefield Major Incident Investigation Board, 2005).

[54] *The Guardian*, 6 April 2011.

Finally other physical acts include vandalism of physical parts of the infrastructure. Vandalism (the motives of which are beyond the scope of this study) might also have effects on the availability of internet infrastructure and elements of cyber space. For example, it has been recorded that burning rubbish bins have taken parts of the UK telecommunications infrastructure[55] offline for short periods of time.

This discussion is not wholly academic because firms report incidents in different ways and prioritise different types of incident depending on the specific nature of their own business.

Under ENISA's 2013 Technical Guidance (Article 13a), the reporting regime for providers of e-communications services (mainly although not exclusively fixed or mobile telephony and fixed or mobile internet access) security incidents is defined as: 'a breach of security or a loss of integrity that could have an impact upon the operation of electronic telecommunications networks and services'.[56]

As part of the formulation of reporting guidance, ENISA agreed with national regulatory authorities (NRAs) to report only 'incidents involving outage of services'.[57] The Agency identifies the following root causes of incidents in 2011:[58]

- natural phenomena – storms, floods, heavy snowfall
- human errors – caused by errors committed by employees of the provider
- malicious attacks – caused by a cyber attack or other forms of malicious behaviour (e.g. cable theft)
- hardware or software failures – caused by a failure of hardware or software
- third party failures – caused by an incident or failure at a third party.

[55] ZDNet, 23 October 2002.
[56] ENISA, 2013a. Under a common information security understanding, integrity in this instance equates to the term availability.
[57] Therefore some forms of security incident (e.g. those that may occur in cyberspace and revolve around exfiltration of sensitive or personal data) do not fall under this scheme. This may go some way to explaining why the incidents included are mainly of a physical nature.
[58] ENISA, 2011b.

2.3 Legal basis of definitions

Table 4 Comparisons of definitions of security incident, security breach and data breach

Legislation	Definition
Security incident or event	
Proposal for a NIS Directive	Article 3(4) Any circumstance or event having an adverse effect on security
Directive 2009/140/EC Article 13a (3)	Not specifically defined but identified in the context of reporting under Article 13a as: "a breach of security or loss of integrity that has had a significant impact on the operation of networks or services"
ENISA (2011) Reporting Major Security Incidents – Implementation of Article 13a Technical Guideline on Incident Reporting	An event which can cause a breach of security or a loss of integrity of electronic communication networks or services
	Reportable incident: A breach of security or a loss of integrity that has a significant impact on the operation of electronic telecommunications networks and services
ISO/IEC Standard No. 27005:2008	[Security event] An identified occurrence of a system, service or network state indicating a possible breach of IS policy or failure of safeguards, or a previously unknown situation that may be security relevant [Security incident] A single or a series of unwanted information security events that have a significant probability of compromising business operations and threatening information security
US-CERT	The act of violating an explicit or implied security policy
US Committee on National Security Systems	Assessed occurrence having actual or potentially adverse effects on an information system
US NIST Computer Security Incident Handling Guide	[Adverse events] Events with a negative consequence, such as system crashes, packet floods, unauthorised use of system privileges, unauthorised access to sensitive data, and execution of malware that destroys data
US proposed legal definitions proposed bill from 2013 on Co-ordination of Federal	'An occurrence that (A) actually or imminently jeopardises without lawful authority the integrity, confidentiality or availability of an information system or the information that system

Information Security Policy proposes a definition of an incident in Section 332 of Title 44 of the US Code	controls, process, stores or transmits or: (B) constitutes a violation or imminent threat of violation of law, security'
RTF 2350 Guide	Any adverse event which compromises some aspect of computer or network security
JP-CERT	Human manipulation related to computer security; abuse of resources, denial of service breaking data information leakage
Security breach	
Proposal for a NIS Directive	No clear definition exists in legislation, interpretation based on proposal for a NIS Directive, Article 3(2): A security breach is present when a provider has breached its security duties as obliged by the Directive
Article 4 of the e-Privacy Directive 2002/58/C, as amended by the 2009 EU legislative framework on electronic communications	'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'
Article 15 of the Trust Services Regulation	Not specifically defined but identified in the context of reporting under Article 15(2) as a 'breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein'
US Defence Industrial Base Pilot Guidance	Any circumstance or event with the potential to adversely impact organisation operations (including mission, functions, image, or reputation), organisation assets, individuals, other organisations, or the nation through an information system via unauthorised access, destruction, disclosure, modification of information and/or denial of service
Data breach	
Article 30, 31 and 32 of the proposed data protection regulation	'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'
US Health Insurance Portability and Accountability Act	An impermissible use or disclosure under the privacy rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual

2.3.1 Security incident

Of the three terms 'security incident', 'security breach' and 'data breach', the first one is the only one defined in the NIS Directive. As we have seen, Article 3(4) defines incident as 'any circumstance or event having an actual adverse effect on security'. This is a broad definition. In paragraph 3 of Article 13a of Directive 2009/140/EC the term 'incident' is not used, but the term notification duty is introduced for 'a breach of security or loss of integrity that has had a significant impact on the operation of networks or services'. ENISA does define 'incidents' and 'reportable incidents' in its non-legally-binding Technical Guideline on Reporting Incidents:

- *Incident is herein defined as an event which can cause a breach of security or a loss of integrity of electronic communication networks or services.*
- *Reportable Incident: A breach of security or a loss of integrity that has a significant impact on the operation of electronic telecommunications networks and services.*[59]

ENISA's definition of a reportable incident is thus similar to the definition of a security breach for which the notification duty in Directive 2009/140/EC applies. The only difference is in the absence of the word 'had' in the ENISA definition. This has no direct influence on the definition, but rather on the moment at which a notification is required. The wording of the Directive leaves some room for notifying afterwards, while the ENISA definition requires immediate notification once an incident takes place.

The essential element is that there has to be an impact on the security of the core services (significant impact on the operation) provided. This makes it possible to place the other two terms in perspective as sub-categories.

2.3.2 Security breach

A security breach occurs when a provider has breached its security duties as obliged by the Directive. By analogy, on the basis of the Data Protection Directive[60] or the e-Privacy Directive, companies should apply sufficient technical and organisational measures to guarantee the security of the data they process. If these measures are not taken sufficiently, a security breach takes place, regardless of whether there really is a loss of data. Such a breach can take the form of the installation of malicious software, without it being activated, or a DDoS attack.

A clear definition of security breach is not present in legal texts, however. Directive 2002/58/EC (the e-Privacy Directive) mentions the risk of a breach of security in Article 4(2) and Recital 20. The service providers should notify the subscribers of their services about these risks. Thus the security breach is linked to a certain risk. A broader introduction of data breach notification duties came with Directive 2009/136/EC, which amended the e-Privacy Directive, but definitions are still not included.

The Article 29 Working Party has found that Member States have been following closely the core elements of the personal data breach provisions in the e-Privacy Directive, including definitions and thresholds. Accordingly,

[59] Ibid, pg 8.
[60] See article 30 of European Parliament & the Council, 2012.

> *It is expected that competent national authorities and relevant actors will increasingly rely on these concepts to deal with personal data breaches. In the next years, these concepts and procedures will therefore 'solidify' across EU Member States.*

Therefore, the level of granularity and preciseness of definitions in EU legislation can have repercussions on the conceptual frameworks adopted at the Member State level as well.[61]

The absence of a general security breach notification duty has led to a patchwork of national legislations, with two basic flavours: notification to either the supervisory authorities or to the individuals that may be affected by the security breach is required.[62]

2.3.3 Data breach

A data breach takes place when there is any impact related to the data themselves, such as the data being lost or illegitimately accessed, and not only related to the security of the system. These data do not necessarily have to be personal data. When personal data are involved the breach is a 'personal data breach', which is defined in Article 4(9) of the proposal for a general data protection regulation: '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'. Once the regulation is in place as the general legal framework concerning personal data protection, this definition can be applied to the NIS Directive as well.

2.4 Generalising comparisons between cyber attacks and the real world

As we have seen, understanding technical security incidents can be complex even for experts. Table 5 provides a generalised analysis of close comparators from the real world to some of the phenomena discussed above.

Table 5 Generalised comparisons between cyber attacks and real world incidents (Source: RAND Europe)

Cyber-security incident	Broad non-cyber equivalent
Phishing is like…	Theft of your wallet
Identity theft is like…	Theft of your bank statements from a rubbish bin
Distributed denial of service is like…	Barricading the doors to a business or bank
Web defacement is like…	Graffiti on the front of a shop
Attacks against critical infrastructure are like…	Covertly sabotaging infrastructure (e.g. physically interfering with control systems)

[61] Article 29 Working party, 2011, p. 32.
[62] Kuner and Pateraki, 2012.

Hacking or network penetration is like…	Covertly breaking into a business or organisation to go through offices and filing cabinets
Hacking or network penetration into a bank is like…	A bank robbery
An advanced persistent threat is like…	A complex extended campaign of trickery, deception, espionage, break-ins and going through offices and filing cabinets
Personal data breaches are like…	Filing cabinets or drawers full of data about citizens or customers being lost or stolen

2.5 Conclusions

This chapter has outlined the range of definitions applying to the categories of attack, security incident and data breach based on definitions from ISO, policy documents and the legal framework. Consistent and unambiguous definitions across legislative instruments are often lacking.

Incidents can have a variety of root causes, including malicious attacks and accidents. These include environmental conditions, such as storms or floods, human error, malicious intent, hardware or software failure, and third party failure.

An information security incident can be defined as a breach, when an incident breaches or causes a state where certain perimeter based security controls are compromised. The term 'breach' implies the penetration of a barrier or some other form of protection mechanism, as in the transfer of information from a trusted to an untrusted environment.

A data breach takes place when there is an impact related to data (in the sense of personal data) itself, such as data being lost or illegitimately accessed, and effects do not only have repercussions on the security of the system. Under the proposed data protection regulation, '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.

3 WHO IS AFFECTED AND WHERE? THE SCALE AND TRENDS OF SECURITY INCIDENTS AND BREACHES

KEY FINDINGS

- No common framework exists under which security incident or breach data is collected.
- Different actors in the public and private sector collect and compile incident reports.
- Incident reporting is beset by structural characteristics, and the number of those reported is generally acknowledged to be smaller than actual incidents.
- The trend appears to suggest that incidents are increasing but the rate of increase is uncertain.
- There is nothing to suggest that Europe is any more or less secure than other comparators such as the US or Japan.
- It is difficult to determine the effect of policy interventions on incident trends.
- Based on conservative estimates and available Eurostat data, the total minimum direct costs for all types of security incident (including hardware and software failure) affecting companies is 0.004% of GDP and for other countries 0.061% of GDP.
- At EU level, the estimated minimum total cost to SMEs was €2.3bn, or 0.017% of EU GDP.

Although systematic comparable data sources covering the EU[63] are hard to come by, there are several proxies that can help us gain an understanding of the distribution and frequency of information security and data breaches in Europe. Table 3 in Chapter 2 illustrates recent examples of such breaches. In this chapter we present the available data by different types of evidence; a wide variety of biases should be kept in mind.

Data usually include the counts, sizes or losses due to incidents, but none of these incidents can tell us much on its own – all three indicators are needed to attempt to understand the equilibrium between attackers and defenders.

Table 6 summarises the available data sources and their respective strengths and weaknesses in providing an evidence base for decisions.

Table 6 Overview of available data sources

Source type	Examples	Strengths	Weaknesses
Anecdotal evidence	Datalossdb.org Hackmageddon.com Shadowserver.org[64]	Detailed information on individual breaches Often only source of information on breaches	Unfit as a basis for analysis Data collection relies on publicly available reports

[63] Noting Croatia joined the EU on 1 July 2013 thus making 28 Member States

[64] Data loss db, Open security foundation (http://Datalossdb.org); Hackmageddon Website, publishing Cyber attack timelines (http://Hackmageddon.com); Shadow Server Foundation (http://Shadowserver.org).

		Can help contextualise and illustrate trends	
Industry statistics	UK Information Security Breach Survey (ISBS)[65] Publications by organisations such as Club de la Sécurité de l'Information Français (CLUSIF), CLUSIT,[66] etc.	Often only data source on industry perspective	Lack of common frameworks for reporting Data limited by awareness or propensity of companies to disclose incidents
Official statistics	Eurostat, Eurobarometer, reports from national or governmental CERTs ENISA	Robust and presumably bias-free reporting Many databases cover all EU MS	Limited availability of indicators Lack of common definitions for CERT reporting
Information security companies	Microsoft Security Intelligence Reports[67] Symantec Internet Security Threat Reports[68]	Automated data collection not dependent on awareness or propensity to report of targets Wide coverage (according to market share)	Misaligned incentives: cyber-security companies have an interest in framing threats in a way that supports demand for their products Data collection depends on market share of individual company

3.1 Collection of data on incidents

3.1.1 Anecdotal evidence

Systematic reviews of available open-source information (such as those reported by the media and entities such as datalossdb.org) can give some evidence on the landscape of breaches in a country. However, the validity of aggregative or comparative analyses on the nature, sector breakdown and magnitude of breaches based on these sources is constrained by biases and a lack of uniform standards for reporting incidents. Most of the reported attacks noted in Table 3 were targeted at high-profile institutions and companies with the implicit aim of publicity, in addition to a few instances of internal error or other sources that were reported on these lists. This illustrates that such anecdotally derived compilations are subject to significant selection bias as media outlets base their choice of incidents to report on their access to suitable corroborating detail and level of interest to their audience. Similarly, reports to online databases depend on the willingness of affected or detecting entities to share the information (companies are understandably reluctant to disclose information about incidents), those reporters' ability accurately to describe the events and the consistency of their reports.

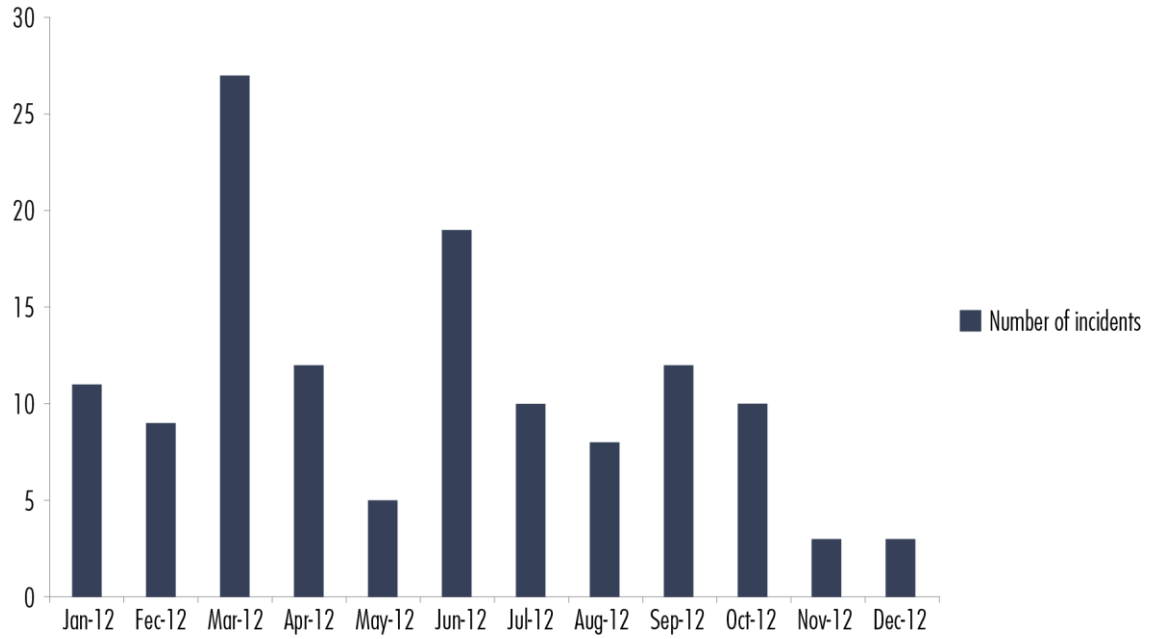
[65] E.g. BIS, 2013.
[66] E.g. CLUSIT, 2012.
[67] E.g. Microsoft, 2012.
[68] E.g. Symantec, 2013.

3.1.2 Evidence from the industry: surveys and other empirical data

Associations and clubs of information security professionals in some EU Member States[69] have been conducting annual surveys of the frequency of breaches and different types of incidents for some years.

Italy's CLUSIT is an example of such an effort. Figures 5, 6 and 7 illustrate the frequency and sectoral breakdown of incidents in Italy in 2011 and 2012.[70] The figures show that the public sector accounted for the largest proportion of publicly reported breaches in both years for which the information has been synthesised. However, this picture is likely to be at least partially the result of the above-mentioned selection bias, as public sector breaches and high visibility cases (in particular a series of defacement attacks targeting political parties in 2011) often attract more media attention and thus are likely to be over-reported in comparison with breaches in industry sectors.

Figure 5 The number of incidents in Italy (Source: CLUSIT)



[69] For a full list of these 'Information Security Clubs' see: CLUSIF website: http://www.clusif.fr/fr/clusi/
[70] See: CLUSIT website: http://www.clusit.it

Figure 6 Sector breakdown of targets in Italy in 2012 (Source: CLUSIT)

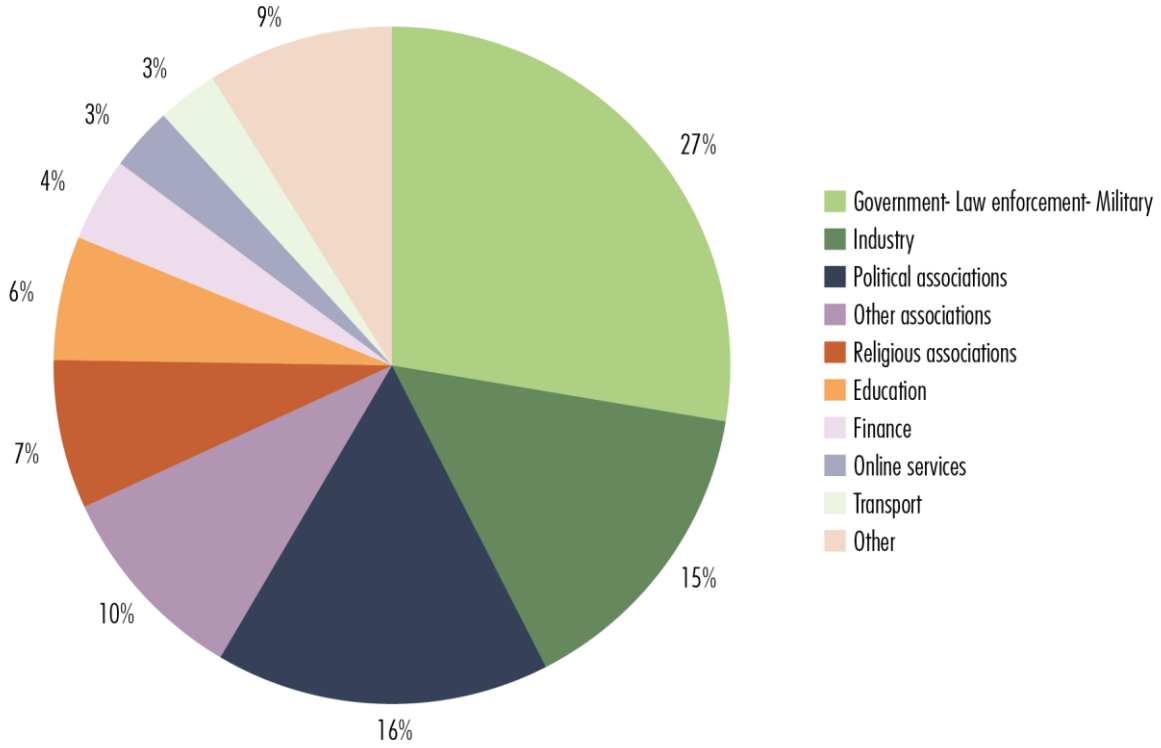
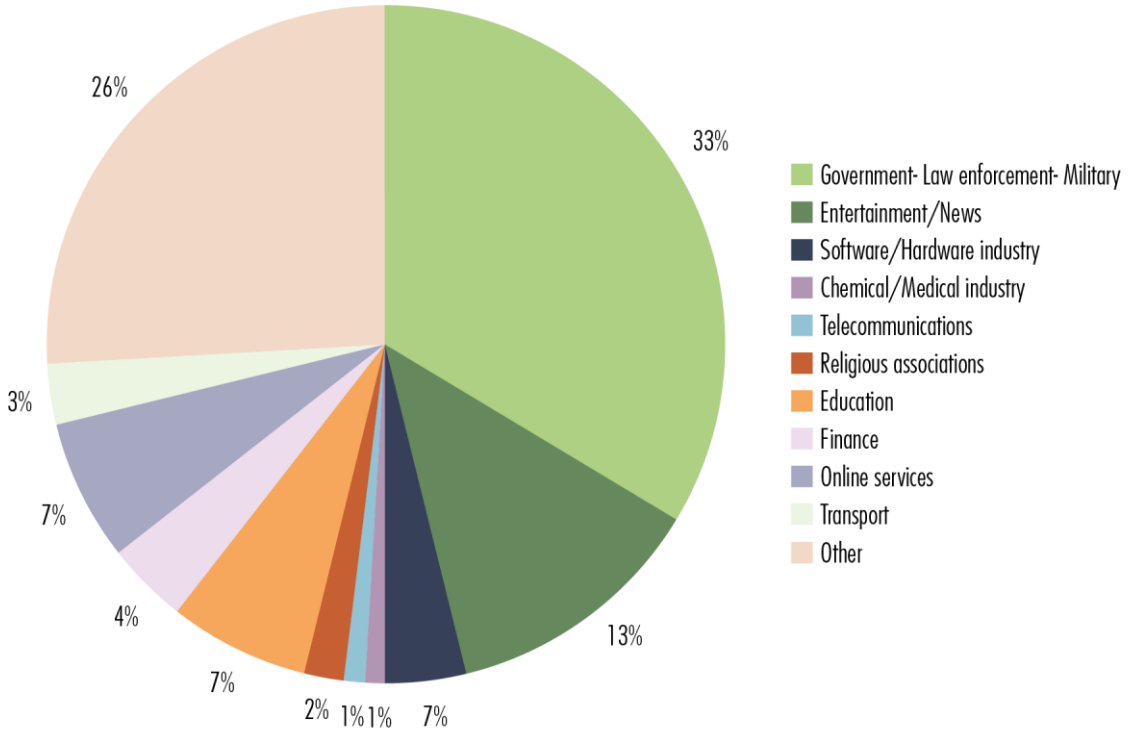


Figure 7 shows the segmentation of targeted organisations in 2011 according to the CLUSIT data for 2011.

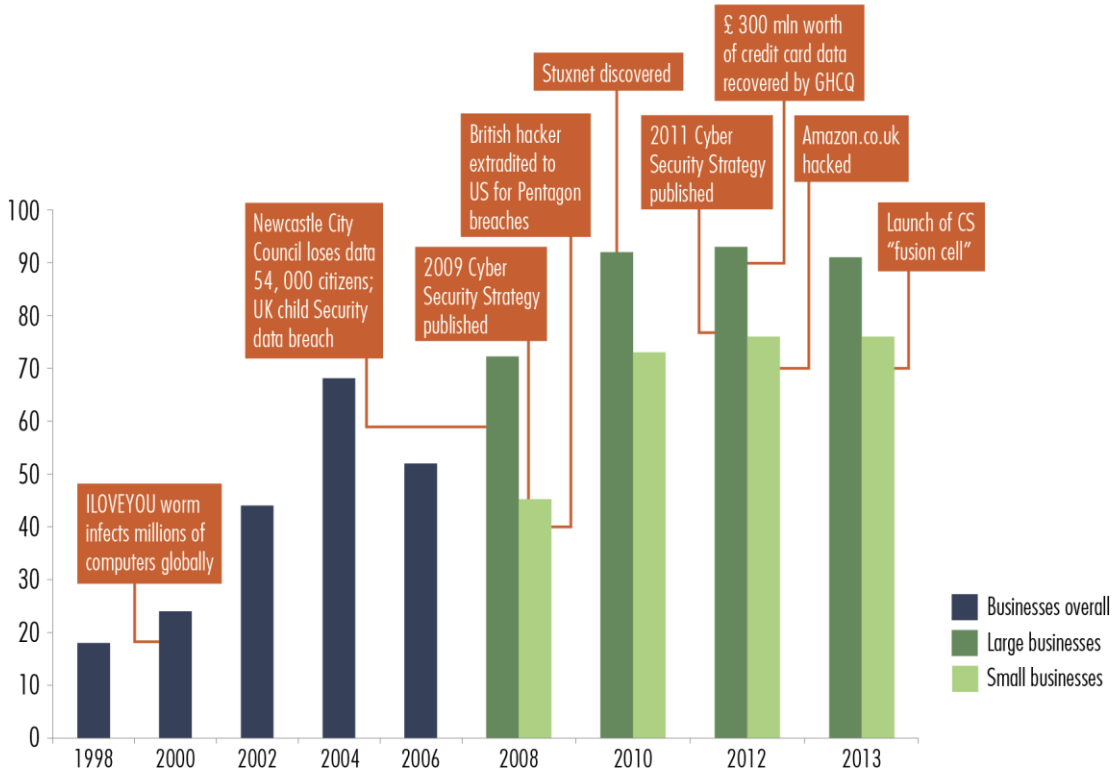
Figure 7 Targets by sector in Italy in 2011 (Source: CLUSIT)



There is longitudinal survey data for only a few European countries. For example, the annual report commissioned by the UK Department of Business Information Security Breach Survey (ISBS), compiled by approximately between 500 and 600 companies, provides biannual or annual data, broken down by size of the companies affected by the incidents.

For this study, we mapped major events in information security, such as law enforcement events, regulatory updates and major incidents on the timeline of reported incidents. As Figure 8 shows, beyond an overall largely upwards trend in information security breaches, increased spending on information security and policy actions such as the definition of cyber-security strategies and policy units have not been associated with a discernible limitation of the number of incidents. We have performed the same exercise for a number of other countries as well, with similar results.

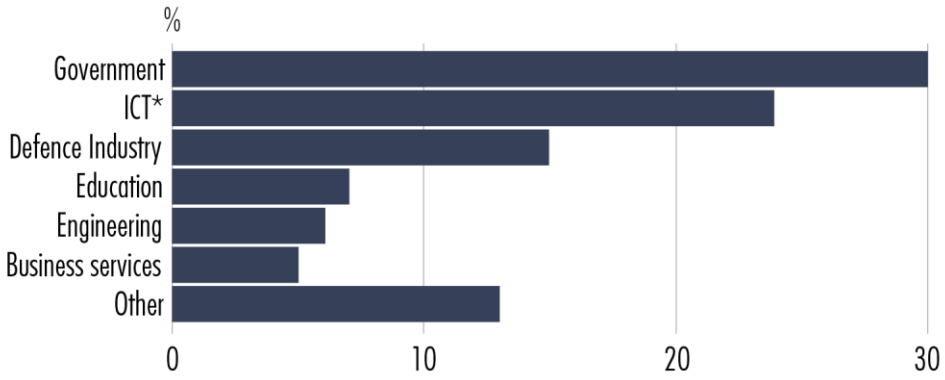
Figure 8 Percentage of firms experiencing an incident in the context of major events in the UK (Source: ISBS)



According to the data on sophisticated cyber attacks released by the UK Government Communications Headquarters (GCHQ), the government sector is targeted by almost a third of these, followed by the ICT industry and the defence sector.[71] However, these data only refer to a limited number of particularly sophisticated attacks (e.g. acts of cyber and industrial espionage) and can likely not be extrapolated to indicate the incidence of information security breaches in the wider economy.

[71] Limell, 2013.

Figure 9 Breakdown of targets of sophisticated attacks by sector per month in 2013 (Source: GCHQ)



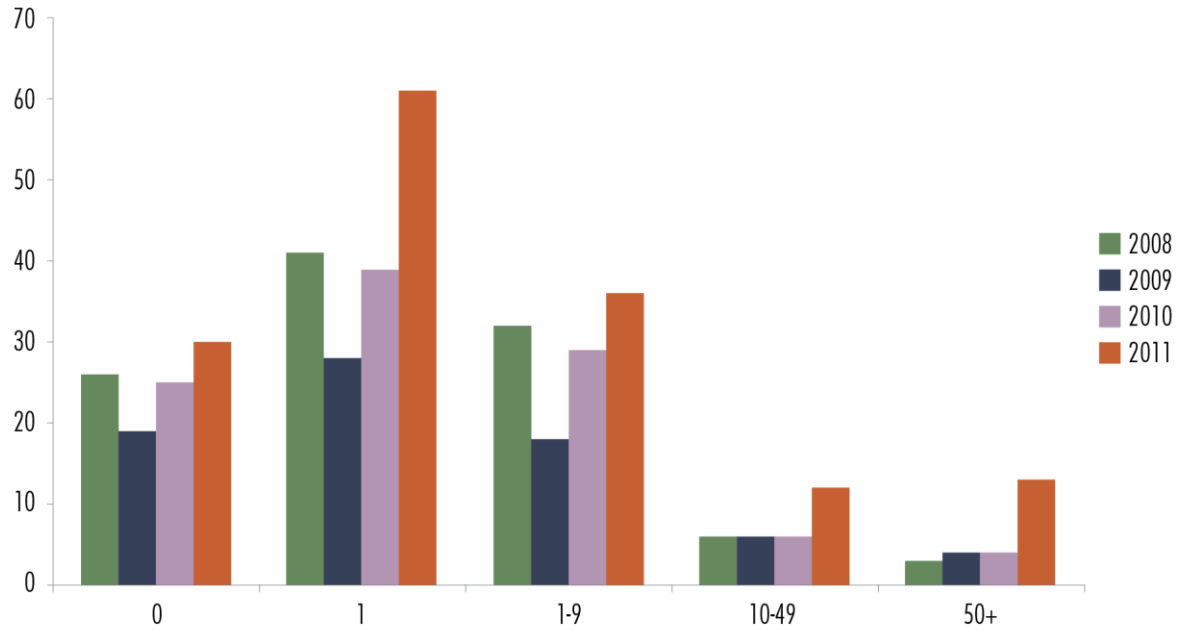
*Information and Communication Technology
Source: GCHQ

In France, the PwC Information Security Survey has provided a breakdown for country level data and by number of incidents that the approximately 600 surveyed companies had reported having suffered in the year preceding the survey.[72] By definition, these data sources do not offer insights into the absolute number of incidents that have taken place in a given time period, and survey respondents only recall the breaches and attacks they are aware of, which can lower significantly the numbers reported. These data offer insight into the gravity of the situation or the influence of security events in the country's economic and social life by reporting the scale on which economic operators and private users have to deal with security breaches.

Micro-level or interview data would also give insights into the dissemination of awareness and/or good practice and the degree to which (well-publicised, serious and/or reported) incidents potentially trigger adoption of better cyber-security practices or participation in joint initiatives to tackle the problem.

[72] PricewaterhouseCoopers (PwC), 2012.

Figure 10 Number of incidents reported by companies in France for the preceding year (Source: PwC, 2012)



3.1.3 Official statistics

Official statistical agencies at Member State and EU level (e.g. Eurobarometer surveys and Eurostat, see sections 3.2–3.5.) as well as CERTs and ENISA collect data on a variety of indicators related to cyber security.

In October 2012 ENISA published an analysis of the 51 serious incidents reported under the Article 13a regime to the Agency in 2011.[73] Over half (60%) of reported incidents in 2011 affected mobile telephony. Such mobile network outages affected many users (around 300,000) (see figures 11 and 12). In terms of root causes, hardware or software failures and third party failures were the most prevalent. Incidents with a root cause involving natural phenomena caused 45 hours of outage on average. Power supplies were also seen as a key secondary victim of natural phenomena having a subsequent impact on telecommunications. Another complicating factor was the limited battery life in infrastructure for mobile networks. Hardware or software failures hit mobile networks more than other services possibly due to higher complexity, less redundancy or more modern networks use hardware and software that is less mature and less reliable.

In August 2013 the analysis of incident reports submitted in 2012 was published by ENISA. Despite the Agency estimating in 2012 a ten-fold increase in the 2011 reported numbers because around half the EU Member States were not included in the Article 13a provisions,[74] only 79 reports were recorded. System failure was the most frequently occurring root cause (76%), followed by third party failure (13% of all reported incidents). Incidents with a root cause of natural phenomena caused the most lengthy outages (36 hours).

[73] ENISA, 2011a.
[74] Ibid.

Looking at the detailed root causes, hardware failure and software bugs proved to be the most frequently reported detailed causes (38% and 23% respectively).[75]

Figure 11 Percentage of incidents affecting different services, incidents reported under Article 13a to ENISA (most incidents affect more than one service) (Source: ENISA, 2012)

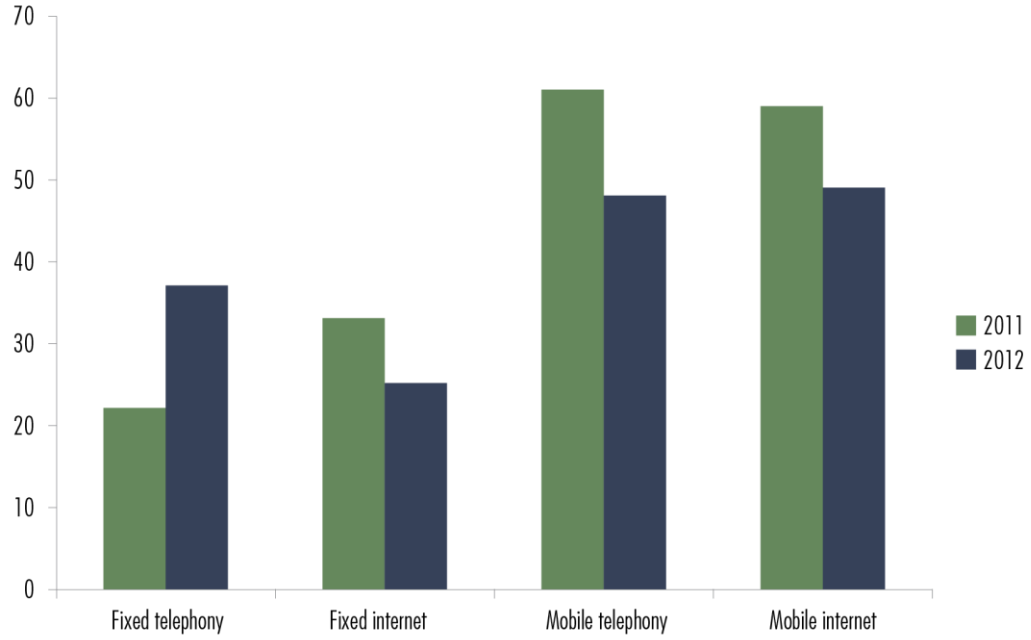
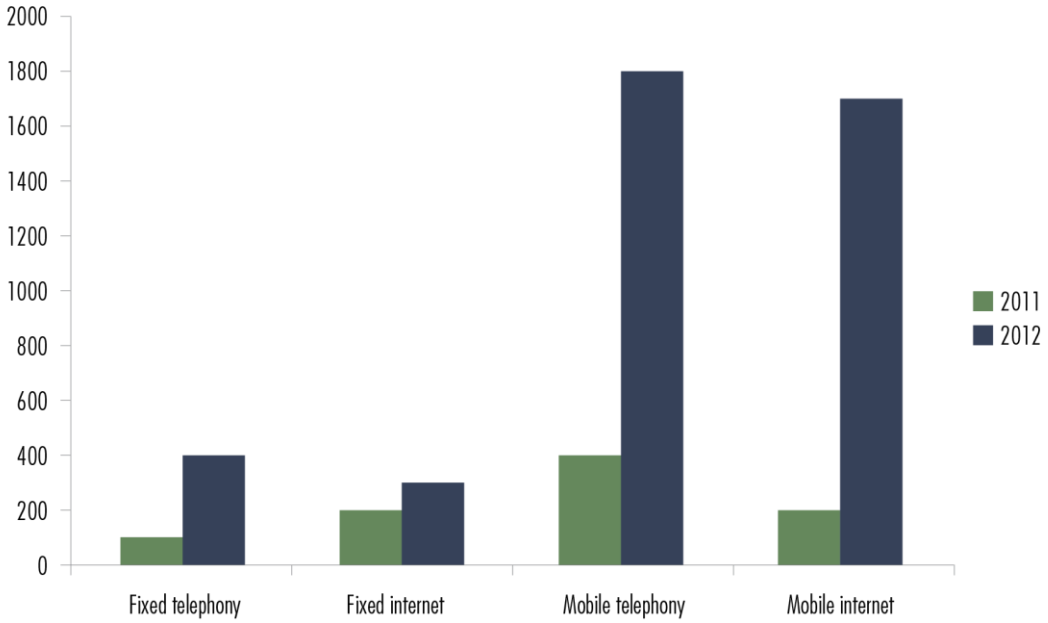


Figure 12 Average number of users affected by incidents reported under Article 13a (Source: ENISA, 2012)



[75] ENISA, 2013c.

Government CERTs (for a more in–depth discussion see Chapter 5) also collate data on their activities. These data by definition only represent the fraction of incidents reported to the CERTs whose share of the total number of incidents depends on the gravity of incidents, the reporting regime in place and the general awareness of the public of the incidents taking place. Although most European countries have one or more CERTs, the data reported by these organisations is often not comparable. CERTs have to deal with different types of constituencies and different types of incidents, and thus the quantity and quality of activities differ depending on whether academic or research institutions, governments, or the private sector are hosting and operating these CERTs. Therefore, statistics from e.g. an academic CERT cannot be compared with statistics provided by a national CERT or a CERT of a multinational enterprise. With no common rule of reporting, CERTs do not report the same categories of data. Some CERTs report only particular incidents, others only alerts and warnings issued, while a minority of CERTs also report the number of security management services provided. Common taxonomies have to be applied by CERTs to ensure that data collected are comparable. This is for instance the case for the concept of 'incidents', which sometimes includes different security-related events depending on the CERT. Furthermore, subcategories are sometimes difficult to compare because they are aggregated at different levels across CERTs.[76]

Challenges in interpreting data on incidents reported to CERTs are illustrated well by the fluctuations in the number of incidents reported in Denmark. While in 2007 a particularly high number of cases were reported, since that year there has been a steady decline. According to DK-CERT, the high number of cases reported in 2007 (the highest since 2004) were connected to vulnerabilities in Windows XP operational system and a large number of botnets and identity theft incidents. The CERT itself, while attributing part of the decline since 2007 to a general improvement in IT security (for instance the 2007 Service Pack released for Windows XP), notes that other factors, such as legal arrangements around the performance and detection of port scans and SQL injections, have contributed to the change in the number of reported incidents. Furthermore, it does not excludes the possibility of an evolution in computer crime in a direction that is not detected or reported to the CERT.[77]

[76] OECD, 2012.
[77] DK CERT, 2012; Jensen, 2008.

Figure 13 Total number of incidents reported to DK-CERT (Source: DK-CERT)

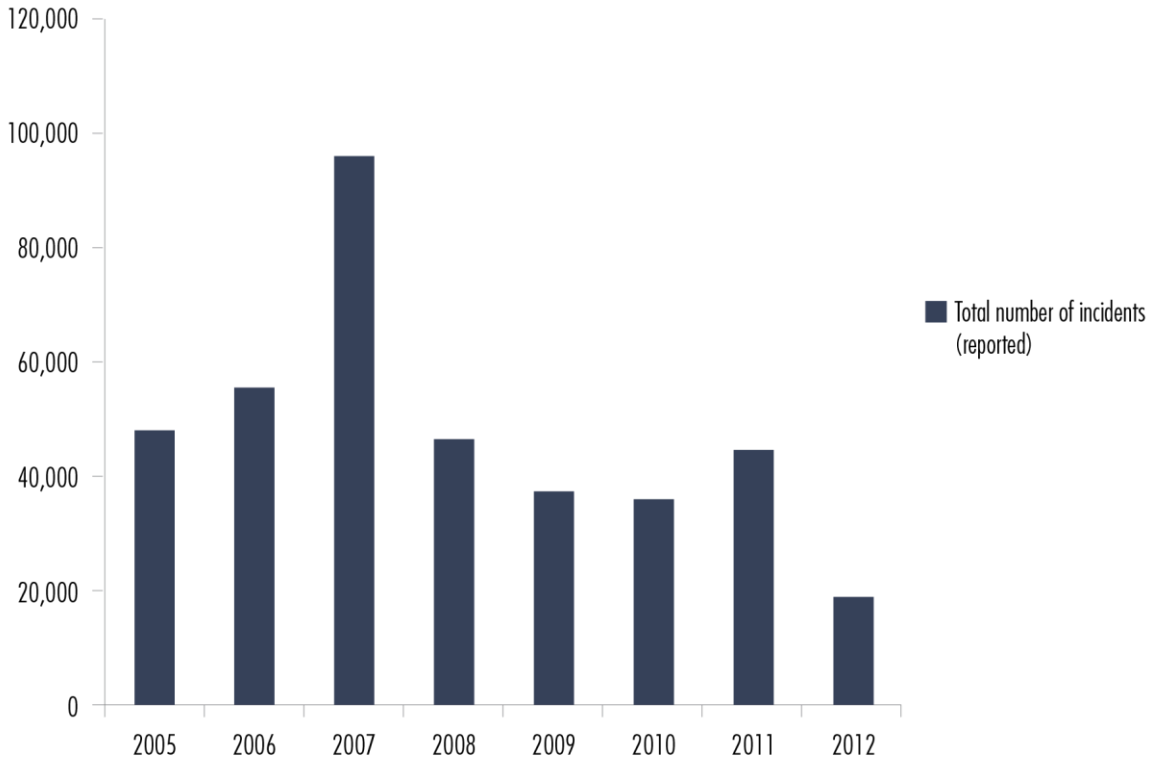
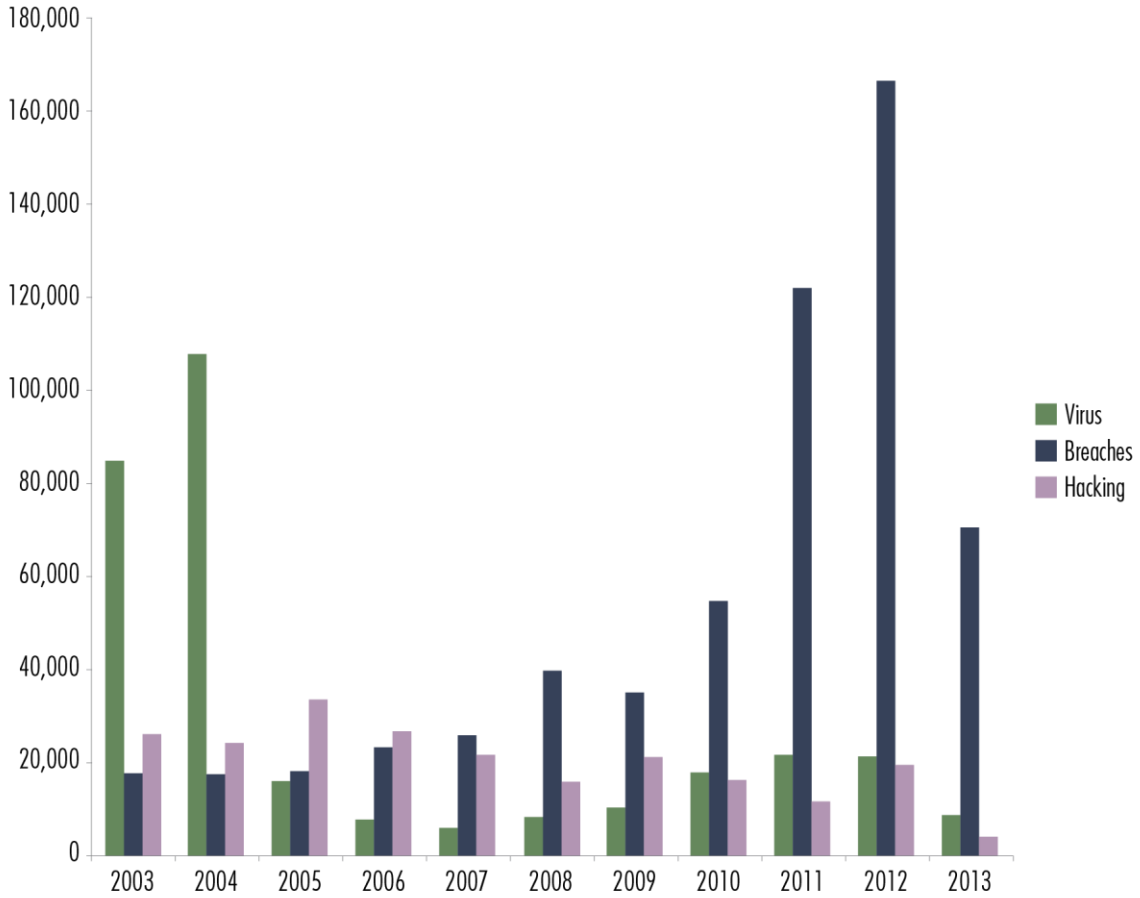


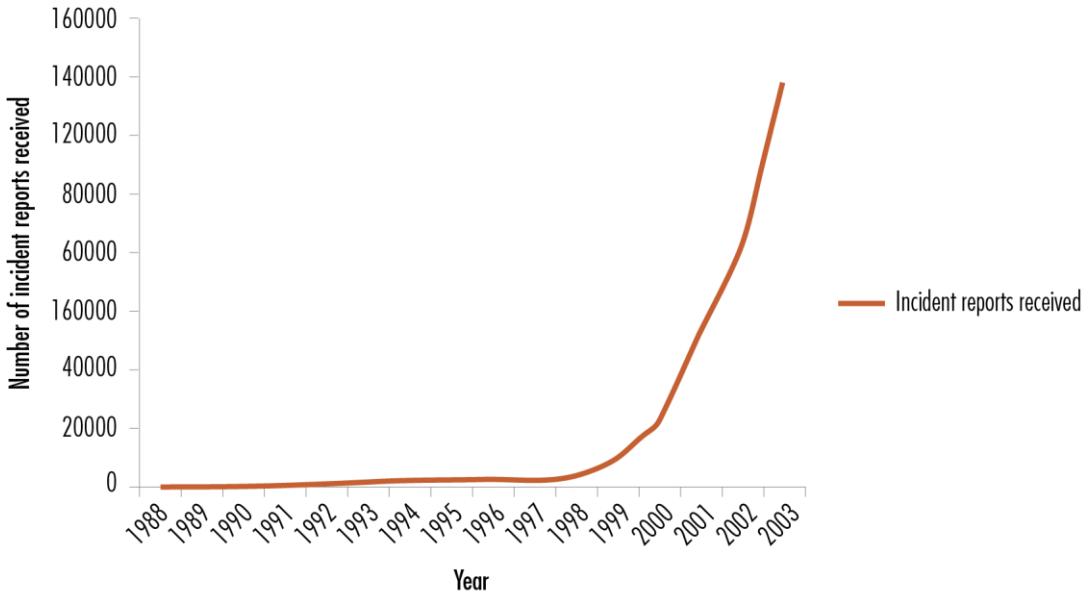
Figure 14 presents this data for South Korea between 2003 and 2013.

Figure 14 Information security breaches reported in South Korea (Source: Korea Communications Commission; Korea Information Security Agency)



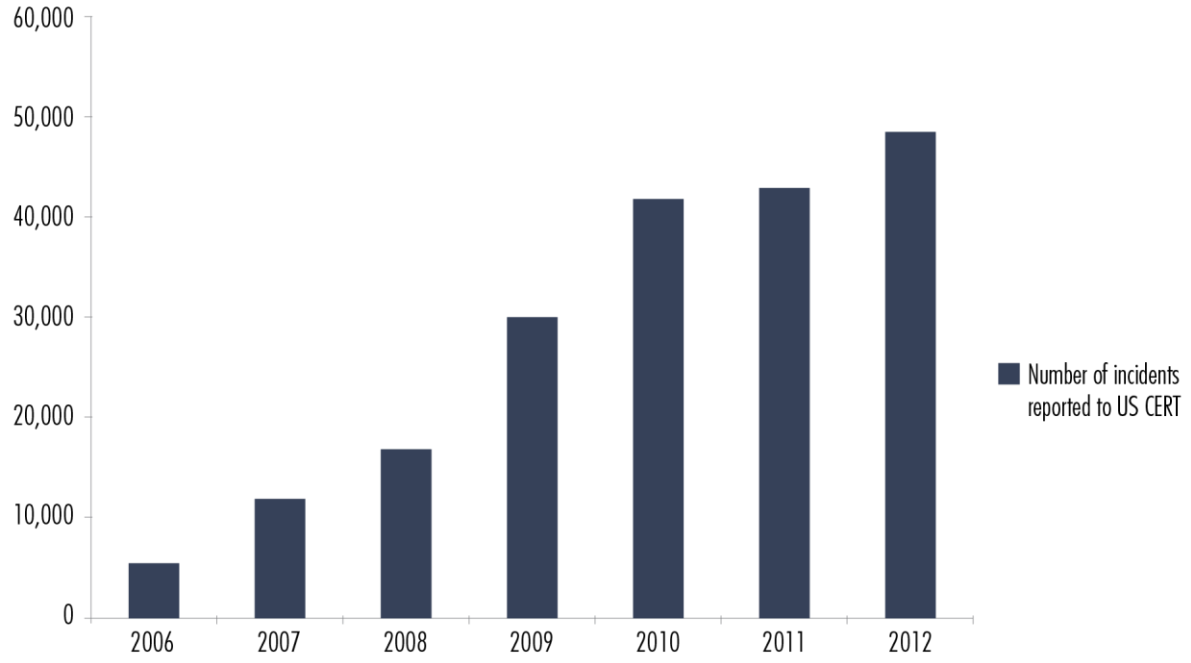
The CERT Co-ordination Center (CERT/CC) at Carnegie Mellon University (CMU) in the US collected incident reports from 1998 until 2003. At this time, according to CERT/CC, the use of automated attack tools meant that attacks became so commonplace that the collection of incident reports became meaningless as an indicator of their scale and the service was discontinued in 2003.

Figure 15 Incident reports received by US-CERT 1998–2003 (Source: CERT/CC)



However, as can be seen, the US-CERT established in 2003 (national level CERT in the US, which assumed some of the responsibilities of the CERT/CC) has continued collecting statistics, but it is hard to gauge based on the publicly available data to what extent these statistics capture the same sort of information.

Figure 16 The number of incidents reported to US-CERT 2006–2012 (Source: US-CERT)



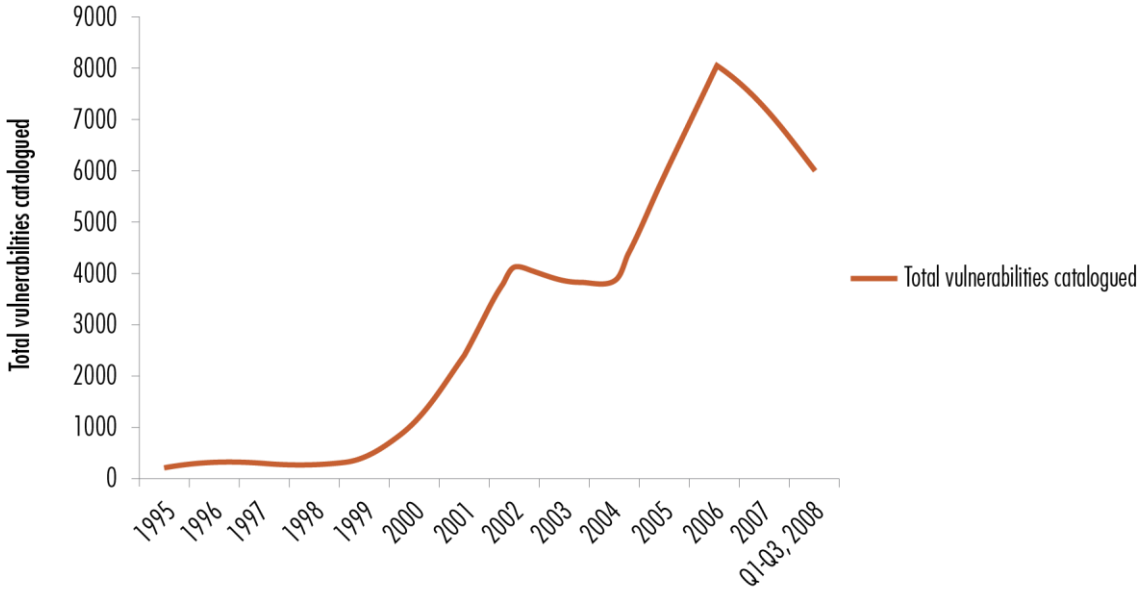
The CERT/CC was also cataloguing types of vulnerabilities until 2008. Figure 17 shows the number of new types of vulnerabilities catalogued by the CERT until Q3 2008 (not weighted by seriousness or the associated likelihood of attack).[78]

Although most European countries have one or more CERTs, the data reported by these organisations are often not comparable. CERTs have to deal with different types of constituencies and different types of incidents, and thus the quantity and quality of activities differ depending on whether academic or research institutions, governments or the private sector are hosting and operating these CERTs. Therefore, statistics from e.g. an academic CERT cannot be compared with statistics provided by a national CERT or a CERT of a multinational enterprise. With no common rule of reporting, CERTs do not report the same categories of data. Some CERTs report only particular incidents, others only alerts and warnings issued, while a minority of CERTs also report the number of security management services provided. Common taxonomies have to be applied by CERTs to assure that data collected are comparable. This is for instance the case for the concept of 'incidents', which sometimes includes different security-related events depending on the CERT. Furthermore, subcategories are sometimes difficult to compare because they are aggregated at different levels across CERTs.[79]

[78] A vulnerability can be defined (by Microsoft, for example) as 'a security exposure that results from a product weakness that the product developer did not intend to introduce and should fix once it is discovered'. Vulnerabilities cause a flaw in the logic working of the software and can be exploited to allow unauthorized access, elevation of privileges or denial of service by malicious software written purposefully to make use of these flaws. (Microsoft, 2013); see also Cencini, 2005.

[79] OECD, 2012.

Figure 17 Total vulnerabilities catalogued by CERT/CC 1995–2008 (Source: CERT/CC)



In some other Member States, such as Germany, official criminal justice statistics can provide an idea of the trends in incidents, but they also come with caveats since they are recorded crimes and therefore subject to different forms of bias. In Germany, interception of data – in particular industrial espionage – appears to be among the most salient threats to the German economy and businesses. In a particular case foreshadowing the recent National Security Agency scandal,[80] the German police and various Lander governments were exposed for their use of Trojans to monitor information systems (see Figure 20).[81]

Similarly, in the Republic of Korea, government bodies such as the Korean National Police Agency and the National Intelligence Service publish data on crime-related incidents and data involving public sector bodies, while the Korean Information Security Agency covers private sector businesses, as illustrated in figures 18 and 19. These statistics reflect a strong focus on criminalised incidents, hence overlooking incidents that can be linked to human error or external causes.

[80] In June 2013 UK newspapers published leaks revealing the details of mass data collection activities by the US National Security Agency among others in the framework of the PRISM program. For more on PRISM collection documents see e.g. PRISM Collection Documents published at the Washington Post website: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents

[81] Fitsanakis, 2011.

Figure 18 Sectoral breakdown of security incidents reported to the National Intelligence Agency, Korea (Source: National Intelligence Agency, Korea)

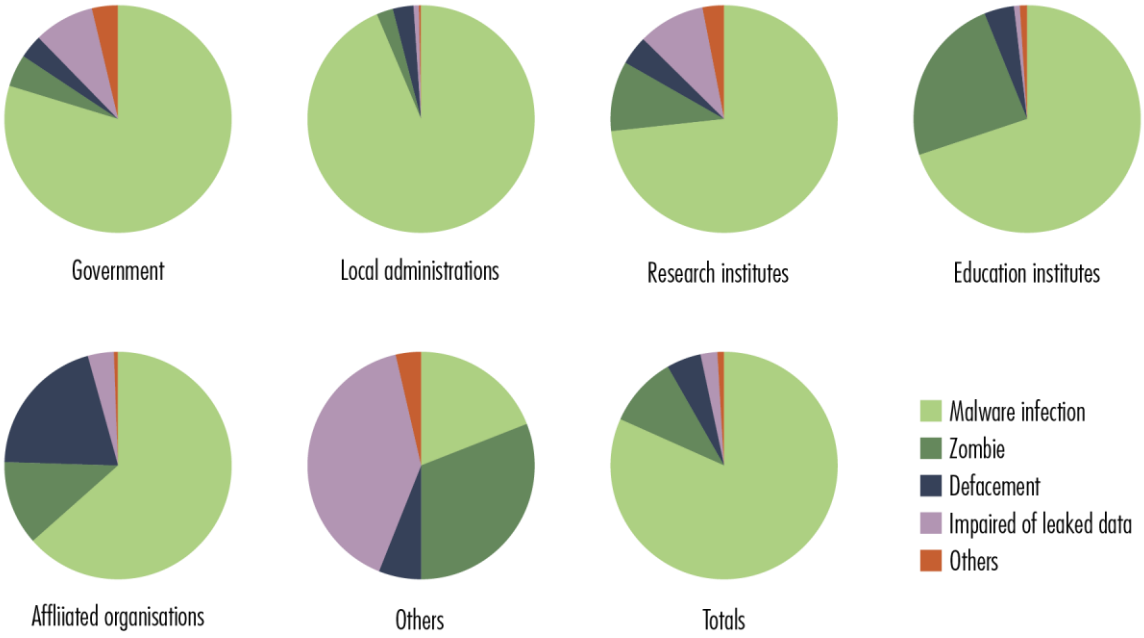


Figure 19 Trends in security incidents reported to the KNPA (Source: Korean National Police Agency)

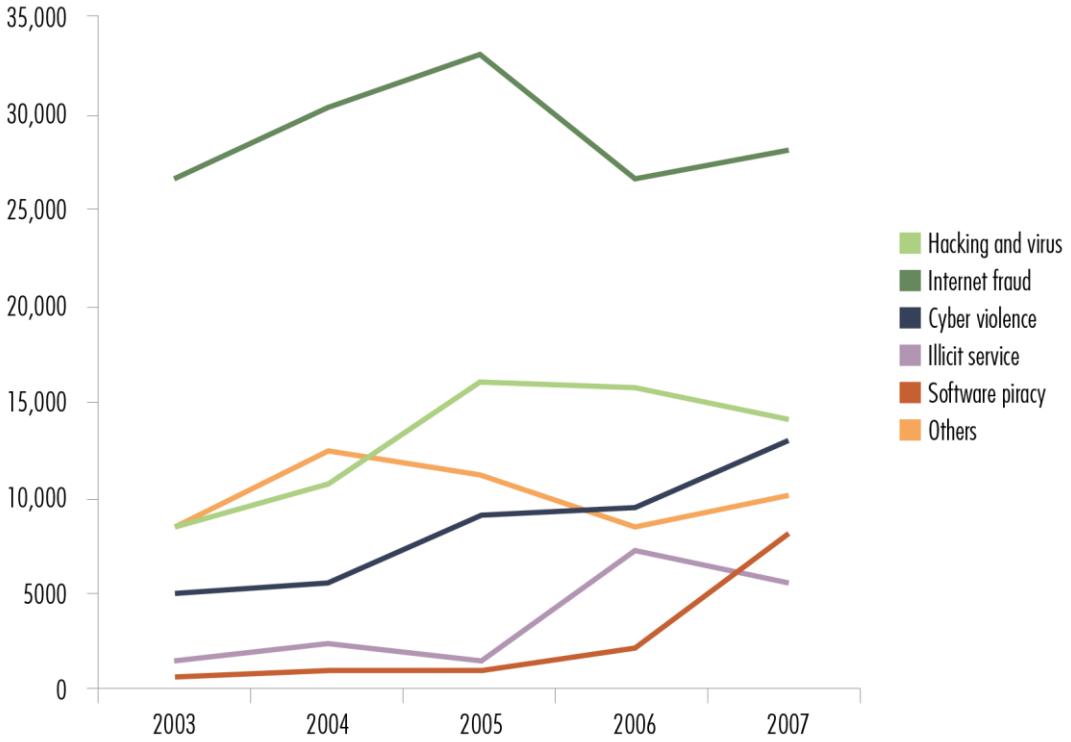
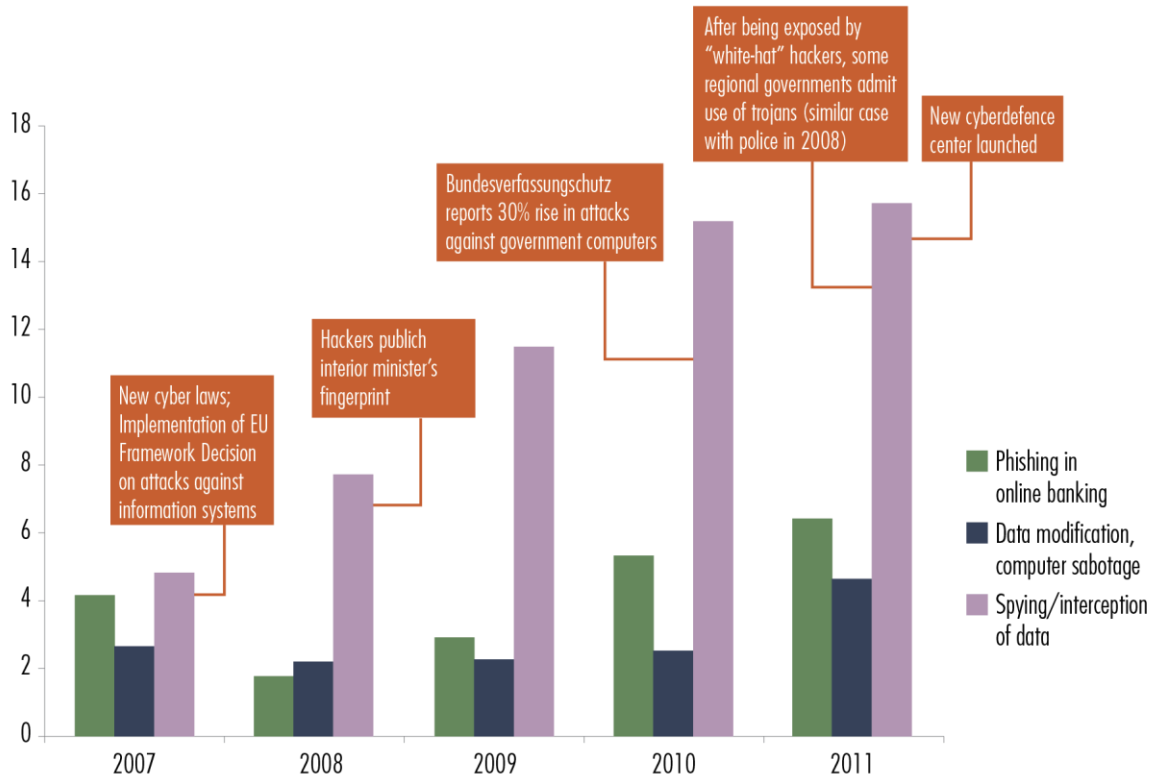


Figure 20 Number of reports of cyber crimes in Germany (000s) (Source: German Annual Crime Report, 2012)



3.1.4 Evidence from cyber security and technology companies

Technology companies and cyber-security firms also publish composite indices aiming to capture different aspects of vulnerabilities. However, comparing these numbers across different data sets and data providers can present challenges as there are no industry-wide standards for defining the variants of malware being taken into account. A well-known example is the index in the Microsoft Security Intelligence Report (SIR).[82] While these indices are useful in comparing data across countries and relatively large numbers of users, as well as making it possible to capture data on vulnerabilities regardless of the awareness level of the end-user, it has to be kept in mind that the depth of insight depends on the market share and reporting mechanisms of the company. Furthermore, these indices usually capture vulnerabilities as opposed to attacks or breaches that have taken place.

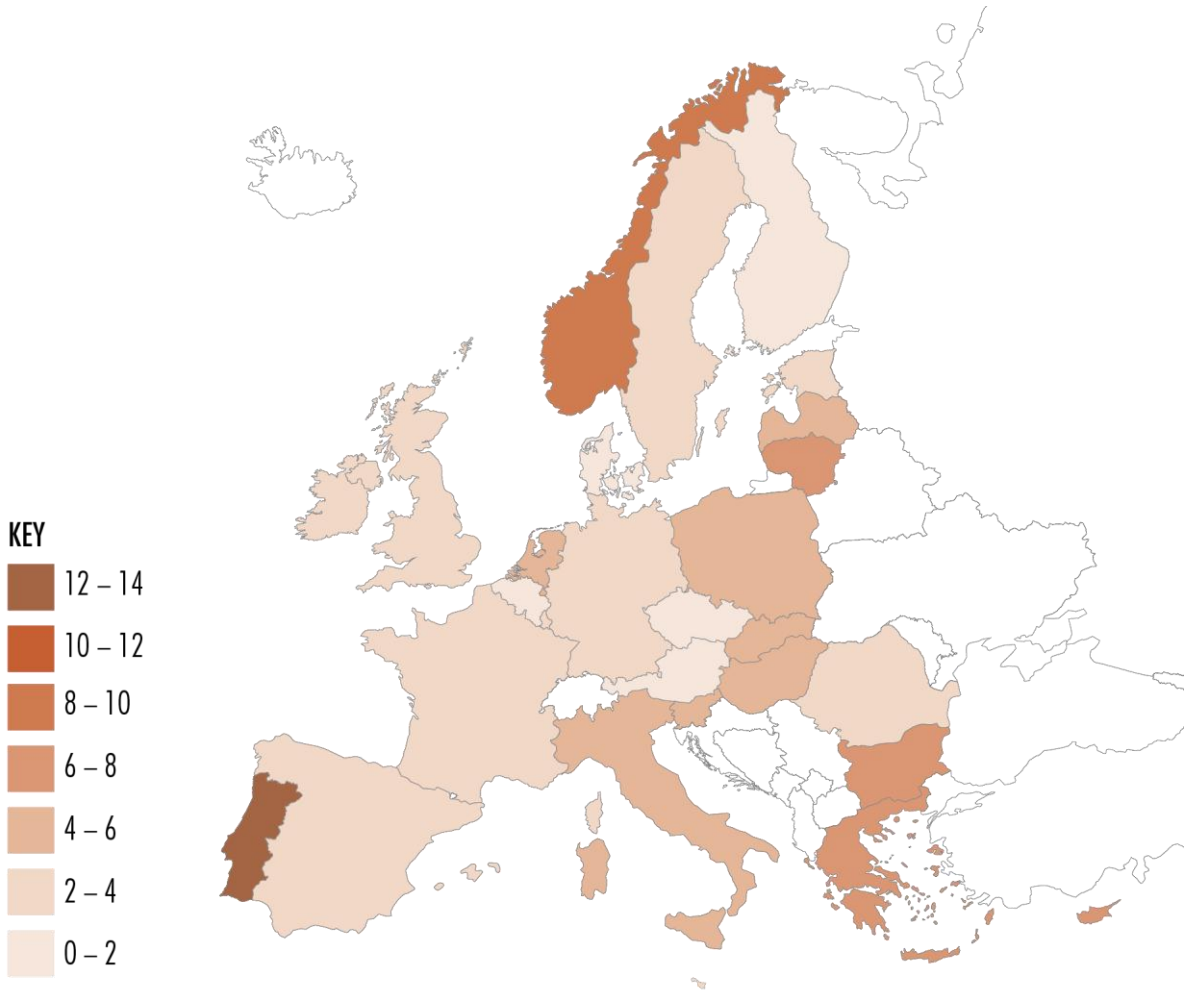
SIR data only reflect malicious code picked up by the Microsoft Malicious Software Removal Tool (MSRT) from those computers running (counterfeit or legitimate) copies of Windows – accounting for the bulk (85%) of operating system market. This may be seen as a measure of the vulnerability of computers running Windows operating system software.

[82] Microsoft, 2012.

Figures 21 to 23 illustrate the relative state of insecurity in European countries. The charts show an index of vulnerabilities detected and cleaned up by Microsoft's MSRT across a range of vulnerabilities in computers running official and unlicensed illegal copies of Windows operating system software.[83]

Figure 21 shows the Microsoft SIR index scores for EU countries in 2012, with countries scoring higher, e.g. presenting a higher level of detected vulnerabilities, showing in darker colours.

Figure 21 SIR scores (lower is better) for European countries 2012 (Source: Microsoft Security Intelligence Report, 2012)[84]



Some of the assumed correlations underlying these charts can be summarised as following. Wealthier nations (with higher GDP) are likely to possess more information or financial assets, therefore are a more attractive target for potential attacks and potential subjects for non-adversarial incidents such as involuntary data disclosure. Wealthier nations also have a higher average number of consumers (as illustrated by the correlation between GDP and online population), therefore presenting a wider range of possibilities for information security incidents, so we can expect higher SIR scores for richer countries.

[83] The measure of malicious software installed on computers does not necessarily equal the number of victims as these types of software are likely not exploited 100% on all infected computers.
[84] The scores related to the percentage of computers infected, detected by the MSRT software, see above.

At the same time, in richer countries we can also assume a greater willingness to pay for information security and a greater government and business interest in protecting the internet economy, while companies in stronger internet economies could also be more likely to incorporate higher security as a basis for competition in their strategies. We can also assume that internet users in these countries are better educated and more aware of the risks connected to information security breaches and therefore are more cautious in their transactions and more willing to pay for protective measures. The presence of outliers in figures 22 and 23 show that the large differences we encounter in the level of awareness and preparedness are likely the result of a combined impact of these (and other) policy and context variables, as no direct correlation between incidents reported and policy initiatives was found in the preliminary research conducted for this study.

Figure 22 illustrates the relative state of insecurity for countries with an online population *larger* than 15 million. There appears to be a clear correlation between GDP and total population online, but the number of vulnerabilities detected (as shown by the size of the bubble) does not always decrease in line with the growth of GDP (or with that of people using the internet). For instance, data for Spain show a much higher score than those of the Netherlands or Poland.

Figure 22 2012 Security Intelligence Report index to GDP and the online population (>15m) (Source: Microsoft Security Intelligence Report, 2012, and RAND Europe)

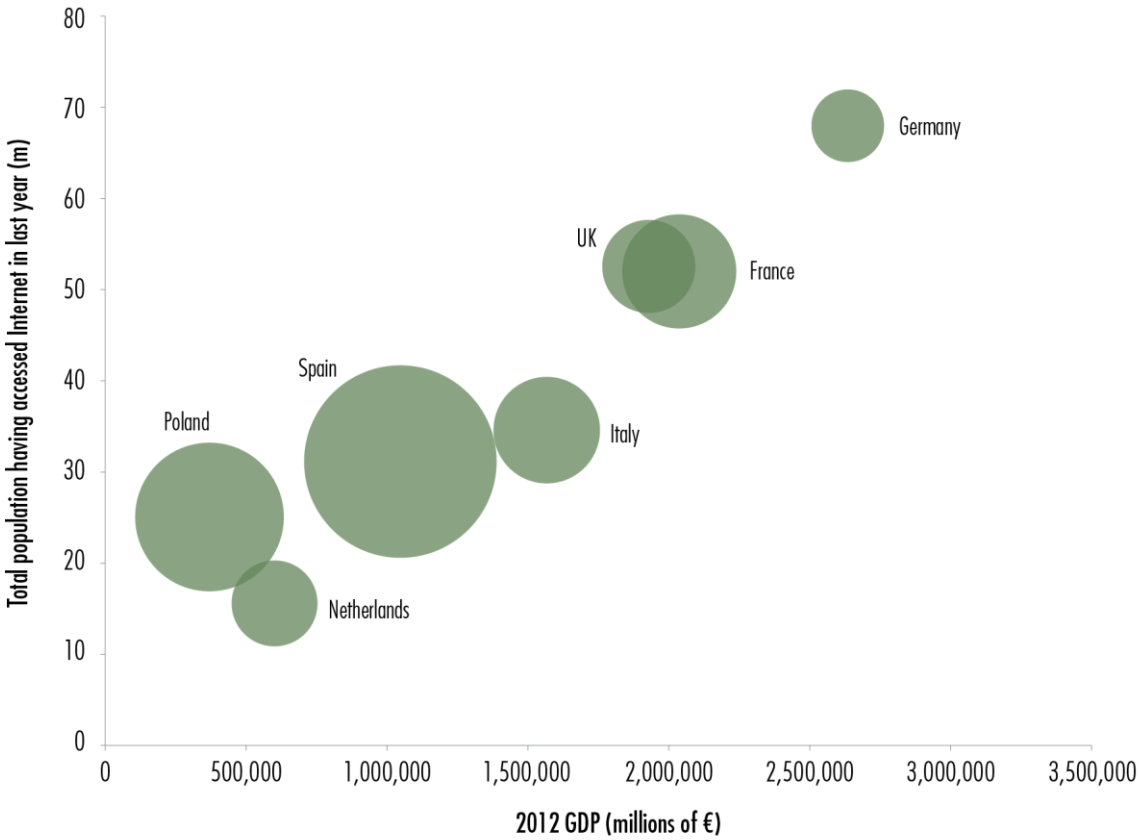


Figure 23 summarises the same data for countries with online populations of *less* than 15m. The correlation between GDP and online population as well as these two variables and the SIR score appears to be less strong than for countries with larger online populations.

In many cases, countries with lower GDP still present relatively high percentages of population using the internet. Furthermore, in these countries, higher GDP and larger online populations do not seem to be as strongly correlated with improved security as in the larger countries. In particular, Belgium, Greece, Hungary and Portugal appear to present a higher SIR score than countries in their respective clusters based on the other two variables.

Overall, based on regression analysis, higher GDP and higher numbers of internet users are both associated with a higher SIR score reflecting more malicious code discovered by the MSRT tool. The same statements also held true for GDP per capita measurements. Interestingly, after controlling for GDP and internet penetration, new Member States (which joined the EU since 2004) have significantly higher levels of vulnerability indices.

Figure 23 2012 Security Intelligence Report index to GDP and the online population (<15m) (Source: Microsoft Security Intelligence Report, 2012, and RAND Europe)

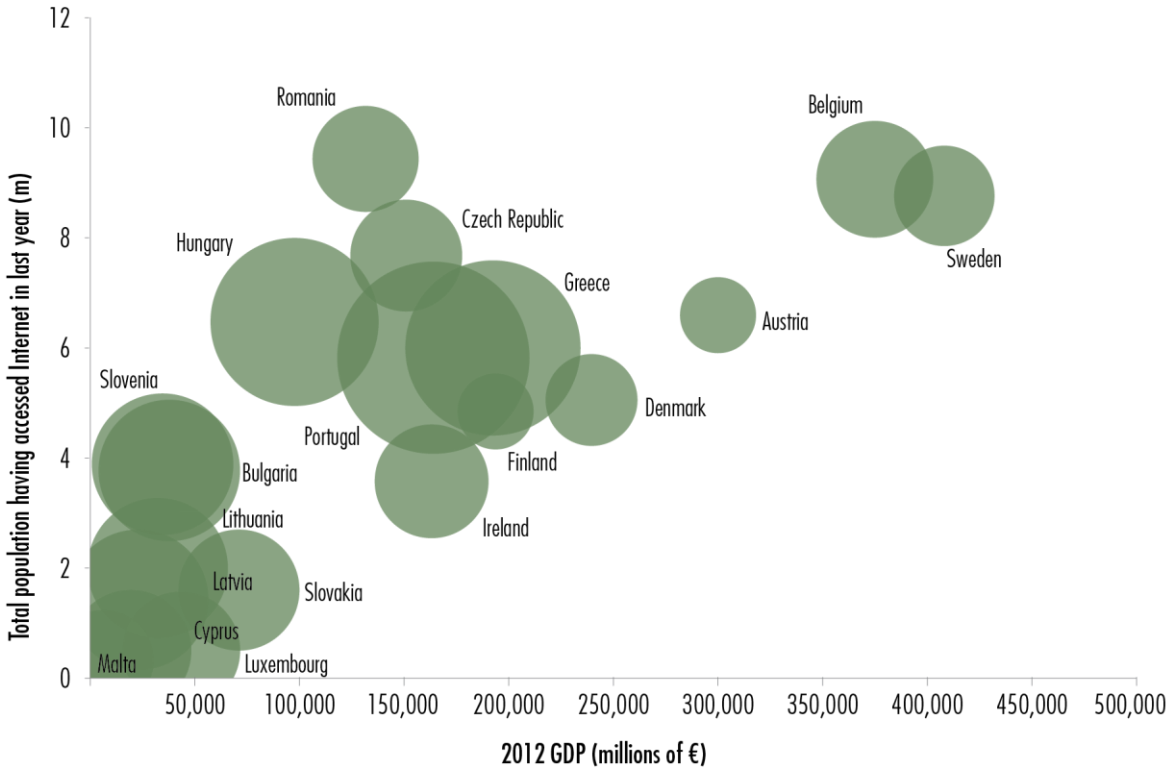


Figure 24 shows the degree of change between Microsoft's security intelligence report score for 2010 and 2012. As can be seen there are a few outliers: Romania, France, Poland, Greece, Hungary and Spain have shown significant changes between the two periods of measurement. The root cause of these changes, e.g the equlibrium between the relationships outlined in the introductory paragraph (such as the relationships between wealth as a driver for security and better security awareness of users as an outcome versus wealthier countries presenting more attractive targets) warrants further detailed investigation.

Figure 24 Annual rate of change 2010–2012 for SIR index

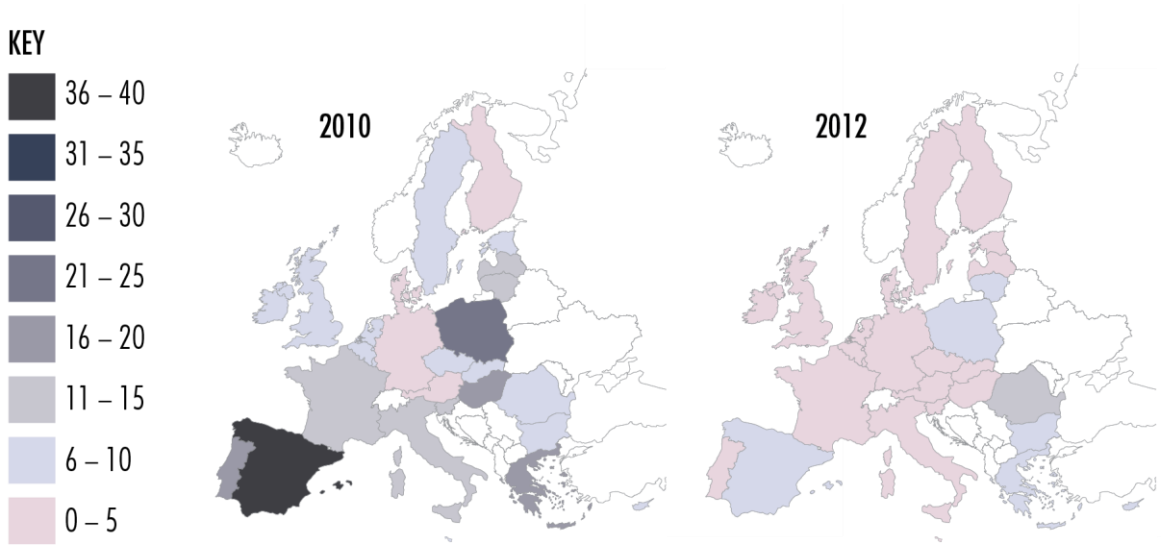
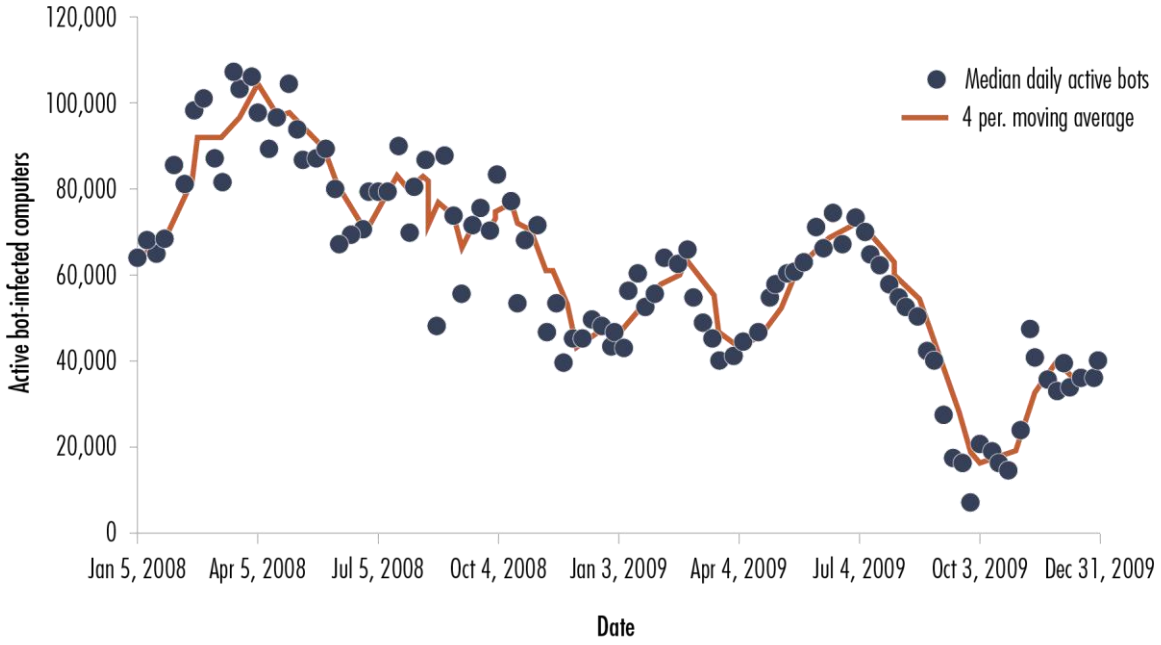


Figure 25 shows the median daily active bots (compromised computers participating in a botnet) recorded by Symantec for the period January 2008 to December 2009.[85]

Figure 25 Median daily active bots 2008–2009 (Source: Symantec, 2009)



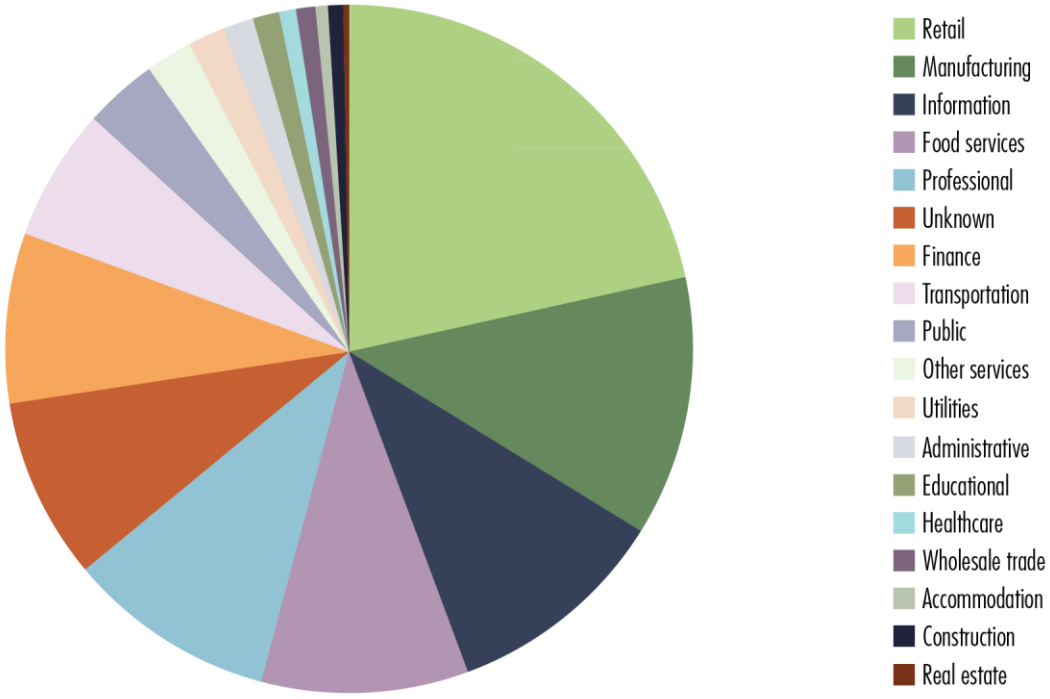
Verizon's 2012 Data Breach Investigations Report analyses data on 621 breaches captured in more than 20 countries.[86] It focuses on data breaches as opposed to information security breaches (for definitions please see Chapter 2). Besides the obvious limitations due to definitions and sample bias, it offers a useful breakdown by industry. Although financial services and healthcare are often among the industries captured as most exposed to data breaches, a large proportion of these are often not cyber-security related (e.g. ATM frauds in the financial sector often do not involve computer systems but scanners applied on card-reading machines, cameras installed over ATMs or other methods).[87] When filtered for breaches perpetuated through network intrusion, the retail, manufacturing and information services presented the highest incidence of breaches.

[85] The term bot (short for robot) is used to designate a computer infected with malicious software allowing outside actors to control it. Bots are used to perform automated tasks without the user's knowledge. Large numbers of connected infected bots are called a botnet and are often used , among other purposes, to send out spam e-mail messages, spread viruses, attack computers and servers. However, not all malicious software installed on computers means that those computers are actively functioning bots at any given moment. Therefore, the charts illustrate the median daily activity of these (see Microsoft, 2013b).

[86] Verizon, 2012.

[87] See e.g. Sharme, 2012.

Figure 26 Data breaches through network intrusions, by victim industry (Source: Verizon, 2012)



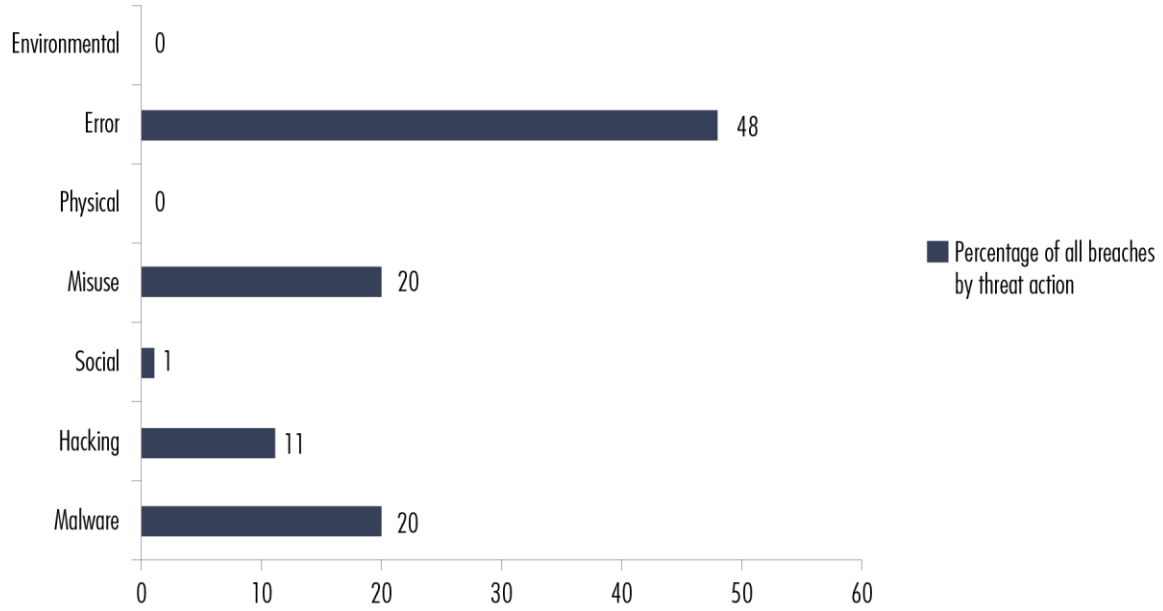
The analysis of connections between actions and assets illustrated in Figure 27 shows that the most relevant targets of actions differ according to the type of threat. For instance, physical threats (a darker cell) are most frequently related to a user's account while social engineering practices target the people with access to the system.[88]

Figure 27 Analysis of threat actions by assets (Source: Verizon, 2012)

[88] The expression 'special engineering' in a security context refers to incidents in which an information system is penetrated through the use of social methods, for instance by persuading an individual to give up confidential information through disguising the attacker as a trustworthy person of authority (See e.g. Tetri and Vuokkinnen, 2013.

At the same time, the assessment for the whole database of more than 47,000 information security breaches (not only data breaches) captured by Verizon's tool shows that overall error, misuse and hacking are the most persistent threats to information security, and environmental and physical threats are associated with less than 1% of breaches. Figure 28 shows the relationship between different types of threats from Verizon's database.

Figure 28 Categories of threat action (Source: Verizon, 2012, and RAND Europe)



3.2 Costs of breaches

Evidence on the costs of related phenomena is even harder to acquire for all Member States. The US-based Ponemon Institute has conducted studies based on in-depth examination of data breach costs (those relating to loss of confidentiality of personal data held by organisations) in a very limited number of organisations (between 15 and 30 for each country surveyed).[89] While a small sample size prevents us from generalising industry cost differences, technology, financial and consumer product companies tend to have a per capita cost above the mean and retail, public sector and service companies have a per capita cost significantly below the mean in Italy.

Costs associated with data breaches were often highest in heavily regulated industries, such as financial and pharmaceutical businesses. The average per capita cost across the four European countries surveyed was €153 for financial businesses, and €119.5 for pharmaceutical companies, above the overall average cost of €118. Public sector organisations had among lowest per capita cost, at an average of €78 across the four countries.

[89] See e.g. Ponemon, 2013.

Figure 29 Costs of data breach per record by sector in 2012 (Source Ponemon, 2013)

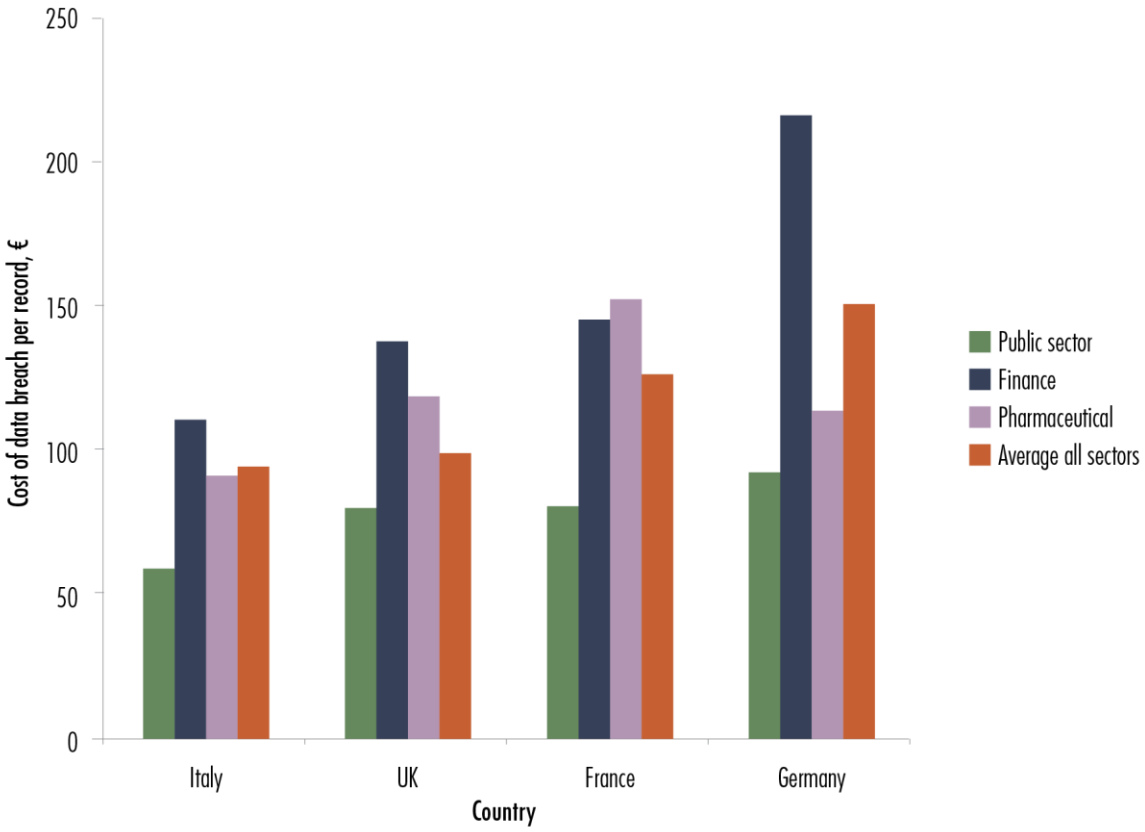


Figure 30 shows the total cost of data breaches at country level for all sectors covered by the small sample size in the Ponemon study across a number of countries.

Figure 30 Organisational cost of individual breaches by country across all sectors in 2012 (Source: Ponemon, 2013)

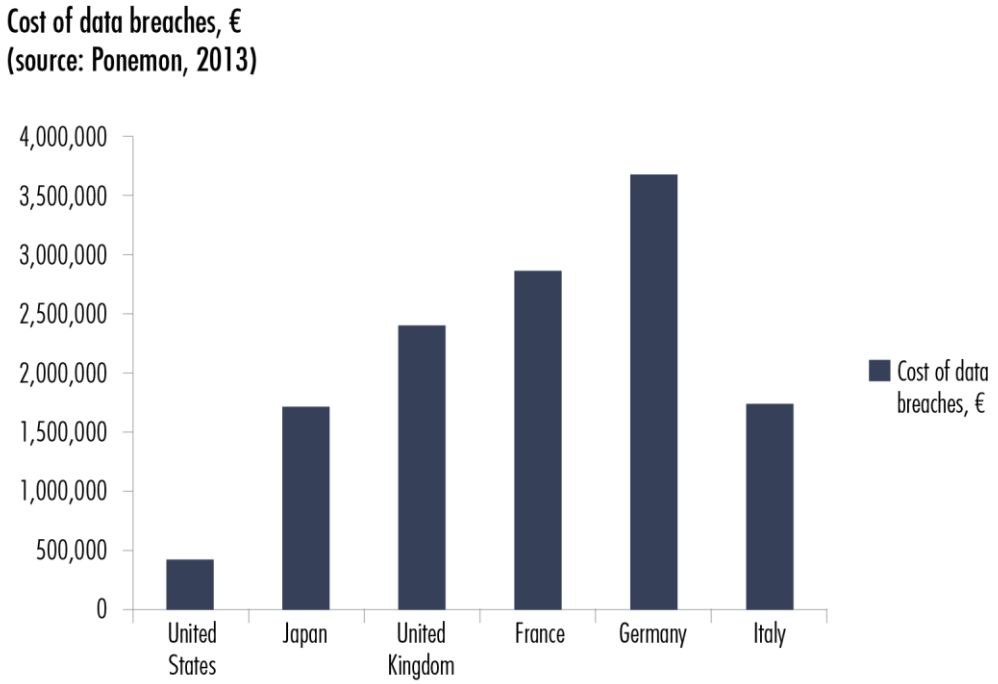
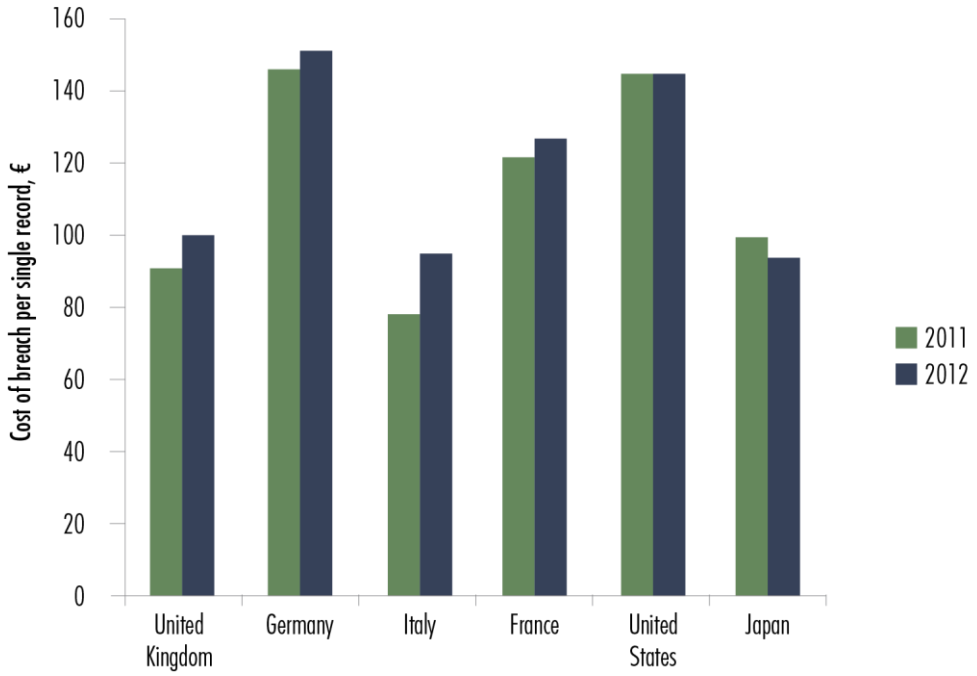


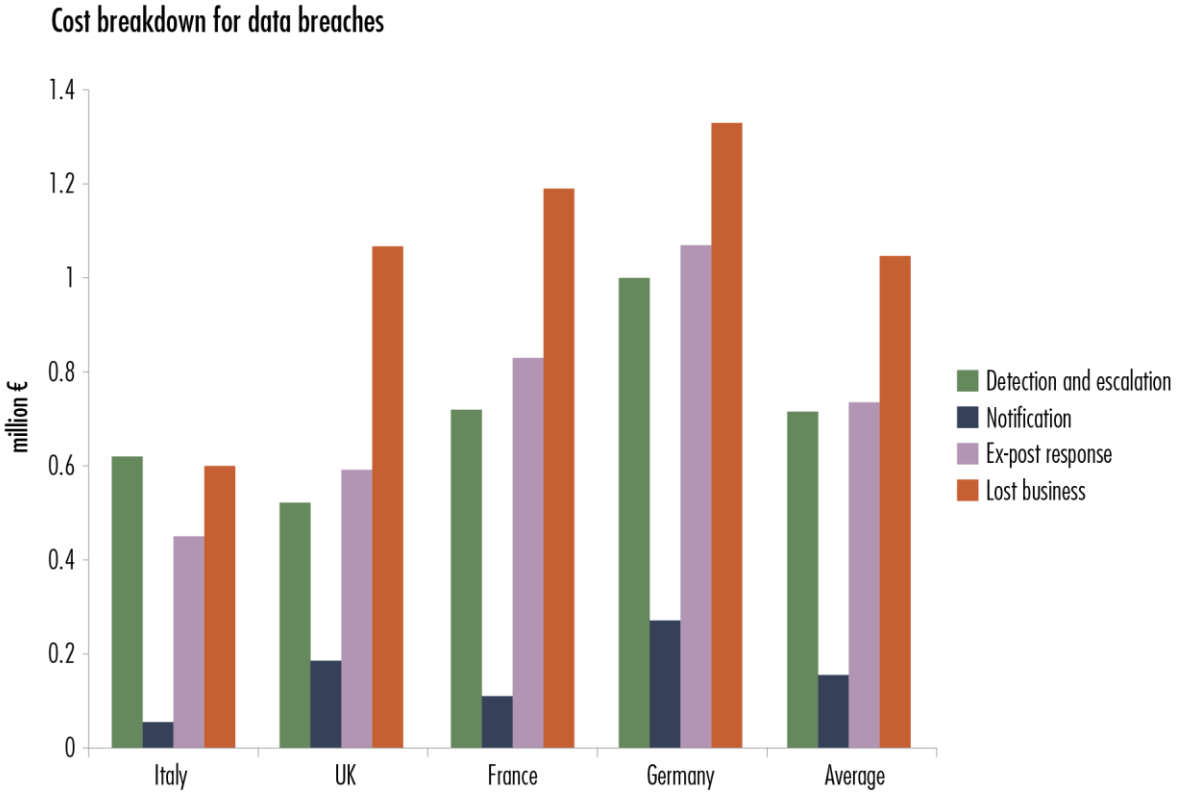
Figure 31 shows a comparison of the costs of data breaches in 2011 and 2013 reported by the Ponemon Institute. Excepting Italy and Japan, there appear to be no significant differences. In Italy, the costs have appeared to increase markedly relative to the others in the figure, whereas Japan is the only country recording a decrease.

Figure 31 Costs of data breaches in 2011 and 2012 (Source: Ponemon, 2013)



The breakdown of costs associated with the breach described shows that lost business, and immediate and ex-post response are significantly more important expenses than those of notification, amounting to an average of approximately €155,000 per breach.

Figure 32 Cost breakdown for data breaches in 2012 (Source: Ponemon, 2013, and RAND Europe)



Another study, again focusing on breaches of personally identifiable information, which analysed the outcomes of data breaches in 117 US firms occurring between 2005 and 2010, has found that the average cost per data breach was approximately $2.4 million (approximately €1.84m) – the equivalent of $5 (approx. €3.83) per corrupted file, incorporating costs occurred for crisis services (forensics, notification, credit monitoring and legal counsel), legal damages (defence and settlement), business interruption costs and fines.[90] Like the Ponemon studies, notification costs are relatively minor, but these data also includes defence and settlement costs, which may be regarded as somewhat unique to the US given the differing legal systems.

[90] Greisiger, 2011.

Figure 33 Average costs per breach from 2011 reported by 117 firms (Source: Greisiger, 2011)

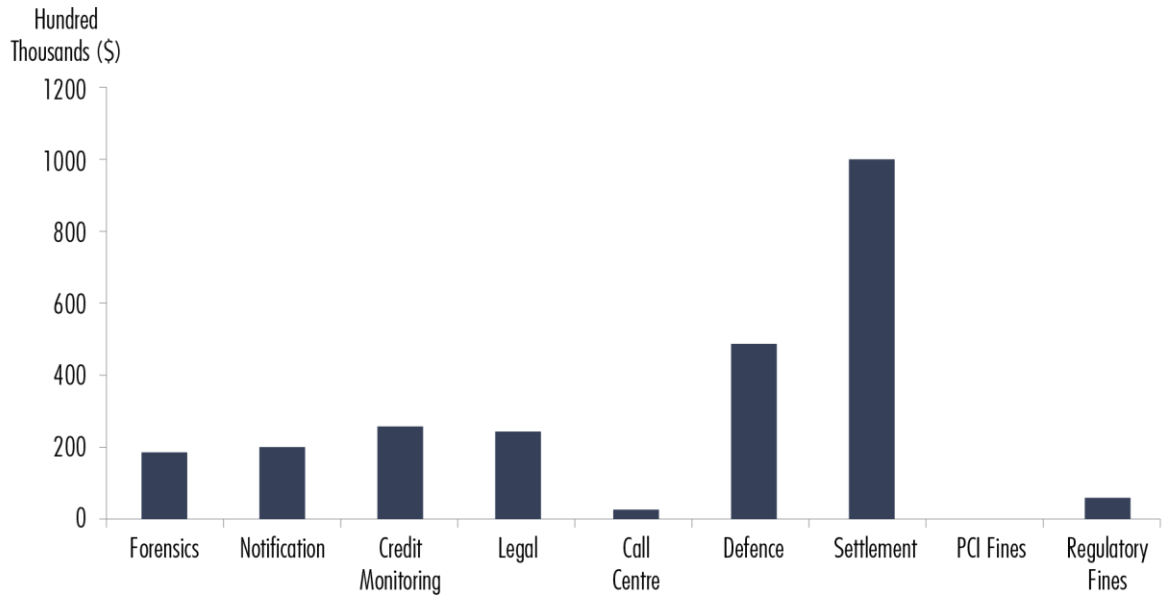


Table 7 lists the costs related to breaches in 2011 and 2012 taken from data from the same research in 2012, based on 137 successful claims by organisations possessing a cyber liability or 'data breach' insurance product.

Table 7 Analysis of costs from 137 claims made by US firms on data breaches of personally identifiable information in 2009–2012 (Source: Greisiger, 2012)

Item	Costs
Average cost per breach 2012	$3.7m (approx. €2.79m)
Average cost per breach 2011	$2.4m (approx. €1.81m)
Range of breaches	$2k–76m (approx. €1.5k–57m)
Typical claim	$25–200k (approx. €18,850–150,800)
Average cost per record	$3.94 (approx. €2.97)
Average cost of defence	$582k (approx. €438,850)
Average cost of settlement	$2.1m (approx. €1.58m)
Average cost for crisis services	$983k (approx. €741,215) per event

In the UK we can analyse costs relating to all kinds of incidents, not just those affecting the confidentiality of personal data or personally identifiable information.

Relatively few studies of this kind exist that would allow an international comparison, although the mean financial loss from computer security events against Australian businesses is estimated to be $4,469 per incident (approximately €3,103), with mean losses of $2,431 (approx. €1,688) for small businesses and $49,246 (approx. €34,204) for large businesses, according to a survey conducted by the Australian Institute of Criminology in 2006–2007.[91]

Table 8 gives ISBS definitions of costs attributed to information security breaches by company size in the UK in 2013.

Table 8 Cost breakdown for information security breaches by company size (Source: ISBS, 2013; own calculations)

Type of cost	Small businesses (ISBS 2013)	Large businesses (ISBS 2013)
Business disruption	£30,000–50,000 (approx. €34,836–57,940) over 3–5 days	£300,000–600,000 (approx. €348,360–695,274)
Time spent responding to incident	£2,000–5,000 (approx. €2,322–5,793) 6–12 man days	£6,000–13,000 (approx. €6952–15,064)
Lost business	£300–600 (approx. €348–695)	£10,000–15,000 (approx. €11,587–17,388)
Direct cash spent responding to incident	£500–1,500 (approx. €580–1,738)	£35,000–60,000 (approx. €40,574–69,527)
Regulatory fines and compensation payments	£0 (€0)	£750–1,500 (approx. €869–1,738
Lost assets (including lost intellectual property)	£150–300 (approx. €173–348)	£30,000–40,000 (approx. €34,836–46 370)
Damage to reputation	£1,500–8,000 (approx. €1,738–9,289)	£25,000–115,000 (approx. €29,030–133,260)
Total cost of worst incident on average	£35,000–65,000 (approx. €40,574–75,321)	£450,000–850,000 (approx. €521,455–984,969)
Total direct costs	£2,950–7,400 (approx. €3,418–8,575)	£51,750–129,500 (approx. €59,967–150,124)

[91] Richards, 2009.

3.2.1 Extrapolating from ISBS to an EU-wide estimate

As we have seen, the estimates listed in the previous paragraphs cover a wide range of values in terms of frequency, distribution and cost of breaches. To illustrate this we have conservatively estimated the costs incurred by companies at country level, based on the Eurostat special module data on incidents and the lower estimates of direct costs from the ISBS 2013 data, as the data from Eurostat appear significantly at odds with those from other sources presented in this report.[92] For example, the 2011 Eurostat special module on cybersecurity reports that only 1% of SMEs were affected by some categories of security incident. Even accounting for the differences in absolute numbers of SMEs in different-sized countries, when set against data such as the UK ISBS, this would appear to be a low figure. Hence, the Eurostat data should be taken as a very conservative estimate.

Furthermore, we exclude figures extrapolating from reported indirect costs in the ISBS data because they reflect an estimate of the costs from the worst or biggest incident from the respondents. Nonetheless, it is important to note that as we have seen, indirect costs (lost business) are very often the biggest cost to business (but by far the hardest to measure).

Finally, we make the following assumptions, taken from the ISBS 2013 data, which demonstrate that interpretations of our extrapolations should be taken with great care:

- We assume that each company that has reported having had an incident in the previous year has had one incident of that type, as there are no data on the frequency of incidents.
- The estimates do not include eventual scale effects to costs if a company has had multiple types of incidents (if you have three incidents, it might cost less than three times the costs of one) as no data is available on how many of the companies have had multiple incidents.
- We assume that the direct cost of incidents is comparable or similar to those reported by companies in the UK.
- We assume that the distribution of costs is uniform across size groups (UK data were reported for small companies <250 employees and large companies >1,000; EU category SMEs 10–249 and large 250+).

The results suggest that ICT-related incidents of a malicious nature could incur direct costs more than €560m per year for SMEs while all types of incidents (including data loss due to hardware or software failures, which we took also as including upstream environmental or physical problems such as natural disasters) could incur direct costs of more than €2.3 billion across SMEs. If we look at all companies employing more than 10 employees, (adjusting the cost estimate for the lower range of direct costs breakdown reported by large firms in the ISBS 2013 survey), the figures are respectively €935.8 million for malicious incidents and €4.151bn for all sources of incidents.

[92] Eurostat Special module 2010: Internet Security (isoc_ci_sc) Enterprises – ICT security policy, incidents and measures taken (isoc_ci_sce): http://epp.eurostat.ec.europa.eu/portal/page/portal/information_society/data/database?_pireff296_1906068_296_1905938_1905938.p=h&_pireff296_1906068_296_1905938_1905938.expandNode=doAction&_pireff296_1906068_296_1905938_1905938.nextActionId=1&_pireff296_1906068_296_1905938_1905938.nodePath=.EU_MAIN_TREE.data.icts.isoc.isoc_ci

Figure 34 illustrates these projections across EU Member States[93] as a percentage of GDP under various conditions (SMEs and all organisations excepting micro-enterprises), for malicious incidents and all incidents (including hardware and software failure) controlling for the reported number of incidents in the Eurostat special module on cyber security. The cost data are presented as a minimum (lower end of the scale) per country; for example, in Figure 37 in some countries the total minimum direct costs for all types of security incident (including hardware and software failure) affecting companies is 0.004% of GDP and in other countries the minimum is 0.061% of GDP.

Figure 34 Cost projections for malicious-type attacks as a percentage of GDP, across all companies with less than 10 employees

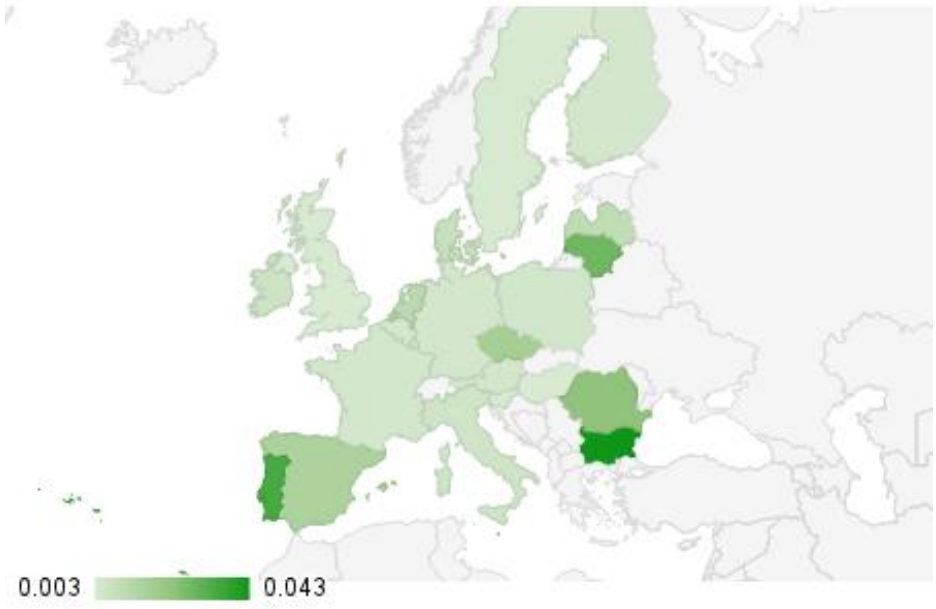
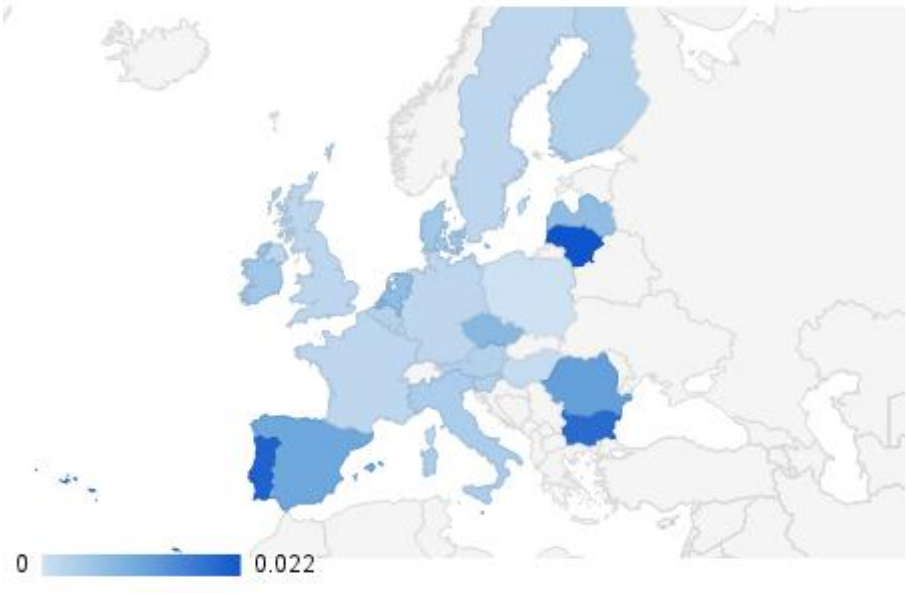


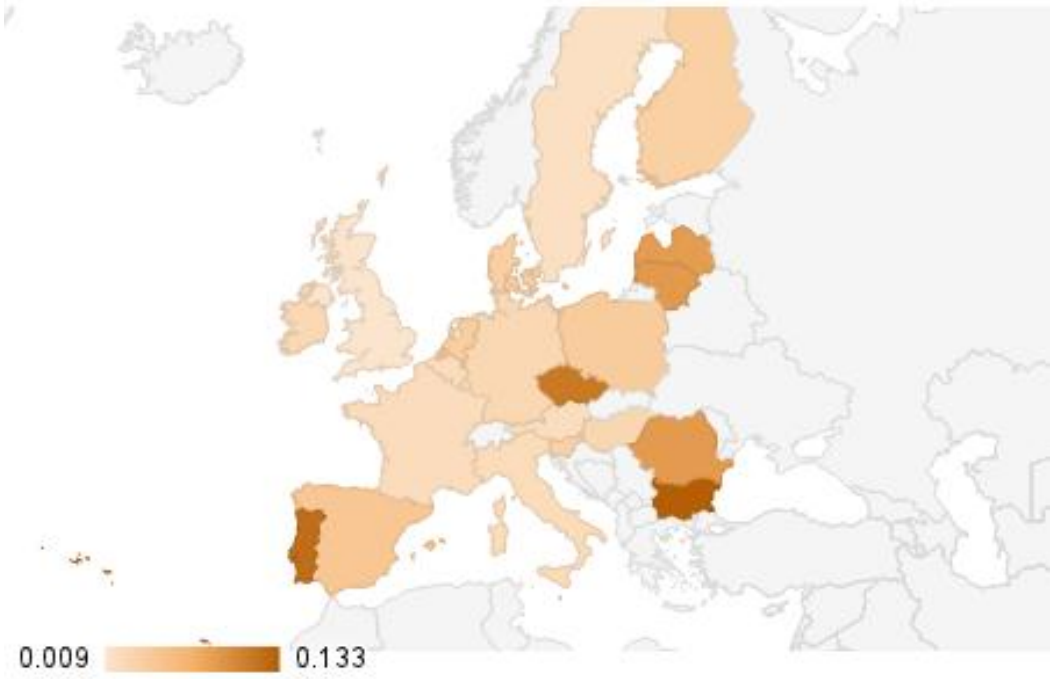
Figure 35 Cost projections for malicious-type attacks for SMEs



[93] Data not available for Greece, Estonia and Slovakia.

Figure 36 provides data for all types of incidents (including hardware and software failure) as a percentage of GDP for all enterprises with more than 10 employees.

Figure 36 Cost projections for all types of ICT-related incidents, all enterprises with less than 10 employees



Finally, Figure 37 gives these data for all incidents affecting SMEs.

Figure 37 Cost projections for all types of ICT-related incidents, SMEs

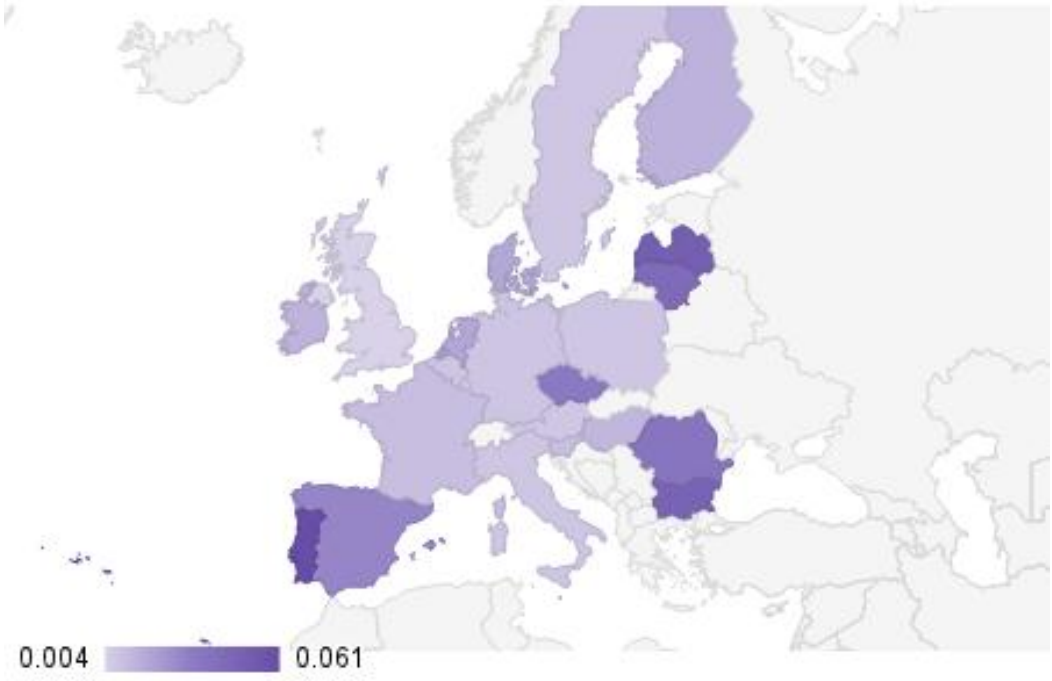


Table 9 shows the minimum direct costs of malicious attacks and incidents, and what these are as a percentage of EU GDP.

Table 9 Minimum direct cost estimates by category of attacks and enterprises (Source: RAND Europe)

Cost	Minimum cost, €	Minimum cost as a % EU GDP
Total estimated cost of malicious attacks to SMEs	562m	0.004
Total estimated cost of all incidents (incl. hardware and software failure) to SMEs	2.3bn	0.017
Total estimated cost of malicious attacks on all enterprises except micro-enterprises	935m	0.007
Total estimated cost of all incidents (incl. hardware and software failure) on all enterprises except micro-enterprises	4.15bn	0.032

By comparison, the cost of automobile accidents, noise and pollution (including indirect costs attributed to automobile phenomena) in Europe has been estimated at 3% of EU GDP.[94]

3.3 The reaction: the state of cyber-security preparedness in EU enterprises

Given this picture, what is the state of cyber-security preparedness? This is again difficult to estimate and according to data from Eurostat (2010) it varies greatly among enterprises across the EU. Figure 38 shows the percentage of enterprises (with over 10 employees, not including the financial sectors) with a formally defined ICT security policy and a plan of regular review.[95]

[94] *The Guardian*, 25 December 2012.
[95] Source: Eurostat (isoc_cisce_ic), 2010.

Figure 38 Percentage of EU companies with more than 10 employees, excluding the financial sector, that reported having a formally defined ICT security policy and a plan of regular review (Source: Eurostat)

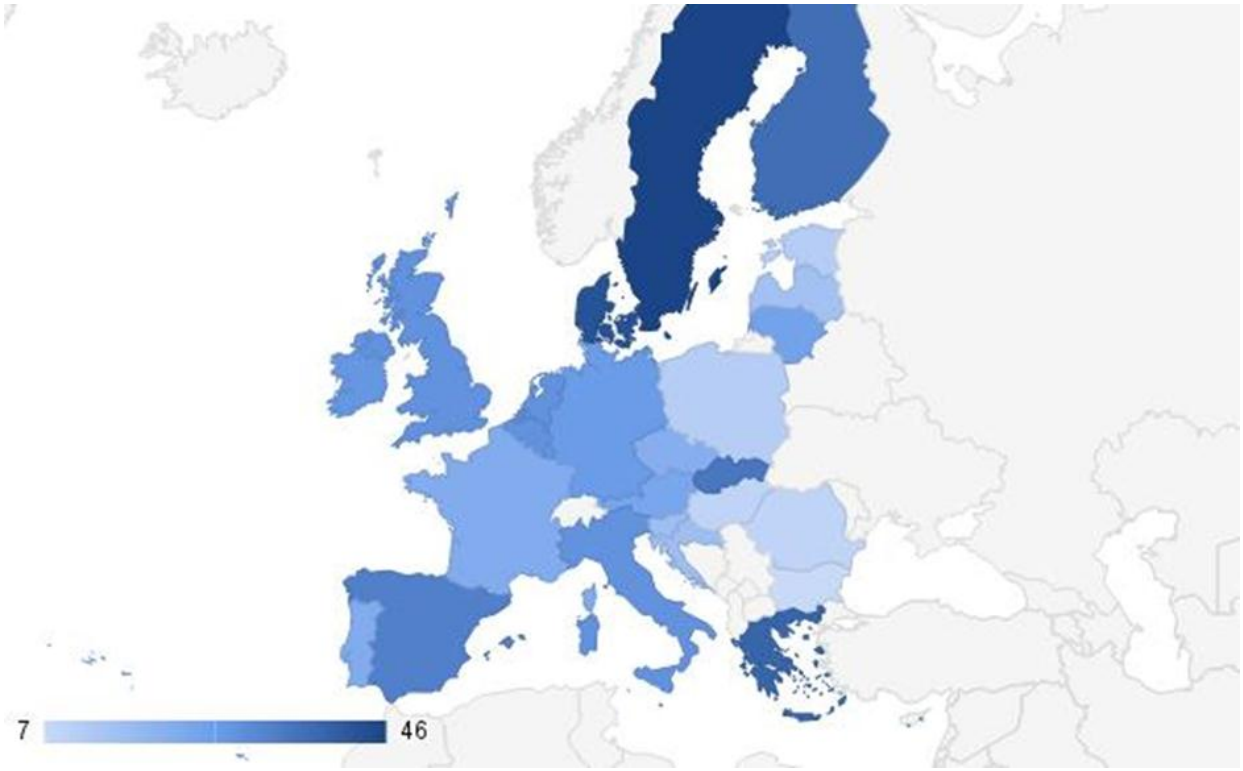
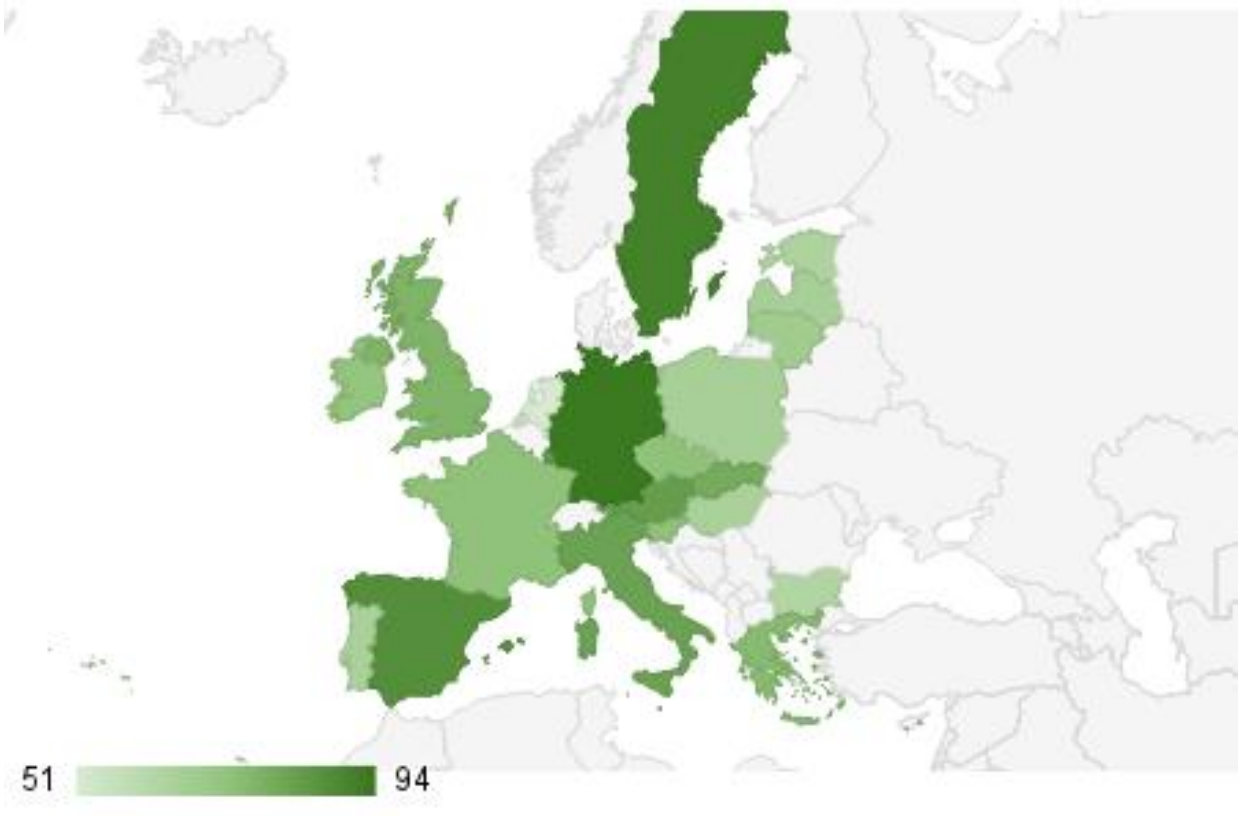


Figure 39 shows that the financial sector appears to be characterised overall by a much higher level of security awareness across Europe than other sectors. However, the data show similar regional discrepancies to that including all other sectors, as the financial sectors of certain EU Member States are much less protected than others.

Figure 39 Percentage of all financial enterprises with more than 10 employees with a defined ICT security policy and plan of regular review (Source: Eurostat and RAND Europe)



3.4 Cyber-security practices in public administrations

Despite the existence of ICT security policy documents in several Member States, we did not come across any EU-wide reliable comparable dataset on the state of play for information security or data breaches at the level of public sector organisations and governments. This lack of data and shared security standards is likely to become more pressing with the increasing importance of e-government instruments across the EU.[96]

3.5 Cyber-security skills and preparedness of European citizens

Finally, we consider the relationship between trends in incidents and breaches identified above and consumer behaviour.

[96] See for instance material shared at the STOA's hearing on Security in e-government systems (European Parliament, 2013).

Figure 40, below, shows responses to a Eurobarometer question on whether consumers have changed their online behaviour as a result of cybersecurity concerns (excluding installing anti-virus software), for example by changing passwords or refraining from using other people's computers.[97]

We use the average of respondents across four categories of behaviour change – certain categories such as installing anti-virus have much higher incidence, so were taken out and are displayed separately in Figure 41.

Figure 40 shows that even in the most security conscious countries (darker colour) only around half of consumers report changing their behaviour as a result of cyber-security concerns.

Figure 40 Effects of cyber-security concerns on individual behaviour, excluding installing anti-virus (Source: Eurostat)[98]

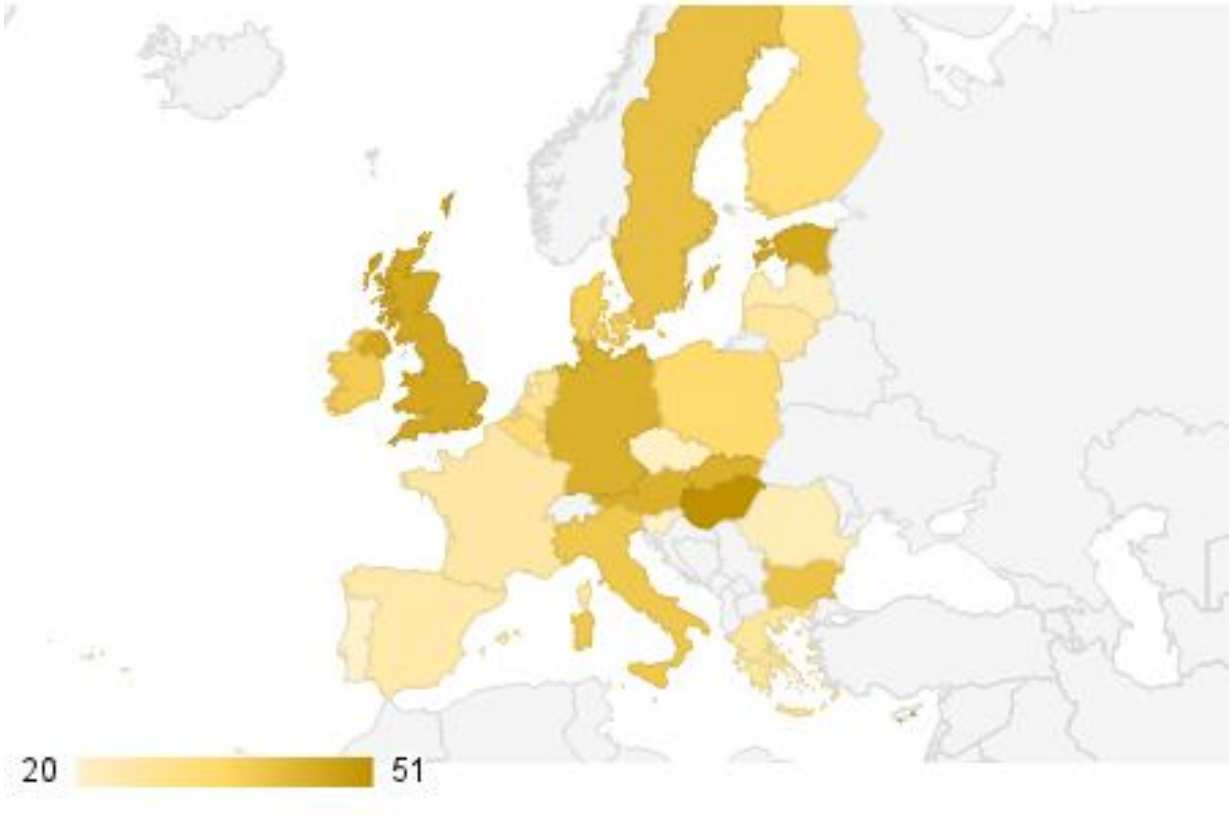
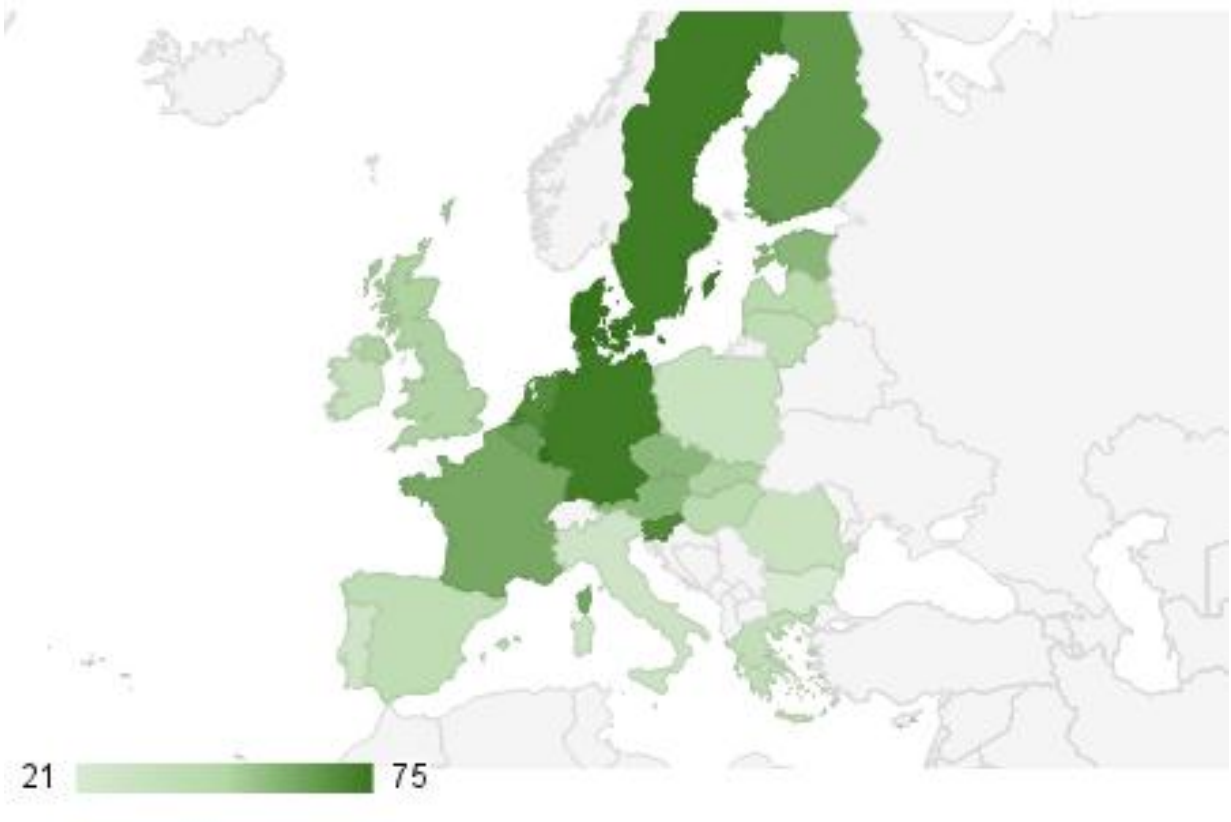


Figure 41 shows that the most common protective action respondents to the survey took was to install anti-virus protection, but the proportion who took this action varied considerably (from 21% to 75%) across EU countries.

[97]Eurobarometer 390, 2012. Eurobarometer 390, 2012. This discussion does not aim to cross-examine Eurobarometer data with baseline cybersecurty attitudes reported elsewhere, rather concentrates on the effect of cybersecurity concerns on changing individual behaviour.

[98] Average of respondents who have reported changing their behaviour in one of the following ways as a result of concerns about cyber security: changed privacy settings; used different passwords; do not open e-mails from people they don't know; less likely to give personal information on websites; only use own computer (ibid).

Figure 41 Effects of cyber-security concerns on individual behaviour, specifically installing anti-virus (Source: Eurostat)



3.6 Conclusions

In the absence of reliable comparable data on the incidence and targets of information security breaches, this chapter has surveyed the available information sources and performed some calculations to gain a preliminary view on the scale of the problem.

Overall, attacks (as captured by data from cyber-security companies) and incidents (as shown by surveys) appear to be on the rise in IT-related attack categories. While a significant proportion (12%) of EU companies reported having suffered incidents involving the failure of hardware or software, this failure does not appear to have led to a similarly high incidence of data breaches following hardware or software failure. The data show that the proportion of data breaches that occurred for environmental reasons or following physical disruption is much lower than breaches due to human error or malicious attacks.

According to Eurostat statistics, the level of preparedness of European companies (using the existence of an ICT security plan as proxy) in sectors excluding the financial sector is much lower than in the financial sector, where up to 90% of companies have such a plan. However, in all sectors there are large discrepancies between countries between the levels of preparedness.[99]

Where we have information of the incidence of information security breaches (e.g. in the UK), we see that larger companies tend to report larger numbers of breaches. This

[99] Eurostat Special module 2010: Internet Security (isoc_ci_sc) Enterprises – ICT security policy, incidents and measures taken (isoc_ci_sce).

phenomenon could potentially be a result of these companies benefitting from better detection and reporting capabilities, e.g. having more IT security staff or experiencing a larger number of attacks to begin with because they are bigger targets. Individual attacks could have important effects on small companies, in particular in cases where they disrupt business because smaller firms might be less resilient than larger ones.

4 HOW IS EUROPE CURRENTLY MANAGING THESE PROBLEMS?

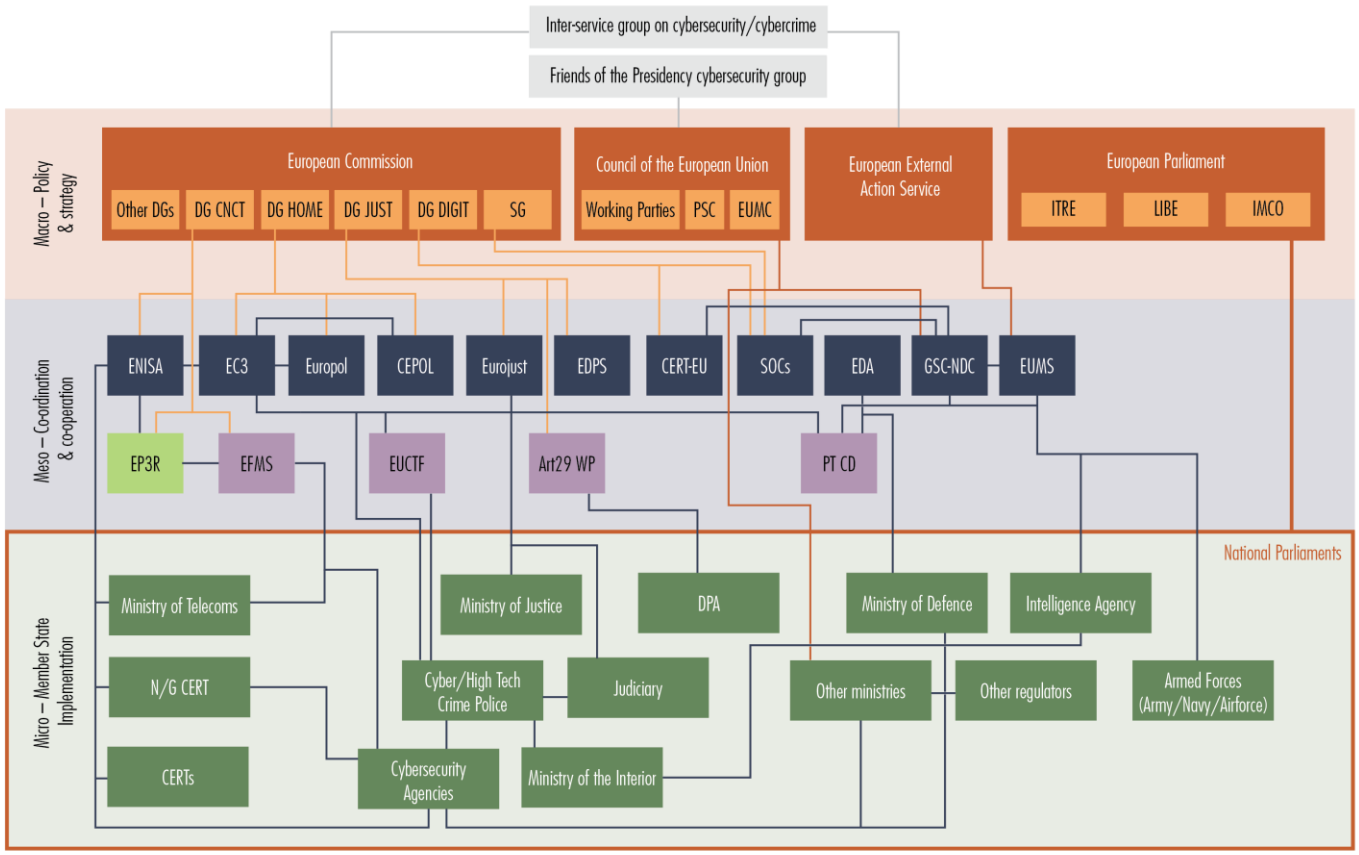
KEY FINDINGS

- There is no single coherent understanding of how European efforts in this area are organised and meant to work together across the different aspects of an incident cycle (prevent, detect, react and recover).
- ENISA's efforts to engage CERTs and build capacity are maturing and the Agency has been at the forefront of implementation of Article 13a incident notification in the communications sector.
- Many EU institutions are in an early stage of development such as the European Cybercrime Centre (EC3) and CERT-EU.
- The EP3R is the main mechanism for engaging the private sector but its future is uncertain with the NIS Platform being launched.
- There are complex mandates and roles of different organisations that can be difficult for outsiders to understand.
- Although certain sectors of the ICT industry are involved, end-users of ICT from finance, healthcare, transport and energy are notably absent in many initiatives.
- There is no mature mechanism to involve private sector end-users of ICT as information society service enablers, as identified in the proposal for a NIS Directive.
- There is a very apparent danger of overlapping regulation in some sectors.

The existing framework under which European institutions and agencies, different organisations in the public and private sector within Europe and globally, interact over cyber-security incidents is undoubtedly highly complex, as noted in a hearing by the UK House of Lords on the Critical Information Infrastructure Protection (CIIP) Directive in 2009.[100] This is partly because of the complexity of the domain, as joint ownership of the risks for governments, business and consumers requires concerted action by the public and private sector in a multidisciplinary approach. However, the historical institutional mandates of those assigned accountability and responsibility for response at the European level also play a role. In this chapter we provide an overview of how different institutions tackle (in a broad sense) security incidents and breaches. Figure 42 illustrates the links between these institutions. Note that the figure does not show what kind of links exist, nor their effectiveness, but merely that they exist.

[100] House of Lords 5th report of session, 2009-10.

Figure 42 Who talks to who about cyber security in Europe (Source: RAND Europe)

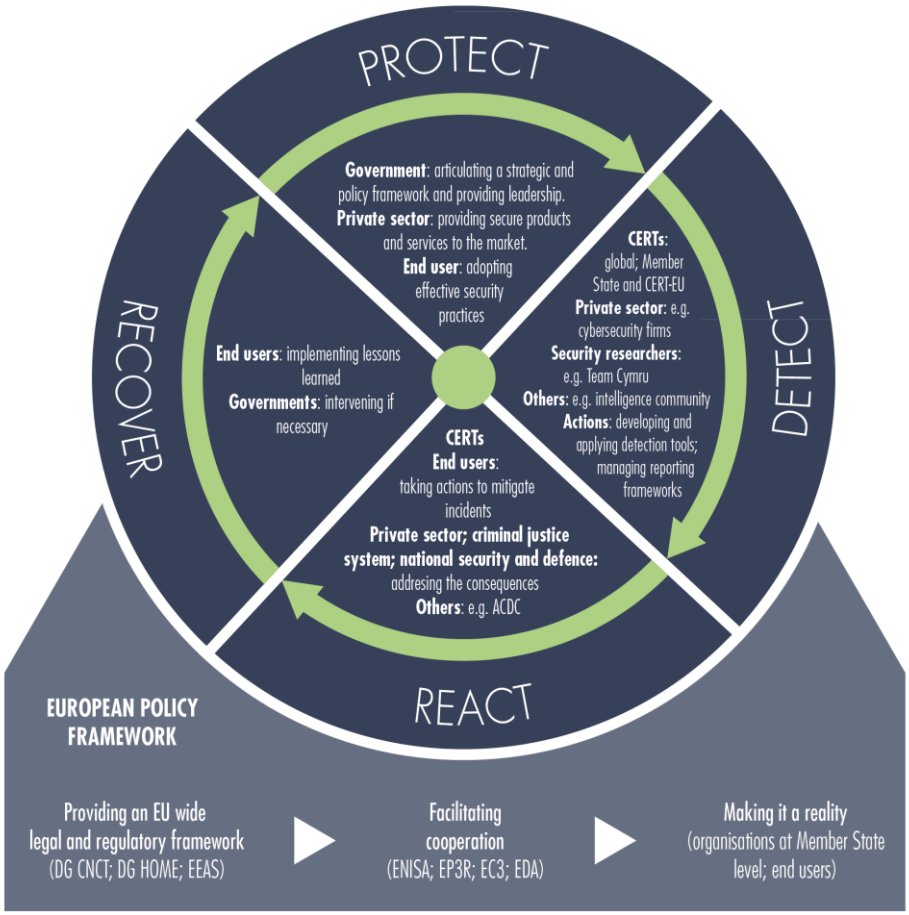


KEY

Art29 WP	Article 29 Working Party
CEPOL	European Police Training Academy
CERT-EU	Computer Emergency Response Team for the European Institutions
DG CNCT	Directorate General Communications, Networks, Content and Technology
DG HOME	Directorate General Home Affairs
DG JUST	Directorate General Justice, Freedom and Fundamental Rights
EC3	European Cybercrime Centre
EDA	European Defence Agency
EDP	European Data Protection Supervisor
EFMS	European Forum for Member States
ENISA	European Network and Information Security Agency
EP3R	European Public Private Partnership for Resilience
EUCTF	European Union Cybercrime Task Force
EUMC	European Union Military Committee
EUMS	European Union Military Staff
GSC	General Secretariat of the European Council of Ministers
IMCO	Consumer Affairs Committee of the European Parliament
INTCEN	Intelligence Centre
ITRE	Industry, Research and Environment Committee of the European Parliament
LIBE	Civil Liberties and Justice Committee of the European Parliament
PSC	Political and Security Committee
PT CD	Project Team Cyber Defence
SG	Secretariat General (COM)
SOC	Security Operations Centre

Figure 43 shows the broad roles different types of organisation play when there is a cyber-security incident.

Figure 43 The relationship between incident management lifecycle and different stakeholders (Source: RAND Europe)



4.1 Overview of the interaction between European-level institutions

Figure 42 gives an overview of the co-operation and interaction between EU-level institutions involved in cyber security. Interaction is incredibly complex as there is a panoply of organisations with links at the macro, meso and micro level.

A number of institutions create or support the implementation of public policy on cyber security. ENISA is perhaps the best-known example; it works to improve the state of network and information security across Europe. The recently established European Cybercrime Centre (EC3) at Europol acts as the focal point of European efforts to co-ordinate an effective response to all forms of cyber crime (but focuses on those with an economic element). Cepol (the European senior police training network) and Eurojust (the European network of public prosecutors) support the work of EC3 and Europol. The CERT-EU has been set up recently as an incident response team for European institutions (rather than a peer to the US-CERT, the US national CERT).

Finally, partnerships such as the European Public–Private Partnership for Resilience (EP3R) and the European Public–Private Partnership for Trust in Digital Life aim to create mechanisms to foster co-operation between the public and private sectors to address the market failure that seemingly characterises cyber security.[101]

4.1.1 The European Network and Information Security Agency (ENISA)

ENISA was established as a decentralised agency in 2004, initially for a period of five years.[102] This was subsequently temporarily extended in 2008 to 2012 and then again in 2011 for a further two years until September 2013,[103] ostensibly to permit enough time for debate and agreement on its revised mandate. Its new regulation came into force on 19 June 2013.[104]

In its original mandate of 2004, ENISA was broadly tasked to contribute to development of a culture of NIS for the benefit of citizens, consumers, enterprises and public sector organisations throughout the EU. This included advising and assisting the Commission, promoting risk assessment and risk management methods, and developing awareness and co-operation between different actors.[105]

In order to accomplish these objectives it carried out a range of activities. An informal evaluation carried out as part of a 2011 ITRE study listed some of them:

- demonstrating and promoting good practice in a variety of areas, providing advice to the Member States and the European Commission on NIS topics and support for CERTs
- liaising with the EFMS and EP3R over CIIP
- conducting exercises at the European level and with the US in 2011
- assisting with breach notification data as envisaged by the 2011 FWD
- participating in the expert group for the CERT-EU pre-configuration team
- interacting with data protection stakeholders
- interacting with other international stakeholders.

The 2013 Regulation[106] which was agreed by the European Parliament in April 2013 and signed by the European Parliament and the Council on 21 May 2013 substantially modifies the mandate of the Agency, and orientates its focus towards public administration, CERTs and the Commission in line with the NIS Directive and EU Cybersecurity Strategy. This demonstrates positive recognition of the Agency's efforts in supporting the work of CERTs.[107] The revised mandate is for seven years and thus will expire in 2020. The operational office of the Agency will sit in Athens although its formal office will remain in Crete. No branch office in Brussels is foreseen.

Although many parts of ENISA's mandate are consistent with the tasks and activities described above, which have been ongoing since 2004, one crucial element of the mandate (establishing co-operation with the private sector) appears to have been given low priority.

[101] For an overview see Robinson et al., 2012.
[102] Regulation 460/2004.
[103] Regulation 580/2011.
[104] ENISA, 2013b.
[105] ENISA Regulation 460/2004, Article 27.
[106] Regulation 526/2013.
[107] With the caveat that many CERTs are reluctant to participate in ENISA activities because of there are many competing requests from the Agency; and the Agency treats CERTs with 'kid gloves' in some respects – placing their refrain concerning flexibility above many other aspects that might improve co-operation.

A summary analysis of articles 19–36 of Regulation 536/2004 shows that the Agency will be more concerned with co-operation between Member States and the Commission and other bodies and agencies (e.g. CERT-EU) than with co-operation and outreach with the private sector. For example, according to Article 23, 'the Agency should facilitate co-operation among the Member States and between the Commission and other Union institutions, bodies, offices and agencies and the Member States'.

Similarly, Article 24 states that in co-operation with Member States and if appropriate statistical bodies and others the Agency should collect relevant information in the network and information security field. It is also empowered to assist EU institutions in efforts to collect, analyse and disseminate network and information security data. Analysis of the risks to the security and resilience of electronic communications infrastructure and services should take place on the basis of information provided by Member States and the Agency's insight into the Union institutions. ENISA should then maintain awareness of the latest state of NIS and related trends for the benefit of Union institutions bodies, offices and agencies of the Member States.

Article 33 of the 2013 Regulation emphasises that efficient NIS and information security policies should be based on well-developed risk assessment methods in the public and private sector. The Agency therefore should support co-operation between stakeholders at Union level, facilitating their efforts to establish European and international standards of risk management and measurable security of electronic products system networks and services.

Article 35 of the 2013 Regulation states broadly that the Agency is to encourage Member States and service providers to raise their general security standards.

In effect, the relationship between the Agency and the private sector is not emphasised. For example, guidance and provision of good practice advice on risk management (a core plank of the NIS Directive) only refers to stakeholders at Union level. But as the NIS Directive places so much emphasis on this as a complement to incident reporting by the private sector, how is the private sector expected to improve its risk assessment and risk management processes? The 2011 report by ITRE remarked on a study undertaken by Deloitte, commissioned by ENISA, which showed that private sector take up of ENISA deliverables was poor.

Whether this has changed is difficult to say. However, anecdotal evidence suggests that the ENISA document on cloud computing security[108] was well received by industry, especially the Cloud Security Alliance (CSA), and the author went on to work for the CSA.

In the deliberations around the role and mandate of ENISA there has been a longstanding debate about whether it should have operational capability. Since the early 2000s European Member States have strongly rejected any idea of a supranational NIS or cyber-security organisation such as a pan-European CERT. Discussion and ideas were originally floated about ENISA being able to take incident reports from Member States to act as a EU CERT but this suggestion was rejected because it assumed the EU to have too much power.[109] Therefore, ENISA evolved into a policy advice organisation, aiming to build capacity in the Member States through the analysis and dissemination of best practice.

[108] ENISA, 2009b
[109] ITRE, 2011.

There are a number of specific elements of ENISA's work relevant to the topic of incidents and breaches:

- ENISA has a role in facilitating the reporting of security breaches under Article 13a of Directive 2009/140/EC (the so called 'Telecoms Package' revised in 2009).[110] This takes place via the Article 13a Working Group of competent bodies. ENISA's work in this regard has focused on devising:
  - technical reporting guidelines that significantly affect the continuity of electronic communications
  - minimum standards for security that should guarantee the security and integrity of telecommunications networks and services across the EU.
- ENISA has supported capacity building in Member States by:
  - encouraging well-functioning CERTs, providing guidance and help in the form of practical tools, training and exercises; these range from initiatives regarding baseline capabilities for CERTs to workshops on co-operation between law enforcement and CERTs; ENISA has tended to focus its efforts on national governmental CERTs, but given the diversity of such CERTs (many being de-facto in status) this has proved vague
  - working on national cyber-security strategies with the publication of a guide to setting up such strategies in 2012[111]
  - working on crisis management and co-operation by facilitating a number of exercises such as Cyber Europe 2010, which aim to test Member State capability for rapid crisis response.

The EU Internal Security Strategy 2010 stated:

> *Firstly, every Member State, and the EU institutions themselves should have, by 2012, a well-functioning CERT … [A]ll CERTs and law enforcement authorities co-operate in prevention and response. Secondly, Member States should network together their national/governmental CERTs by 2012 … developing, with the support of the Commission and ENISA, a European Information Sharing and Alert System (EISAS) to the wider public by 2013 … Thirdly, Member States together with ENISA should develop national contingency plans and undertake regular national and European exercises.*[112]

A 2011 report evaluating the work of the Agency for the ITRE Committee[113] argued that a continuation of the Agency under the terms of its original mandate from 2004 would be inappropriate because of the new challenges and missions. This report pointed out that although progress under a new management team had been good since an evaluation in 2007, the small size of the agency and its remote location were barriers to its effectiveness. The operation of the breach notification system under Article 13a was cited in the 2009 report as an example of where its responsibilities grow, implying a 'somewhat operational data collection role' in processing incident reports under Article 13a and 13b of the framework Directive.[114] The report noted that although there was opposition to the agency having an operational role, in many respects, e.g. with regard to the management of breach notifications under Article

[110] European Parliament & the Council, 2009.
[111] ENISA, 2012b.
[112] European Council, 2010.
[113] European Parliament, Directorate General for Internal Policies, Policy Department A - Economic and Scientific Policy, 'The Role of ENISA in Contributing to a Coherent and Enhanced Structure of Network and Information Security in the EU and Internationally', 2011: http://www.europarl.europa.eu/committees/en/itre/studiesdownload.html?languageDocument=EN&file=42251
[114] European Parliament and the Council, 2002a.

13a, this is precisely what it now possesses. The report suggested that it would be appropriate for ENISA to assume 24x7 responsibilities that have no overlap with Member States.

ENISA was seen as a crucial player in the 2006 Strategy on the Secure Information Society: Dialogue Partnership and Empowerment.

The 2011 CIIP Communication (taking stock),[115] which reviewed progress since the 2009 action plan, described the future for the EFMS and EP3R noting that over the long term and in the context of the new ENISA Mandate, ensuring the functioning of the EP3R was foreseen as a key activity for ENISA. However, as of 2013 with the future over the EP3R uncertain, especially with regards to the NIS platform (where the centre of gravity appears again to be with the COM), ENISA's role appears to be unclear.

In its analysis of the 2010 proposal for a new ENISA Regulation by the Commission, the 2011 ITRE study found that in general the proposed regulation appeared to imply that ENISA would have less direct responsibility in cybersecurity than under the previous legislation, but instead focus its efforts on supporting the Commission and Member States (albeit with a broadening of the scope by including cyber crime and considering data protection).[116]

In January 2013 ENISA opened a forward operating office in Athens in accordance with its expanded mandate and the general strategic direction of the proposal for a NIS Directive. However, the recommendation that a branch office should be opened in Brussels, made in both the 2007 IDC evaluation and the 2011 'informal evaluation', has still not been adopted. ENISA's staff numbers are expected to increase to around 100 people to cope with reporting of security breaches in the other sectors covered by the NIS Directive.
According to ENISA's Annual Report,[117] in 2012 ENISA ran three Article 13a workshops in Lisbon, Luxembourg and Mainz, developed a framework for collecting annual national reports of security breaches (architecture and implementation of cyber incident reporting and analysis system – CIRAS) and provided a second version of technical guidelines on incident reporting. Furthermore, it was active in t supporting the CERT and other activities, and provided an updated baseline of national and governmental CERTs; a status report on the deployment of a current set of baseline capabilities of national governmental CERTs provided new exercise material and an update to the ENISA inventory of CERTs in Europe. Finally, ENISA has been keen to offer guidance and support to Member States as they develop their cyber-security strategies.[118] In 2012 ENISA formally reported that it handled 14 official requests (from either Member States or the Commission) and 10 inquires.

Despite this reported progress, there are a number of aspects that merit further investigation. First, although the Agency has been keen to stress the large number of national and government CERTs it has helped establish (and indeed the minimum baseline capabilities), there are a few countries that still do not have a nominated national level CERT, Italy being a prime example.

Second, noting the diversity in approaches to operating their CERTs, the Agency has tried to play a role (somewhat unsuccessfully) in helping Member States operate a common baseline, through an approach based on guidance rather than proscription.

[115] European Commission, 2011a.
[116] Marcus et al., 2011.
[117] ENISA, 2012c, under the heading 'Improving Pan European CIIP and Resilience' (WP4).
[118] ENISA, 2012d.

Certain efforts have been made, for example exchanging practices on CERT co-operation with other stakeholders and training. Despite this, a number of Member States have still not taken up recommendations made in ENISA reports on various matters, for example to establish a firm legal footing to allow them to process personal data in the interest of enhancing the efficiency of incident handling.

4.1.2 The European Forum for Member States (EFMS)

The EFMS may be considered a counterpart to the EP3R (discussed below). Set up following the 2009 CIIP Directive, the EFMS acts as a platform for Member State representatives to discuss aspects of European NIS policy as a peer group. Membership of the EFMS is limited to government officials of Member States. It is chaired by members of ENISA and DG CNECT. EFMS deals with policy and is not intended to cover operational or technical matters. The House of Lords report on the CIIP action plan noted that the 'EFMS fulfils a real need for policy-makers to exchange experience'.[119]

Topics discussed include:

- criteria to identify ICT infrastructures
- priorities, principles and guidance for internet resilience and stability
- the long-term strategy on developing pan-European exercises
- international co-operation (especially in regard to the EU–US working group on cyber crime and cyber security
- the European cyber-security strategy.

The EFMS has undertaken 10 meetings since its inception and is now registered as an expert group of the Commission. Anecdotal evidence from interviewees suggests that the EFMS was instrumental in preparing the Article 13a breach notification guidance and that it fulfils an important role in devolving regulatory action down to sectoral regulators (e.g. telecommunications regulators like Onafhankelijke Post en Telecommunicatie Autoriteit (OTPA) in the Netherlands, Autorité de Régulation des Télécommunications (ART) in France, and the Office of Communications – Ofcom – in the UK).

As has been indicated in the impact assessment accompanying COM (2012) 0027, the organisation in charge as the de-facto lead is markedly different across Member States Given open and flexible entry conditions of the EFMS there is a risk that attendance and success is hampered by infighting between Member States over who has primacy with regard to attendance and being the voice of the Member State. These challenges also affect other expert groups (such as the European Cybercrime Task Force) where responsibility for issues being discussed is unclear at the Member State level and may be spread across several departments.

4.1.3 The European Public–Private Partnership for Resilience (EP3R)

The EP3R was established in 2009 as a way to bring public and private sectors together. It is intended to be a mechanism to drive public–private partnership to foster NIS. Its provenance comes from the CIIP Directive adopted in 2009.[120]

[119] HoL European Committee 5th report of session, 2009-10.
[120] European Parliament and the Council, 2009.

The objectives of EP3R include: information sharing and stocktaking of good policy and industrial practices to foster understanding, discussing public policy priorities, improving policy consistency and co-ordination across Europe, identifying and promoting good baseline practices for security and resilience, and issuing recommendations.

In 2010, work was undertaken on three areas:[121]

- the key assets, resources and functions for continuous and secure electronic communications across countries
- baseline requirements for security and resilience
- co-operation and co-ordination needs and mechanisms to prepare and respond to large scale disruptions.

These themes were then broken down into four tasks in line with the mission of EP3R:

- WG1 – definition of European critical infrastructures
- WG2 – security baselines for existing equipment
- WG3 – assessment of national botnet initiatives
- WG4 – exercises – focusing on mutual aid agreements.

Four workshops were held in 2011 to progress these tasks. In 2012, partly as a result of slow progress on these topics and an appaarent attempt to rejuvenate the EP3R, a number of work packages were devised under the following eight headings:

- terminology definitions
- trusted information sharing mechanisms
- mutual aid strategies
- categorising assets
- incident management
- tracking down botnet offenders
- cyber attacks mitigation and response
- wide-scale and systematic malware disinfection.

Although EP3R aims to include public and private stakeholders to jointly devise its objectives, principles and structure it appears to have suffered from two major challenges. First, institutional struggles over which EU organisation should be the primary facilitator appear to have confused and hampered progress. Initially, the European Commission took the role of facilitation of the EP3R, seemingly using it rather conservatively as a mechanism to further distribute policy messages on cyber security and CIIP. Since late 2012, ENISA has assumed the lead role in developing the EP3R.[122]

Second, the EP3R has been beset by questions about what incentives to offer to encourage the private sector to participate.[123] No funding was made available by the EU to cover travel costs for participation (except for moderators in the last two years) and there was a failure to understand the possible incentives that might encourage the private sector to join.

[121] ENISA, 2012b.

[122] The 2010 non-paper establishing EP3R noted: 'In the starting phase, the European Commission will lead and facilitate EP3R – including the secretariat function. It is proposed that ENISA assumes increasingly more responsibility regarding EP3R, and after a reinforcement of its mandate the running of EP3R could be one of the key activities of a modernised European NIS agency.'

[123] Irion, 2013.

Initially, when the European Commission ran the EP3R, many private sector organisations regarded it as an opportunity to influence or lobby the EU, but participants became disillusioned with progress when outcomes were not clarified. EP3R also suffered from a lack of involvement of end-users of ICT. Although major ICT firms (and a few end-users) participated in meetings, there were not enough representatives from infrastructure companies to ensure a robust enough debate on how EU CIIP efforts might have positive economic benefits.

The latest attempt to revitalise EP3R through its task forces and experts may yet bear fruit, although experience suggests that a key driver of the success of such public–private information sharing activities is consistent management of the platform.

In late 2012 the NIS Public–Private Platform was announced. An open day was held in Brussels on 17 June 2013, which attracted over 100 stakeholders including end-users of ICT such as energy companies.[124]

4.1.4 The CERT-EU

The CERT-EU is the Computer Emergency Response Team for EU institutions. Around 60 institutions form the constituency of the CERT-EU. As has been described, the need for an EU-wide CERT that would have a mandate to detect and react to cyber-security incidents across Europe was widely disputed and rejected by the Member States. This initiative, known as EuroCERT,[125] was rejected 'in favour of co-operation and collaboration'. As a result, the mandate of ENISA was specifically crafted to exclude any operational role as this would be a step too far.

In June 2011 the decision was taken to establish a CERT for the EU institutions.[126] The first year was taken up with activities from the CERT-EU pre-configuration team, which was intended to work in close co-operation with IT security teams in institutions, agencies and bodies and liaise with the community of CERTs in the Member States and elsewhere, exchanging information on threats and how to handle them. Evidence from presentations given by the CERT-EU pre-configuration team in 2012 illustrated that it performed a role as a kind of informal security consultancy because it did not have direct access to networks of its constituency. However, with the CERT-EU pre-configuration team turning into a formal CERT, this situation is evolving.

The CERT-EU joins a number of existing security operations centres (SOCs) run by the Secretariat General (SG) and the Directorate-General for Informatics of the European Commission, covering the security management of networks such as sTESTA and EU-wide information systems such as the 2nd Generation Schengen Information System (SISII), Visa Information System (VIS); EURODAC via its management authority based in Estonia.[127] The role of the CERT-EU is to provide computer emergency response team services to over 60 different EU institutions.

---

[124] See: EC Digital Agenda, NIS PPP Call for expression of interest: http://ec.europa.eu/digital-agenda/en/news/nis-public-private-platform-%E2%80%93-call-expression-interest

[125] See: ENISA wbsite, CERT Co-operation: http://www.enisa.europa.eu/activities/cert/background/coop/past-present/regional-coop/europe

[126] European Commission, 2011b.

[127] See: EC DG Justice & Home Affairs website: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/agency/; see also DG Justice & Home Affairs, 2012. STesta is the European Community's own private network, isolated from the Internet and allows officials from different Member States for secure communication of confidential documents at a trans-European level.

This was seen as a much needed response following significant cyber attacks on the EU's Carbon Trading System (CTS)[128] and nation-state sponsored incidents in 2011 and 2012,[129] and most recently at the 2012 Internet Governance Forum in Azerbaijan.[130] A CERT-EU pre-configuration team was established in 2011 and during this phase the CERT did not have direct real-time access to Member State networks. The pre-configuration team focused on the collection and dissemination of indicators of compromise related to an incident.[131] During this phase, its role therefore might be characterised as providing a form of cyber-security consultancy and advice. It was understood that members of the pre-configuration team were often called on by an institution after an incident to discuss the implications and remediation. The CERT-EU pre-configuration team often asked the affected institution questions such as 'what information was affected?', 'what was the value of this information?'

Crucially, from the perspective of co-ordination, the CERT-EU pre-configuration team was not permitted to handle protectively marked information so CERT services (such as detection and incident response) covering EU-CONFIDENTIAL and information exchanged on the Operational Wide Area Network used for EU-led common security and defence policy operations are actually undertaken by the Network Defence Centre of the General Secretariat of the Council.

4.1.5 The European Cybercrime Centre (EC3)

The EC3 may be thought of as a core plank of a broader response where a security incident is deemed to be criminal in nature (of a malicious nature breaching provisions in Member State criminal law as approximated by Council Decision 2005/222 JHA).

Following a feasibility study conducted in 2011,[132] the EC3 was established within Europol in The Hague and launched formally in January 2013 at a large opening ceremony attended by around 400 people and the world's press.[133] The nexus of the EC3 can be found in Europol's pre-existing high tech crime unit, located within its Operations Directorate ('O'), which had existed since 2009.

The background to the EC3 can be found in the European Council Conclusions of 2008 and 2010, when it was decided that a European cyber-crime centre was necessary to co-ordinate responses to tackling cyber crime across Europe. The EC3's mission[134] is to act as 'a fusion centre [for expertise]; operational investigative and forensic support'; helping to mobilise all relevant resources in EU Member States to 'mitigate and reduce the threat from cyber-criminals'.

The EC3 is also intended to facilitate R&D and build capacity among law enforcement judges and prosecutors, producing threat assessments, trend analysis forecasts and early warnings. When fully operational EC3 will run a cyber-crime help desk for Member State law enforcement agencies, gather and process cyber-crime-related data and offer

[128] See e.g. *The Financial Times*, 2011.
[129] See. among others, the hacking of IMF allegedly by a nation state-sponsored group, as well as several high-profile cases attributed to organisations sponsored by the People's Republic of China (CSIS 2013)
[130] See e.g. *European Voice*, 15 November 2012.
[131] Indicators of compromise may be considered to be technical details concerning the incident but crucially do not attempt to make any consideration regarding the motivation and characterisation of a possible adversary ('attribution').
[132] Robinson et al., 2012.
[133] European Commission, 2013b.
[134] Ibid.

operational support to EU countries against a range of cyber-crime commodities. Finally it is envisaged that it will deliver high level technical, analytical and forensic expertise in EU joint investigations.

The EC3 will have 40 personnel based in The Hague when it becomes fully operational in 2015. It has begun with five personnel in the office of the director and personnel responsible for outreach and strategic partnership. Its governance is supported by its Programme Board aimed to drive a coherent approach to delivering the goals of the EC3 through inclusion of stakeholders such as the EU Cybersecurity Task Force, the Collège Européen de Police (CEPOL), the European Cybercrime Training and Education Group (ECTEG) and ENISA, which each have a role to play in helping EC3 achieve its goals.

The activities of the EC3 include:

- acting as a fusion centre for operational and investigative support to tackle cyber crimes, including analytical and forensic expertise
- facilitating cross-border joint investigations
- providing a platform for co-ordinated intelligence sharing to tackle cyber crime
- supporting capacity building through training and education for personnel across the criminal justice system (law enforcement, judiciary and public prosecutors)
- producing threat assessments, forecasts and early warnings.

In the interests of furthering the work of the EC3, Europol signs strategic and co-operation agreements with a range of other organisations within Europe and globally across the public and private sectors. Operational co-operation agreements permit the exchange of nominal data (name; date of birth; address etc.) about suspects and those under intelligence scrutiny. Strategic co-operation agreements are more general and facilitate information sharing. At present it is understood that several such agreements have been concluded with ENISA, private industry (especially companies involved in cyber security) and organisations from third countries (e.g. the US Secret Service and the US Department for Customs and Border Protection).

The crime commodities that the EC3 focuses on are primarily fraud related (economic fraud or credit card fraud) or child pornography related (the distribution or circulation of child pornography, defined as 'illegal online activities carried out by organised crime groups'). Although crimes affecting critical infrastructure and information systems in the EU are also covered, in public statements so far the focus of the EC3 has been on fraud and economic crimes.

Thus, the extent to which the EC3 focuses on incidents affecting information systems directly (rather than exploiting the value carried over them) is unclear. For example, many of the services offered by the EC3 focus on fraudulent use of ICTs (banknote examination, for example, to detect technology used for counterfeiting money) rather than investigation of high tech forms of cyber-crime incidents. Hence, its relation to the scope of the proposal for a NIS Directive is confusing and unclear.

Data fusion is also supposed to interact with CERTs but the means by which this occurs is not currently specified, especially as the EU's relationship with non-governmental CERTs is primarily managed by ENISA.[135]

[135] Other research suggests that CERTs do not tend to speak to law enforcement agencies in other countries directly but go via national agenices.

In spring 2013 the EC3 Programme Board announced a request to participate in three advisory boards (roughly understood as working groups). Each advisory board is expected to run for a term of two years and be composed of 12 experts. The role of the advisory boards is to bring knowledge and expertise, information and advice to the EC3 Programme Board in three main areas:

- *financial services*[136] – understanding the needs and priorities of retail and financial services in the context of the fight against cyber crime; as one of its activities for 2013–2014 this advisory board will: 'advise the Programme Board on the development and implementation of a mechanism for anonymous incident reporting and preventative notification within the sector'
- *industry cross-sector developments*[137] – understanding the technological evolution that may give rise to opportunities for criminal exploitation; in 2013 and 2014, this advisory board will work to set up a mechanism to feed cross-sector developments related to cyber crime to the EC3 and provide an impact assessment of developments in technology as they relate to the work of the EC3, cyber security and cyber crime in general
- *internet security*[138] – bringing knowledge and expertise and sharing information on developments in internet security and advising on co-operation with CERTs and partners in the ICT security and anti-virus industry and elsewhere; in particular, in 2013–2014 the advisory board will elaborate on and propose a concrete model to organise co-ordination between law enforcement agencies, CERTs, ICT security and the anti-virus industry and other relevant partners that will enforce and strengthen of cyber security and develop a proposal on how to strike the right balance between preventative and investigative interests.

A key component of the EC3 is its relationship with the EU Cybersecurity Task Force, a network of law enforcement peers (heads or deputies of high tech crime or cyber-crime police units) from the EU Member States. It is nominally chaired by a rotating head of a cyber-crime unit. It may therefore be considered as the voice of the law enforcement community in Europe in this area.

4.2 Other organisations

A number of other organisations are worthy of note, although they play a somewhat secondary role as they either support capability or deal with the ramifications of incidents.

4.2.1 The Collège Européen de Police (CEPOL)[139]

The European Police College (CEPOL) is the EU's police training college for senior and mid-level law enforcement personnel. It is currently based in the UK in Bramshill and employs 42 personnel. CEPOL is a decentralised agency that was established in 2005.[140] CEPOL's mission is to support a network of senior police officers across Europe and encourage cross-border co-operation to tackle different types of crime, public security and law and order by organising training activities and research findings.

It is understood to have run cyber-crime training course and provided e-learning facilities for law enforcement officers. In 2010/11 its budget was around €8m.

[136] Europol, 2013a.
[137] Europol, 2013b.
[138] Europol, 2013c.
[139] Robinson et al., 2012.
[140] European Council, 2005.

Activities relating to cyber crime include an e-learning module aimed at high ranking police officers, exchange for cyber experts and webinars. The e-learning module in particular comprises aspects of:

- co-operation (links with the EU, national and international police forces and the private sector)
- institution building
- prevention
- legal frameworks
- cases – include case management
- first response
- investigation
- digital forensics
- network forensics
- evidence and admissibility.

4.2.2 The European Cybercrime Training and Education Group (ECTEG)

The ECTEG is a bottom up initiative from the European Cybercrime Task Force. ECTEG delivers a training and educational syllabus offering courses relevant for cyber crime and high tech crime police officers including forensics, network monitoring and so on.[141]

4.2.3 The European Data Protection Supervisor (EDPS)

The EDPS issues guidance and advice to data protection authorities (DPAs) on matters of enforcement and implementation of the EU legal framework on privacy and data protection with regard to the use of personal data by the EU institutions. The EDPS has issued its own opinion on the proposal for a NIS Directive, noting the possible overlap and fragmentation relating to data breach notification under the general data protection regulation[142] proposed in January 2012. This is analysed in further detail in Chapter 5.

4.2.4 The Article 29 Working Party

The Article 29 Working Party was set up under Directive 95/46/EC[143] and is an independent advisory body. It is composed of a representative of the supervisory authority for each EU Member State, a representative of the bodies established for the EU institutions and a representative for the European Commission. It is chaired by a representative from a Member State and has the following tasks:

- to issue guidance and EU-wide interpretation of the legal framework for privacy and data protection
- to examine any question on the application of national measures under the Directive and give the Commission an opinion on the level of protection in the Community
- to advise the Commission on policy and divergences likely to affect the equivalence of protection with regard to the processing of personal data across the Union and make recommendations on other relevant matters
- to draw up an annual report on the state of play of the protection of personal data across Europe.

[141] See: Leone, 2012, ECTEG Presentation: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-Interface-2010/Presentations/Ws%201/Nicola%20Di%20Leone_ECTEG.pdf
[142] European Commission, 2012.
[143] European Parliament & the Council, 1995.

In 2012 the Article 29 Working Party adopted an Opinion on the Data Breach Notification regime in the e-Privacy Directive 2002/58/EC and indicated that the language in the proposed regime was unclear in some cases. The Opinion also proposed that a 12 month period would be necessary to develop electronic schema for breach notification (using XML as the describing language).[144]

We now turn to some further organisations, which lie another step removed from the core policy discussion related to incident notification.

4.2.5 The European Public–Private Partnership for Trust in Digital Life (EP-TDL)

The proposal for a NIS Directive describes the TDL-PPP as a major stakeholder supporting the realisation of the goals of the Directive. TDL is made up of industry players and institutes and was established in 2009 for two years from EU RTD funding in the 7th Framework Programme.[145] It aims to research, pilot and promote innovative and trustworthy ICT environments and technologies. The TDL-PPP may be regarded as a mechanism led by industry to encourage the development innovative information and communication technologies that allow individuals to determine the relative level of security of a particular device in accordance with European values of transparency and accountability. One specific activity of TDL is to raise awareness 'through monitoring the impact of incidents'. Broadly, TDL aims to set out a strategic research agenda for European values in technology developments.

Although TDL describes itself as a PPP it is not clear from openly available information the extent to which governmental organisations, aside from research institutes like the Dutch Organisation for Applied Scientific Research (TNO) and universities, are involved. In April 2013 the TDL general assembly was held.[146]

Critically, the apparent lack of involvement of governments suggests that TDL may be viewed as a self-regulatory mechanism intended to provide a face for lobbying of EU policy-makers from specific elements of the ICT industry.

The TDL-PPP is composed of a number of private sector players and other institutions like TNO.[147] It aims to increase general understanding of the 'social acquis', specifically the right to the protection of personal data in technology, among others by delivering a roadmap to enable these rights to be respected.

4.2.6 The Advanced Cyber Defence Centre (ACDC)[148]

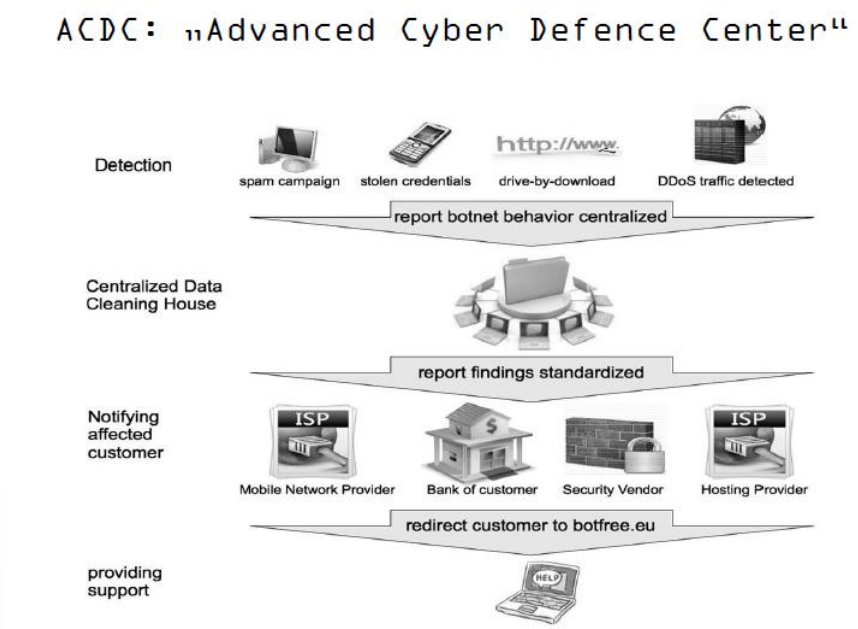
The ACDC is an anti-botnet initiative[149] whose genesis can be found in a project in Germany between ECO.de (the association of German ISPs) and various German government departments (e.g. the BSI) known as Bot-Frei (German Anti-Botnet Advisory Centre).

[144] Data Protection Working Party, 2012.
[145] Trust in Digital Life website: http://www.trustindigitallife.eu/
[146] See: Trust in Digital Life website: http://www.trustindigitallife.eu/calendar/102/10-TDL-Event-and-General-Assembly.html
[147] See: Trust in Digital Life website: http://www.trustindigitallife.eu/uploads/Trust_in_Digital_Life_Overview.pdf
[148] See: Botfree Europe website: http://www.botfree.eu/
[149] Advanced Cyber Defence Centre Factsheet: http://ec.europa.eu/information_society/apps/projects/factsheet/index.cfm?project_ref=325188

Bot-Frei originally received €2m funding in Germany. In 2012 a consortium including the operators of Bot-Frei were awarded a grant of €7.7m from the Competitiveness and Innovation Programme to expand the model to a pan-European level as a Type B pilot.[150] ACDC is currently budgeted with €15m. Although it is expected to run until 2015[151] it is hoped that it will evolve to cover other cyber-defence activities. As described on the project's website, the centralised clearing house is the single point of contact for data storage and analysis, and it distributes data in a standardised format. The support centre then distributes this information to stakeholders and affected end-users in a structured way, and offers disinfection tools and support to affected end-users and SMEs to deal with their incidents. The ACDC is active in the detection and mitigation of infected websites and the detection of network anomalies, including possible cloud- or mobile-based botnets. All data acquired using these services are sent to the centralised clearing house for further analysis. Finally, the ACDC offers a service on the integration of tools for identification and removal of malware (e.g. bots) from end-user devices.[152]

ACDC includes an element of incident reporting from users and compromised devices to a centralised clearing house. Figure 44, from ECO.de, illustrates the ACDC model.

Figure 44 Conceptual representation of the ACDC model (Source: Kraft, 2012)



[150] Type A pilots are aimed at constructing services with interoperability as the central theme aiming to demonstrate a 'federated' solution and borderless operation of national systems. Type B pilots aim at a first implementation of an ICT based innovative service carried out under realistic, market conditions (see: http://ec.europa.eu/information_society/activities/ict_psp/about/implementation/pilot_a/index_en.htm).

[151] 'The ACDC project runs over 30 months from 01/02/2013 to 31/07/2015. ACDC intends to evolve beyond the end of the project into a sustainable European centre for cyber-defence, building on the networked support centres and clearing house deployed during the project and enlarging the cyber-protection scope beyond botnets' (see: http://www.botfree.eu /).

[152] Advanced Cyber Defence Centre Factsheet: http://ec.europa.eu/information_society/apps/projects/factsheet/index.cfm?project_ref=325188

4.2.7 Networks of incident response teams

There are a number of peer groups of CERTs across the world which aim to share best practice and act as informal or semi-formal networks for co-ordination. These primarily focus on security incidents (not data breaches) and anecdotally appear to concentrate on security incidents driven by malicious activity. These peer groups include:

- the Task Force on Computer Security Incident Response Teams (TF-CSIRT), an informal network of incident response teams from Europe, which meets under the auspices of the Trans-European Research and Education Networking Association (TERENA)[153]
- the Forum of Incident Response Teams (FIRST), composed of over 400 teams globally and run as a fee paying membership organisation[154]
- the European Government CERT group (EGC), an informal peer group of European government CERTs, currently composed of CSIRTUK (the UK Computer Security Incident Response Team, DFN-CERT and the Deutsche Forschungsnetz CERT[155]
- the International Watch and Warning Network (IWWN), which was established in 2004 to foster international collaboration on addressing cyber threats, attacks and vulnerabilities; the IWWN is an information sharing mechanism to develop 'global cyber situational awareness and incident response capabilities'; its members include teams and law enforcement from Australia, Canada, Finland, France, Germany, Hungary, Italy, Japan, The Netherlands, New Zealand, Norway, Sweden, Switzerland, the UK and the US.[156]

4.2.8 The Anti-Phishing Working Group (APWG)

The APWG is another clearing house for incident reports. It is a volunteer run organisation which uses the Incident Object Description and Exchange Format (IODEF) IETF standard to process incident reports from CERTs and other organisations.[157] APWG is known to process around 1 million reports per year; a range of private sector institutions, financial organisations and others supply the APWG with data.

4.3 Conclusions

This chapter has laid out in summary the main aspects of the EU architectural response concerning cyber security. Figure 45 in Chapter 5 summarises the relationships between the main stakeholders discussed in this chapter.

Understanding who talks to whom and how co-ordination and co-operation is achieved is very complex. No-one currently has a clear understanding of how all the different pieces fit together. ENISA has been strengthening its efforts with CERTs and formulation of practical guidance on implementing Article 13a but lacks links with the end-user community.

The future of the EP3R is uncertain, especially how it will interact with the recently announced NIS platform.

[153] For more on TERENA, see: http://www.terena.org
[154] Forum of Incident Response Teams, http://www.first.org
[155] European Government CERT group, http://www.egc-group.org
[156] International Watch and Warning Network, http://itlaw.wikia.com/wiki/International_Watch_and_Warning_Network
[157] APWG, http://www.antiphishing.org . The IODEF is a format for computer security incident response teams (CSIRTs) to exchange operational and statistical incident information (see: http://xml.coverpages.org/iodef.html).

The EFMS has been instrumental in formulating guidance for Member States to operate the incident notification regime under Article 13a of the FWD.

The European Cybercrime Centre has been established since 2013 and will become operational fully in 2014. It is also planning discussions with market players active in the internet regarding cyber-crime reporting.

A number of other organisations in the public and private sectors (such as the CERT-EU; ECTEG, the TDL-PPP and ACDC initiative, and global CERT peer networks) have varying levels of capability and capacity to support incident response.

In addition to the organisations covered above, we have not noted in detail a number of other entities that somehow play a role in the security incident value network. These include PPPs such as the European Security of Control Systems Information Exchange (EuroSCSIE),[158] the 2CENTRE network (which facilitates research, training and education on tackling cyber crime)[159] and numerous non-government initiatives such as training for computer incident emergency response teams (TRANSITs).[160] Furthermore, our description above has focused on EU-level interactions, but the EU both participates in and invites formal and informal participation from relevant external organisations and initiatives including:

- the World Summit on the Information Society and Internet Governance Forum
- the International Conference on Cyberspace
- the Council of Europe
- the OSCE
- the United Nations (UN)
- the Organisation for Economic Co-operation and Development (OECD)
- the Group of Eight industrialised nations, which in 2012 declared cyber security a high priority
- NATO, which has its own Network Computer Incident Response Capability (NCRIC) and under the Cyber Defence Management Agency (CDMA) has been discussing incidents with NATO members.[161] The EU and NATO have participated as observers on different exercises exploring incident response in detail.

[158] EUROSCSIE, https://espace.cern.ch/EuroSCSIE/default.aspx
[159] 2 Centre, http://www.2centre.eu
[160] See, e.g. ENISA, 2012f.
[161] On the NATO cyber defence structure, see e.g. NATO website, http://www.nato.int/cps/en/natolive/topics_78170.htm

5 MEASURES FORESEEN IN THE PROPOSAL FOR A NIS DIRECTIVE[162]

KEY FINDINGS

- The proposal for a NIS Directive establishes requirements for Member States and covered entities (public administrations and market operators from the energy, finance, healthcare, transport and internet sector).
- Covered entities will be obliged to notify the CA at Member State level with respect to NIS incidents passing a certain threshold.
- The obligation to notify is intended to help understand a better picture of trends, analyse patterns and aid transparency for users.
- The definition of covered entities is especially challenging with respect to certain categories, such as micro-enterprises and cloud computing service providers and with regards to territoriality.
- The notification regime adds to a complex landscape of other breach notification frameworks across Europe.
- The assumptions underlying the costs are open to criticism, especially those concerning the administrative burden of firms implementing risk management measures.

In this chapter we present a critical analysis of the key aspects of the proposal for a NIS Directive as they relate to various elements of the cyber-security policy puzzle. The proposal for a NIS Directive and the related European Cyber Security Strategy[163] establish some new requirements to improve on EU efforts to tackle cyber security. However, in many respects this may be seen as not entirely innovative: the creation of CERTs with a national emphasis was foreseen in the CIIP Directive of 2009 and its action plan and update in 2011. Nonetheless, the NIS Directive makes the establishment of competent authorities (CAs) and CERTs mandatory for Member States.

5.1 Overview of the NIS Directive

The key elements of the proposal for a NIS Directive are as follows:

- Member States should establish CAs to take the policy lead for cyber security (Article 6). These CAs should:
  - monitor the application of the Directive at national level
  - receive notifications of incidents from public administrations and market operators as defined
  - consult and co-operate with relevant law enforcement and data protection authorities.
- Under Article 8 Co-operation Network, CAs should be connected via a secure network (using for example a secure pan-European electronic data exchange network such as sTESTA) where they can:
  - circulate early warnings on risks and incidents
  - ensure a co-ordinated response

[162] COM(2013) 0048 Final.
[163] See: EEAS Cybersecurity website: http://eeas.europa.eu/top_stories/2013/070213_cybersecurity_en.htm

  - regularly publish non-confidential information on ongoing early warnings and co-ordinate a response
  - at the request of a Member State or the Commission, jointly discuss and assess:
    - national NIS strategies or co-operation plans
    - the effectiveness of CERTs
  - co-operate and exchange information with:
    - the European Cybercrime Centre
    - other relevant bodies in the fields of data protection and critical infrastructures identified as within scope
  - exchange information and best practices at Member State level and with the Commission to help build capacity
  - organise regular peer reviews on capability and preparedness
  - organise NIS exercises at Union level and participate in International exercises.
- Member States should establish CERTs responsible for handling incidents and risks that are to:
  - monitor incidents at national level
  - provide early warnings and alert announcements, and disseminate information to relevant stakeholders about risks and incidents
  - respond to incidents
  - provide dynamic risk management, incident analysis and situational awareness
  - build broad public awareness of the risks associated with online activities
  - organise campaigns on NIS.
- Competent authorities need to report early warnings of NIS incidents or risks to the co-operation network based on thresholds where they:
  - grow rapidly or may grow rapidly in scale
  - exceed or may exceed national response capability
  - affect or may affect more than one Member State.
- Article 14(2) requires public administrations and market operators, as defined under Article 3(8),[164] to notify incidents having 'a significant impact upon the security of the core services they provide' to CAs.
- Competent authorities can inform the public or require the disclosure if they regard the incident to be in the public interest.
- Under Article 14(2) the Commission and Member States may define content, formats and procedures applicable to notification with the possibility for this to be implemented under a delegated acts and implementing acts.

5.2 Why an incident notification regime?

The benefits of establishing an incident reporting or disclosure system are described below.

The proposal for a NIS Directive identifies that information on incidents is essential for public authorities to react and take mitigating measures and set adequate strategic priorities for NIS. The provision of incident reports may better help scope problems and target further intervention. It may also help in the long term by analysing patterns and trends over time.

[164] A non-exhaustive list of market operators provided in Annex II namely certain types of critical infrastructure provider (energy, transport, banking and finance, and health) and information society enablers such as cloud computing companies, etc.

It might also be possible to determine the effect of any policy intervention (such as investment in cyber security, as is the case with the UK budget allocation of £650m (approximately €753m) over four years[165]).

Incident reporting is seen as a means to incentivise good behaviour in firms[166] on a neo-classical economic assumption that customers (individuals or organisations) will rationally choose suppliers that offer better security. There is some evidence to support this.[167] As a result, the predicted negative impact on the share price of stock-exchange-listed firms that can occur after a notification is intended to stimulate better information security practices, following the logic that it is cheaper for a firm to accept the costs of investing in information security measures (such as a chief information security officer or technology) than to accept the loss of stock price.

However, there are three important counterpoints to this argument. First, the evidence that consumers rationally consider security when making choices in any situation is limited at best. Recent research into behaviour suggests that individuals value short-term gains and long-term losses differently and have difficulty in conceptualising risk.[168] Therefore, the idea that breach notification regimes will somehow create a market for security is somewhat theoretical and disconnected from emergent research on how people actually behave (which is predictable but not rational).

Second, the specific mechanism of notification does not take into account temporal market dynamics and the short-term memory of investors. When the investment market sees a company that has good fundamentals (e.g. a solid balance sheet, consistent revenues over time, strong sales) but is priced very low (because of initial market reaction of a recent disclosure) then it may be more bullish about investing – thus paradoxically driving the price back up.[169]

Finally, and related to the point above, disclosure can contribute to transparency of users. In the specific case of what information is provided in the disclosure notice, this may enable individuals to take further appropriate action. More broadly, this can contribute to understanding whether the services being offered (e.g. in the case of information society service enablers) are secure.

The system above is proposed because in the view of the Commission regulatory obligations are required to create a level playing field and close existing legislative loopholes.

5.3 What entities are covered?

The entities that are affected by the proposal for a NIS Directive are very diverse – public administrations and market operators.[170] It is estimated that around 42,000 market players in addition to public administrations across the EU will be covered by it.

[165] *The Guardian*, 25 November 2011.
[166] Campbell et al., 2003.
[167] e.g. see: Cavusoglu et al., 2004, who find that the disclosure of a security breach results in the loss of $2.1 of a firm's market valuation. Telang and Wattal, 2007, find that software vendors' stock prices suffer when information about their products' vulnerability is announced.
[168] Acquisti et al., 2003.
[169] e.g. see Ko and Durantes, 2006, who found, after studying the performance of a firm after four quarters following a disclosure, that although breached firms performance overall was lower (compared with unbreached firms) their sales increased significantly.
[170] Preamble, Recital 5.

In particular, Article 3(8) distinguishes two categories of 'market operators': providers of information society services (3(8)a) and operators of critical infrastructures (3(8)b). In Annex II of the proposal, these categories are backed up with some more substance in the form of a non-exhaustive list. Public administrations are not further defined and also not mentioned in the annexes to the proposal for a NIS Directive.

5.3.1 Public administrations

Public administrations hold significant volumes of personal data, including sensitive data, and are a separate category of entity in the context of the proposal for a NIS Directive. In many countries they are also defined at national level as critical infrastructure although they have not yet been identified as such at European level. In some countries public administrations may own sensitive critical network and information systems not considered to constitute critical infrastructures within Directive 2008/114/EC on critical infrastructure. While the importance of the security and integrity of public administrations indicates the need to have them explicitly included under the scope of the NIS Directive, arguments can be made regarding the extensive certification and security measures these entities are already obliged to perform in the management of such sensitive network and information systems. Such measures are the case for example in those relating to national security, intelligence or military systems. Without greater clarification on the scope of the types of public administration covered (e.g. including military systems) there might be considerable duplication. In conclusion, an assessment of the necessity to include public administrations under the scope of the proposal for a NIS Directive can only be based on an clearer definition of which public services and infrastructures are to be included in this category.

In recital 5 of the proposal for a NIS Directive, undertakings providing public communications networks or publicly available electronic communications services are excluded because these undertakings are covered by the specific security and integrity requirements as laid down in Article 13a of Directive 2002/21/EC.[171] Therefore telecommunications data are excluded from the scope of the NIS Directive. A similar approach is taken towards trust providers. This marked differentiation in the details of reporting obligations and envisioned structures appears at odds with the overarching policy objective of providing a level playing field to all market operators across sectors.[172]

Some additional guidance is welcome to clarify the categories of services included in the definition of market operators. The definition of provider of information society services, as provided in Article 3(8)a of the Directive, seems pragmatic at first sight from the point of view of data processors and law enforcement. It refers to services that enable the provision of other information society services. The categories of critical infrastructures are clear and will likely not be very problematic when applied in practice, but when looking at Annex 2, which contains a non-exhaustive list of examples, some questions arise. The examples mentioned are very general, obviously to prevent unwanted exclusion, but in their generality cover almost everything, except for one category – hosting providers – which do not fall under either of the categories mentioned in the annex. However hosting providers fit well into the definition of market operators and could plausibly be included.

[171] European Parliament & the Council, 2002a.

[172] See Proposal for a NIS Regulation Introduction Section 1.1.; Preamble (22); attached legislative financial statement point 1.5.3.

5.3.2 Social networking services

The annex to the Directive lists a number of examples of categories of services, but some more explanation of them would be welcome. For instance, social networking sites seem to be a clear category, including Facebook and comparable services. A widely accepted definition of social networking is that they are:

> *web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.*[173]

Facebook provides other information society services, such as photo sharing, chatting and e-mailing, but whether Twitter and Whatsapp, which only facilitates text messaging, are social networks is debatable. The latter could be argued to be subject to Directive 2002/21/EC, because it provides a publicly available electronic communications service. Twitter, nevertheless, fits the definition of a social network and is considered to be one by most people. That implies that Twitter could fall under the NIS Directive and probably under Directive 2002/21/EC as well.

5.3.3 Hardware and software providers

Hardware and software providers are also excluded from the scope of the Directive. Companies that produce software (operating systems, applications such as office productivity software, databases and games) and hardware (devices and infrastructure) form part of the complex landscape of players when it comes to cyber security. Flaws or vulnerabilities in such hardware and software can be exploited maliciously to perpetrate misuse or problems resulting from bugs can result in accidents or knock-on effects. Many have argued that the behaviour of software and hardware producers (by not addressing these flaws) are particularly to blame for the poor state of security and consequent high levels of policy focus on this topic.[174] Others argue that a specific focus on technical vulnerabilities does not help; for example, many exploits identified by Microsoft's Malicious Software Removal Tool are those which exploit vulnerabilities for which a patch has been disseminated for some time.[175]

The arguments for including vendors of hardware and software under the proposals for a NIS Directive are rather weak. The main one might be that forcing them to report security events would allow a better understanding of the root cause of incidents, since many attacks and accidents exploit vulnerabilities. It might also act as an added incentive for hardware and software producers to improve engineering practices (the so called 'security by design' approach). There are a number of serious arguments that suggest that hardware and software vendors should not be included.

The most important reason against the inclusion of such entities is the question that the type of phenomena that hardware and software providers would report. Unlike malicious cyber-security incidents and accidents discussed so far, in general, vendors would be not reporting incidents but rather vulnerabilities. For example, vulnerabilities are exploited by adversaries to perpetrate attacks.

[173] Boyd and Ellison, 2008.
[174] Anderson and Moore, 2006.
[175] Microsoft, 2012.

Although it might be imagined that hardware and software vendors could report both zero-day vulnerabilities[176] and others, until a vulnerability is exploited it remains a phenomenon having 'potential': no demonstrable economic or societal harm can be shown. Those receiving the reports would be flooded with (probably highly technical information) about a possible 'attack space' but with no evidence of impact.

There is also an important question of regulatory purchase. Since many hardware and software producers are headquartered outside of the EU, it would be difficult to enforce a rule requiring them to report vulnerabilities. Hardware and software producers might have to comply with two opposing regulatory frameworks in their 'home jurisdiction' and that of the EU.

Finally, the imposition of a rule requiring the reporting of vulnerabilities would further fragment reporting mechanisms and consequently add a large burden to those covered and those receiving such reports. Researchers identified around 19 different vulnerability catalogues, and hardware and software providers already have complex systems to alert customers in confidence. These are often highly automated and orchestrated with patch management practices. Additionally, there are a range of ad-hoc 'bug bounty' programs[177] run by such companies where financial rewards are posted for those that find and report vulnerabilities to the vendor.

5.3.4 Micro-enterprises

Another difficulty lies in the choice to exclude micro-enterprises from the scope of the Directive.[178] It should be clarified whether the definition of the size of an enterprise is based on the number of employees, or the amount of revenues or data processed. In particular start-ups, which can become key players as information service providers, often have few employees and small revenues (in the first years). However, because of the ability of start-ups to leverage other internet enabling services (such as cloud computing providers) they may process huge amounts of (sensitive) personal data. A data breach at a start-up may, thus, have a significant effect.

5.3.5 Definition of market operator

The second part of Annex II, providing the list of market operators referred to in Article 3(8)b, is clear. These are market operators in sectors related to categories of critical infrastructures (energy, transport, banking, financial market infrastructures and health). The inclusion of categories such as energy allow for interpretation of the NIS Directive in light of smart grids and smart metering systems as well. The annex addresses the scope of critical services. There is no legal guidance on who is allowed to make changes to the annex and on what conditions, and no clarity on whether decisions concerning the applicability of the NIS Directive to a particular provider are made by the individual Member States or at EU level. In light of the potential conflicts regarding the applicability of the e-Privacy Directive or the NIS Directive, as described above, and also taking into account any unforeseen technological developments, it would be preferred to include a provision that clearly defines these competences and the related conditions.

[176] See: Zero Day Attacks – symantec threat trends: http://www.symantec.com/threatreport/topic.jsp?id=vulnerability_trends&aid=zero_day_vulnerabilities

[177] Böhme, 2006.

[178] Page 9 of the proposal, section 3.2 Explanatory Memorandum.

5.3.6 Territoriality and cloud computing service providers

Another important aspect of the scope of applicability of the NIS Directive relates to territoriality. The proposal for a NIS Directive does not include a provision on its territorial scope, as opposed to Directive 95/46/EC (DPD, Article 4) and the proposed General Data Protection Regulation (Article 3). As a result, non-EU companies may argue that they are not subject to the Directive. It can be argued that the sectoral US regimes on data breach notifications already apply to US-based companies, which account for most of the major information society services. It is not clear how effective these notification duties are when the data concern EU citizens.

The question of who is covered is also particularly pertinent for cloud computing service providers. In particular, the obligations under the proposed Directive under Article 15 (implementation and enforcement) notwithstanding the listing of cloud computing service providers as a market player could prove challenging. Article 15 states:

> *Member states shall ensure the competent authorities have the power to require market operators and public administrators to:*
>
> - *Provide information needed to assess the security of their networks and information systems, including documented security policies*
> - *Undergo a security audit carried out by a qualified independent body or national authority and make the results thereof available to the competent authority*

Evidence from other research suggests that auditing of cloud computing service providers is not easy. In the case of a deployment by the public administration of the City of Los Angeles of Google's services, after notable difficulties with auditing and gaining some level of confidence in the security of Google's operation,[179] the City eventually withdrew its contract with Google. There have been notable instances of outages of cloud computing providers; for example, in April 2011, major parts of Amazon's web services suffered an outage, which took engineers two days to fix. In June 2012, a severe storm hit Amazon's largest data centre in Northern Virginia, knocking several websites that rely on Amazon's web services offline.[180] It is not clear how these US-based firms report such incidents: the very nature of cloud computing means that the infrastructure (like the architecture of the internet) is 'self-healing'.[181] Furthermore, there is the ever-present question of territoriality given that although the companies may be legally based in the US, they are serving European customers, but the infrastructure (where the incident took place) is located 'in the cloud'.[182]

5.4 Impact assessment

Based on the impact assessment performed to support the legislation, option 2 of the examined approaches was chosen, according to which a regulatory approach is now taken in order to establish a common EU legal framework for NIS regarding Member State capabilities, mechanisms for EU-level co-operation, and requirements for key private players and public administrations.

[179] Robinson et al., 2011.
[180] See: Notification of hit against Amazon centres: http://aws.amazon.com/message/65648/
[181] See e.g. GigaOm, 2008, How Cloud & Utility Computing Are Different, GigaOm column, 28 February 2008: http://gigaom.com/2008/02/28/how-cloud-utility-computing-are-different/
[182] The physical location where the incident (and where a breach following an incident) took place on a cloud service provider might be on other sides of the globe and it may not be easy for a cloud service provider to even determine the exact physical location of an incident.

This seems to be the approach with the strongest positive impacts from a legal perspective. As indicated in the proposal, 'the obligations placed on the Member States would ensure adequate preparedness at national level and would contribute to a climate of mutual trust', which is a precondition for effective co-operation at EU level. The setting up of mechanisms for co-operation at EU level via the network would deliver coherent and co-ordinated prevention and response to cross-border NIS incidents and risks.

The introduction of requirements to implement NIS risk management for public administrations and key private players would create a strong incentive to manage security risks effectively. The obligation to report NIS incidents with a significant impact would enhance the ability to respond to incidents and foster transparency. Moreover, by putting its own house in order, the EU would be able to extend its international reach and become an even more credible partner for co-operation at bilateral and multilateral level. The EU would hence also be better placed to 'promote fundamental rights and EU core values abroad'.[183] However, it can be questioned whether the exclusion of telecommunications service providers from the scope of the NIS Directive is viable. There is uncertainty as to how the proposal for a NIS Directive might interact with the previously described regime for incident reporting for e-communications providers under Article 13a of the 2009 Telecommunications Framework Directive. As we have seen, from available data concerning those types of incidents reported in 2011, the majority of incidents reported have been outages and non-cyber-related security incidents (for example, battery failures). There might therefore be insufficient knowledge of incidents from this sector.

Ways to address security incidents whose causes are unclear (of the types covered by the proposal for a NIS Directive) by providers of public e-communications networks include:

- include them (effectively withdrawing Article 13a)
- exclude them, but ensure that there is consistency in the types of security incidents reported.

The Article 13a regime has been operating since 2011, so is relatively immature. Until it is proven that this mechanism is unworkable, it would therefore be preferable to refrain from intervening. A more efficient approach would be to monitor closely the types of incidents being captured and ensure that the Article 13a system is viable to capture as broad a taxonomy as possible.

5.4.1 Overlap with other proposed breach notification regimes

There are a number of other breach notification regimes that are either already in existence in the EU *acquis* or being considered. We have already noted Article 13a for telecommunications but below we identify other legal texts of relevance.

In 2012, ENISA undertook a comparison of the different reporting mechanisms at EU level.[184] Article 13a of the Framework Directive 'Security and Integrity' states that:

- providers of public communication networks and services should take measures to guarantee security and integrity (availability) of their networks
- providers must report to competent national authorities about significant security breaches

[183] Proposal, section 2.2, pp. 7–8.
[184] ENISA, 2012e.

- national authorities should inform ENISA and authorities abroad when necessary, for example in case of incidents with an impact across borders
- national authorities should report to ENISA and the EC about the incident reports annually.

Article 4 of the e-Privacy Directive[185] under the heading 'security of processing' obliges providers of public electronic communications networks or services to notify personal data breaches to the CA and affected subscribers without undue delay. The obligations are:

- to take appropriate technical and organisational measures to ensure security of services
- to notify personal data breaches to the competent national authority
- to notify data breaches to the subscribers or individuals concerned, when the personal data breach is likely to adversely affect their privacy
- to keep an inventory of personal data breaches, including the facts surrounding the breaches, the impact and the remedial actions taken.

The Data Protection Regulation released in January 2012[186] contains a regime for data breach notification. This covers data controllers (those organisations, regardless of sector, processing and needing to use personal data subject to the obligations in the legal framework). Articles 30, 31 and 31 of this proposed regulation specify that:

- organisations processing personal data must take appropriate technical and organisational security measures to ensure security appropriate to the risks presented by the processing
- the obligation to notify personal data breaches becomes mandatory for all business sectors
- personal data breaches must be notified to a competent national authority without undue delay and, where feasible, within 24 hours, or else a justification should be provided
- personal data breaches must be notified to individuals if it is likely there will be an impact on their privacy. If the breached data was unintelligible, notification is not required.

Article 15 of the proposal for a regulation on electronic identification and trust services for electronic transactions[187] in the internal market puts forward obligations concerning security measures and incident reporting:

- Trust service providers must implement appropriate technical and organisational measures for the security of their activities.
- Trust service providers must notify competent supervisory bodies and other relevant authorities of any security breaches and where appropriate; national supervisory bodies must inform supervisory bodies in other EU countries and ENISA about security breaches.
- The supervisory body may, directly or via the service provider concerned, inform the public.

[185] Article 4 of the e-Privacy directive, part of the EU legislative framework on electronic communications: http://ec.europa.eu/information_society/policy/ecomm/doc/24eprivacy.pdf

[186] European Commission, 2012.

[187] Article 15 of the Regulation on electronic identification and trust services for electronic transactions in the internal market: http://ec.europa.eu/information_society/policy/esignature/eu_legislation/regulation/index_en.htm

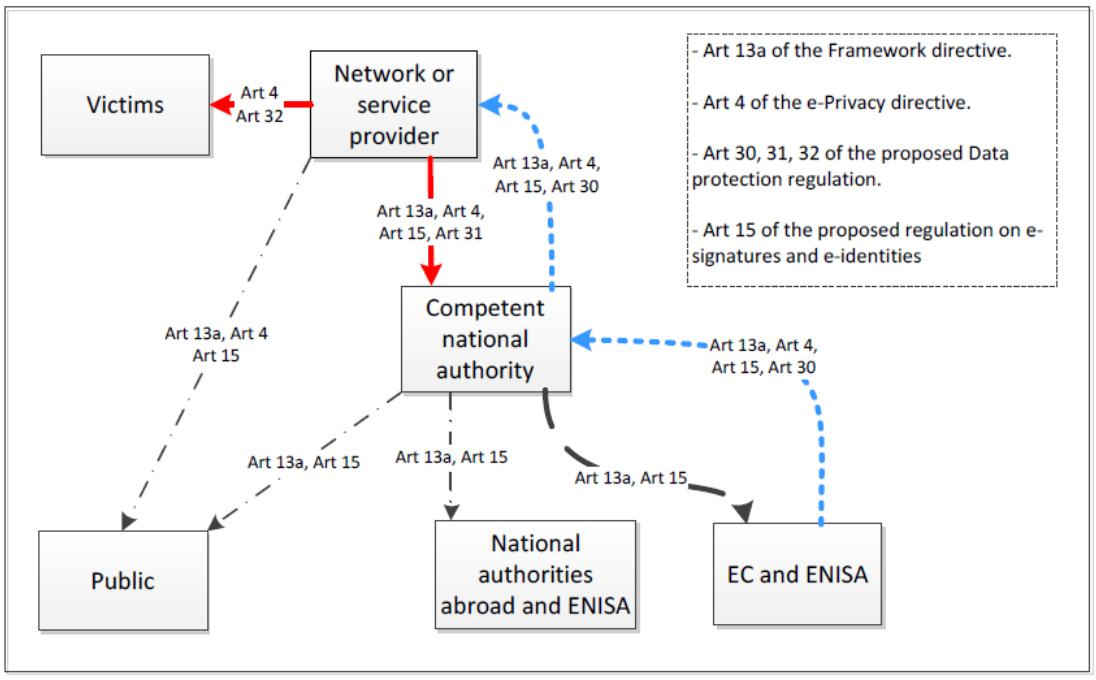
- The supervisory body sends a summary of breaches to ENISA and the EC.

Finally, of relevance, Article 14(1–3) of the agreed Directive on Attacks Against Information Systems[188] approved by the European Parliament in July 2013 also contains provisions on the reporting of statistical data about cyber-crime offences:

- Member States must ensure a system is in place for the recording, production and provision of statistical data on the offences referred to in articles 3 to 7.
- The statistical data referred to in paragraph 1 shall, as a minimum, cover existing data on the number of offences referred to in articles 3 to 7 registered by the Member States, and the number of persons prosecuted for and convicted of the offences referred to in articles 3 to *7.*
- Member States shall transmit the data collected pursuant to this Article to the Commission. The Commission shall ensure that a consolidated review of the statistical reports is published and submitted to the competent specialised Union agencies and bodies.

Figure 45 from ENISA compares the different systems (excepting the reporting of cyber crimes): Article 13a (covering security incidents in the telecoms sector), Article 4 (covering personal data breaches in the context of online privacy), articles 30–32 (covering personal data breaches by data controllers) and Article 15 (covering security breaches in e-ID systems).

Figure 45 The interplay of various breach notification regimes (Source: ENISA[189])



In an Opinion of June 2013[190] the European Data Protection Supervisor (EDPS) raised concerns about the lack of clarity of definitions and potential for overlap between the breach notification provisions of the NIS Directive and others, especially those of the proposed 2012 general data protection regulation.

[188] European Parliament, 2013b.
[189] ENISA, 2012e.
[190] Opinion, 14 June 2013.

It noted that the Cyber Security Strategy and proposal for a NIS Directive are not joined up to existing (Directive 95/46/EC) and the evolving legal framework governing breach notification in privacy and data protection legislation, specifically the breach notification provisions (in for example the e-Privacy Directive and proposed general data protection regulation). The EDPS also remarked that the proposal for a NIS Directive fails to take account of the role of DPAs. The EDPS Opinion also questions why some sectors (such as providers of security software) have been excluded from the non-exhaustive list and whether EU institutions and bodies fall under the list. It also criticises the definition of 'incident' in Article 3(4) as not making clear whether it describes a successful or unsuccessful incident. A suggestion to include some indication of consequence is proposed.[191] Finally, the EDPS notes that the implementation of notification regimes ought to involve DPAs. Specifically, as the mandate of competent authorities is not likely to include investigating data breaches, the NIS Directive should apply without prejudice to personal data breach notification obligations pursuant to applicable data protection law.

5.4.2 Overlap with legislation relative to critical infrastructures

A related piece of legislation on critical infrastructure is Directive 2008/114/EC (hereinafter the ECI Directive),[192] which concerns the definition of European critical infrastructures. It is focused primarily on countering threats from terrorism. Crucially it requires that an 'all hazards' approach for critical infrastructure protection be taken into account, including man-made, technological and natural disasters.

An interpretation of these broad terms might be expected then to include those types of incidents defined in the proposal for a NIS Directive being terrorist in motivation. The ECI Directive requires Member States to identify those infrastructures in their own country that could be defined as European critical infrastructures. These are defined as those whose disruption or destruction would have 'significant cross border impacts', including those defined as: 'trans-boundary cross-sector effects resulting from interdependencies between interconnected infrastructures'.

The ECI Directive requires Member States to notify that a particular infrastructure is regarded as being critical given a set of criteria:

- casualties criterion (assessed by potential number of fatalities or injuries)
- economic effects criterion (assessed by significance of economic loss and/or degradation of products or services, including potential environmental effects)
- public effects criterion (assessed by impact on public confidence, physical suffering and disruption of daily life, including the loss of essential services).

Thus there should logically be a subset of infrastructures in each Member State that falls into this category since they must be those that affect at least two Member States. According to the 2012 report on the European Programme for Critical Infrastructure Protection there were 14 designated ECIs – 1 across the EU in the transport sector and 13 across the EU in the energy sector.[193]

The ECI Directive also establishes mechanisms with a similar objective (although not strictly termed security incident reporting).

[191] Following Article 2(i) of the e-Privacy Directive and Article 4(9) of the Proposed Data Protection Regulation where the breach must lead to a consequence.
[192] European Council, 2008.
[193] European Commission Staff Working Document, 2012.

Under Article 6(4) the Member States should collect information on risks, threats and vulnerabilities from security liaison officers from designated ECIs:

> *Each Member State shall implement an appropriate communication mechanism between the relevant Member State authority and the Security Liaison Officer or equivalent with the objective of exchanging relevant information concerning identified risks and threats in relation to the ECI concerned.*

In turn, every two years under Article 7(2) of the ECI Directive the Commission receives generic summary data from each Member State on risks, threats and vulnerabilities in sectors where ECIs were identified on the territory of the reporting Member State. Although the information exchange mechanism under the ECI Directive is at the classified level,[194] one may assume that this reporting would by its nature include incidents (since impact is a component of risk).

Table 10 compares the characteristics of the ECI Directive and the proposal for a NIS Directive.

Table 10 Comparison between Directive 2008/114/EC and the proposal for a NIS Directive (Source: RAND Europe)

Legislation	Sectors covered	Criteria for inclusion	Threats	Threshold for inclusion or reporting	Binding?
2008 ECI Directive	Energy, transport	Those designated by Member State as owner-operators of European critical infrastructure	All hazards but a focus on terrorism	Disruption or destruction having a specific agreed severity of impact according to three cross cutting criteria (casualties, economic and public effects) on at least two Member States	No
2013 proposal for a NIS Directive	Energy, transport, finance, health, internet enablers	All covered entities in the sectors except micro-SMEs	All hazards	Significant	Yes

Furthermore, under Annex II of the ECI Directive covering an operator security procedure (OSP) for ECI owner-operators, 'permanent measures' covering 'countermeasures and controls' must be implemented, including those covering the security of information systems.

In conclusion, there are several instances of duplication between the ECI Directive and the proposal for a NIS directive.

[194] These reports are classified at an appropriate level by the Member State originating the report.

Furthermore, the opinion of the European Central Bank on the former Directive, besides emphasising the persistence of duplications in the definitions of critical infrastructures, expresses a doubt about setting up pan-European infrastructures by the means of subunits administered by the Member States.[195]

5.4.3 Costs of the system outlined in the proposal for a NIS Directive

The proposal for a NIS Directive includes a number of provisions that it is understood would incur costs to Member States, covered entities (public and private organisations) and the Union:

- the establishment of a CA at national level
- a national level CERT
- a secured network to allow the sharing of incident reports and other relevant information
- administrative burden for public and private sector organisations (e.g. setting up an information security programme)
- formulation of breach notifications to the CA.

The proposal for a NIS Directive analyses these costs according to the framework illustrated in Table 11. Note that we do not sum these items as some of them are annual expenses while others are one-off additional costs.

Table 11 Cost framework proposed by the NIS Directive (Source: Impact assessment for NIS Directive and RAND Europe)

Item	Costs	Requirement	Overall EU implication
Establishing CAs	€360,000 per Member State	On average every Member State would need to recruit an additional 6 FTE to cover the tasks of a CA	€9.72m
Establishing a national CERT in each Member State	€2.5m per Member State	Three more CERTs would need to be established to provide for EU-wide coverage[196]	€7.5m
Participation by MS	€6,000 per year per Member State	Three meetings per year at €1,000 per person for 2 people	€168,000 per year
Modification of sTESTA secured data exchange network	€1m one-off		€1m in first year
Business costs	Between €4,000 and €50,000 per year (depending on approximate size)	Extension of Article 13a and 13b to covered entities (public administrations and market operators as defined in Annex II)	Times number of covered entities (public administrations and businesses)

[195] Opinion of the European Central Bank, 13 April 2007.
[196] Excluding Croatia which joined the EU on 1 July 2013

Enforcement costs for business	Around €25,000 per investigation	Based on an expected 1,200 notifications per year and 1 FTE required to work for 5 months on an investigation	Between €4.25 and €8.5m per year
Notification of significant security incidents	Negligible	Notify of significant incidents	Negligible
Total one-off costs	€3.8m per MS		€18,220,000
Total operational costs per year	€6,000		€168,000
Total business costs per year	More than €4,000 to €50,000 per year (+ enforcement costs)		Upwards from between €4.25 and €8.5m

Table 12 shows where the competency for performing the tasks associated with a CA currently sits and whether the Member State in question has a national level CERT.

Table 12 Current landscape of competent authorities and national level CERTs in Member States

MS	Organisation(1)	National level CERT ?
AT	Unknown	Y
BE	Prime Minister's Office[197] and Belgian National Information Security Forum (BELNIS)	Y
BG	State Agency of National Security (SANS) and Ministry of Transport, Information Technology and Communications (MTITC)	Y
CR	Unknown	Y
CY	Office of the Commission for Electronic Communications and Postal Regulation	N
CZ	Cyber Security Council	T
DE	Bundesamt für Sicherheit in der Informationstechnik (BSI) and National Cyber Security Council (from 2011)	Y

[197] *Telecompaper*, 22 April 2013.

DK	Danish Intelligence Service	Y
EE	Cyber Security Council under Government Security Commission	Y
FI	Government Information Security Management Board	Y
FR	Agence Nationale de la Sécurité des Systems d'Information	Y
GR	National Authority Against Electronic Attacks	Y
HU	Steering committee under development	Y
IT	In progress: a new policy unit is being established, comprising delegates from several ministries with the mandate to define a cyber-security strategy for the country[198]	Y
IRL	In progress: a national cyber-security centre is being developed	N
LT	National IT Security Council	Y
LI	Information Technology and Communications Department, Ministry of Interior	Y
LU	Computer Incident Response Capability Luxembourg	Y
MT	Office of the Prime Minister	Y
NL	National Cyber Security Centre	Y
PL	Unknown	N
PT	Anacom Portuguese Telecommunications Regulatory Authority	Y
RO	Operative Cyber Security Council	Y
SK	Unknown	Y
SLO	Unknown	Y
SP	Centro Nacional para la Protección de las Infraestructuras Críticas	Y
SE	Swedish Civil Contingencies Secretariat	Y
UK	Office of Cyber Security and Information Assurance	Y

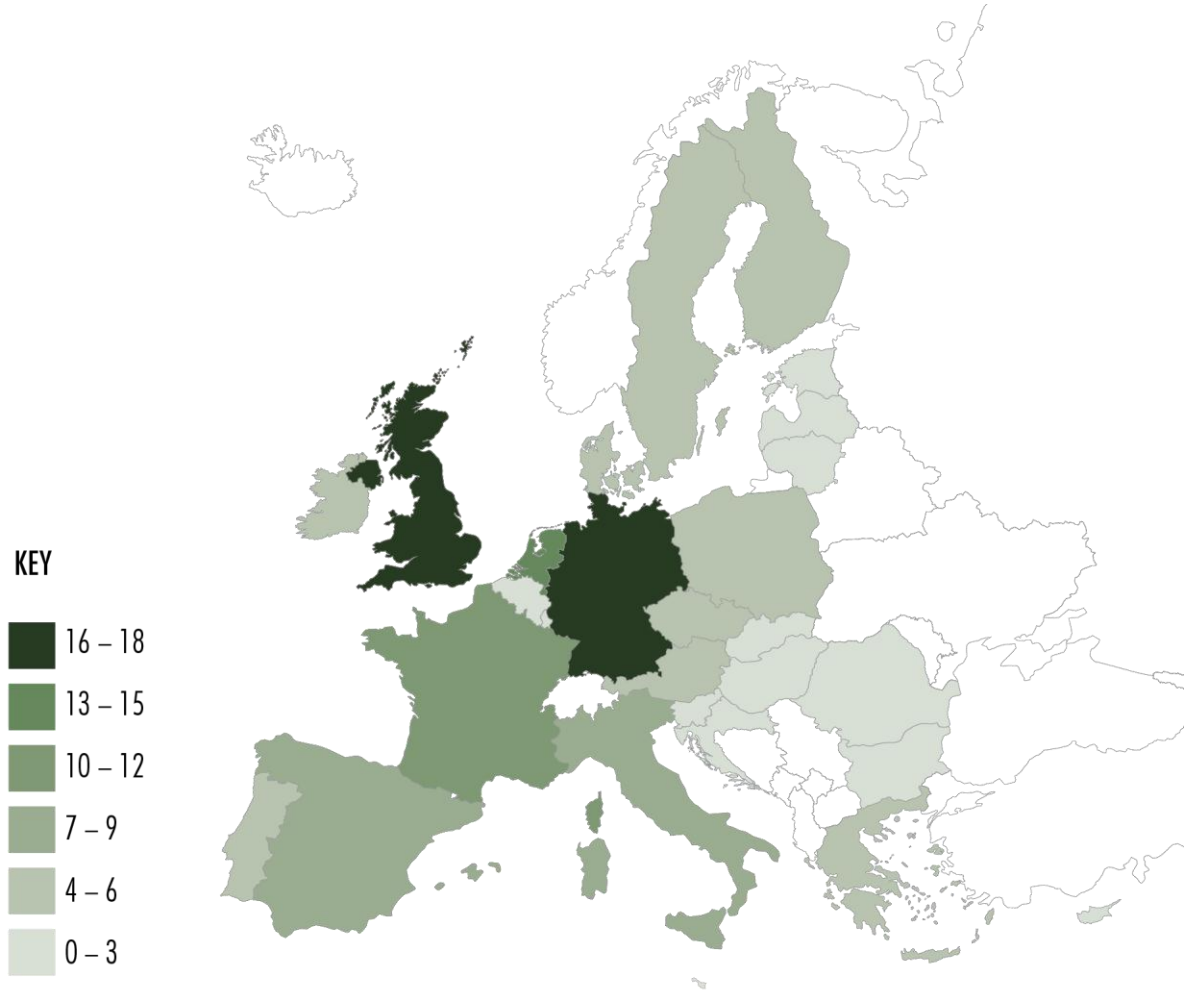
[198] *Official Gazette*, 19 March 2013.

(1) The institution most likely to assume the role and tasks of a CA as envisaged by the proposal for a NIS Directive

Figure 45 shows that there is significant divergence in approaches from Member States of who owns cyber security, especially relating to the CA.[199] Thus, the additional six full-time equivalents (FTEs) estimated per Member State will need to be additional to the headcount of existing ministries or within specific cyber-security organisations.

Figure 46 shows the total number of CERTs of all types in European countries.

Figure 46 The number of CERTs by country (Source: ENISA)



The costs associated with establishing a CERT do not take into account the fact that according to anecdotal evidence[200] it is extremely difficult to estimate FTEs for CERTs because the numbers involved fluctuate depending on the severity of an incident. In a large scale incident likely to fulfil the criteria specified by the NIS Directive, it is likely (by its very character) that the CERT might need to pull in extra resources from elsewhere in order to cope.
Nonetheless, there is some evidence from the US on the numbers of CERT personnel. For example, according to testimony from the US Inspector General speaking to a Congressional

[199] Robinson et al., 2013.
[200] Anonymous interviewee.

Panel in 2010, the US-CERT had 55 personnel and aimed to recruit another 25 (taking the total to 80) in 2011.[201]

The proposal for a NIS Directive also stipulates that a CERT will need to exist in a secured facility. This merits further consideration. Review of ENISA's directory of CERTs in Europe shows that many CERTs of national importance are based in a university or not a government owned facility. The costs for each CERT already existing to be set up in a secured facility is not detailed in the estimate accompanying the proposal and evidence from other research suggests that this is not negligible. For many CERTs of national importance situated on university campuses that have grown out of national research and education networks this could have significant cost implications.

Another complicating factor is the diversity of policy ownership regarding cyber security. There are a number of likely drivers of why, as the impact assessment notes, cyber security is owned by such a diverse range of administrative structures across the EU. Part of this might be attributed to the contextual way in which government is undertaken – as might be expected, this is incredibly diverse. For example, Pollitt and Bouckaert[202] note five key features of public administration systems which are crucial when considering how reforms are implemented in practice. These are state structure, executive government, minister and mandarin relations, and administrative culture and diversity of policy advice. Table 13 summarises Pollitt and Bouckaert's analysis for some countries.

Table 13 Government organisation models in EU countries (Source: Politt and Bouckaert, 2008)

Country	Organisation
State structure	Federal (Belgium) Co-ordinated (Germany) Unitary (Netherlands) Decentralised > centralised Fragmented
Executive government	Majoritarian (UK) Consensual (Finland) Intermediate (Germany) Coalition (Italy)
Minister–or mandarin relations	Separate Integrated Politicised (Italy) > not politicised (UK)
Administrative culture	Public interest *Rechtstaat* Pluralistic
Diversity of policy advice	Civil service Consultants, universities Broad or diverse

These factors influence the practicality of implementing the necessary reforms (such as establishing a CA for NIS or encouraging collaboration between different ministries).

[201] Federal Computer Week, DHS Hearing, 16 June 2010.
[202] Pollitt and Bouckaert, 2011.

Another issue is the size of central government and the breadth of its hold over government spending.[203]

Finally, from a substantive perspective, it is known that there is a difference in how security is dealt with in different countries. Many of the Nordic and Baltic countries have adopted a strategy of 'collective defence' (witness the Estonian Cyber Defence League) where all parties know their responsibility and actively contribute to national defence. Others have a top-down approach (e.g. Italy and Spain) set by legislation and regulation from government. The UK and NL are well known to favour a public–private partnership model, which aims to improve overall security performance by using policy levers to effect actions and behaviour. None of these models have so far been proven to be more or less effective when it comes to cyber security – they merely demonstrate how reforms such as the process of establishing CAs for NIS might play out.

The accompanying impact assessment for the proposal for a NIS Directive suggests from 'consultations with several NIS bodies' that, on average, six additional (FTE) employees would be required to meet the criteria of sufficiency with regard to personnel needed for a CA to implement the common requirements. Noting the diversity of cyber-security organisations in different Member States, this seems like an overly broad estimate. For example an additional six staff in the German Bundesamt für Sicherheit in der Informationstechnik would result in an increase of just under 1% in staffing levels, but an increase of six staff in the UK's Office of Cyber Security and Information Assurance (OCSIA), which currently has an estimated 34 staff, would result in an increase of more than 18% in staffing levels.

Table 14 shows the numbers of personnel known to work at some of the most well-known cyber-security units for which data are readily available.

Table 14 Numbers of people in some existing cyber-security units (equivalent to CAs)

Country	Organisation	Personnel in CA	Total central government ('000s)[204]
France	ANSSI	250[205]	2,190 (2010)
Germany	BSI	550[206]	192 (2009)
South Korea	NCSC	Classified	154 (2008)
United Kingdom	OCSIA	34 (2012)[207]	242 (2012)
United States	DHS	1,024[208]	2,098 (2009)

[203] Ibid, p. 53.
[204] See OECD country profiles: http://www.oecd.org/gov/pem/hrpractices.htm
[205] Report to the French Senate on the public administration: http://www.senat.fr/rap/r11-681/r11-68123.html
[206] German Federal Statistical Service: https://www.destatis.de/EN/FactsFigures/SocietyState/PublicFinanceTaxes/PublicService/PublicServicePersonnel/Tables/FunctionalArea.html
[207] Anonymous interviewee.
[208] DHS Annual Report, 2011.

Although not strictly directly related to security incidents (but rather to the prosecution of those who have been found to break the law in incidents), evidence from comparative analysis of the numbers of personnel in cyber-crime units at Member State level may be seen as a useful comparator (broadly assuming an equal relationship between the level of interest accorded by Member States to investing in tackling cyber crime and in cyber security). Table 15 presents some data from 2011 on the reported numbers of personnel from 15 Member States working on tackling cyber crime in 2010, which vary widely from country to country, illustrating the sheer diversity of different capabilities of law enforcement in this area.[209]

Table 15 Numbers of law enforcement personnel working on cyber crime in 2010 at Member State level and in the HQ (Source: RAND Europe)

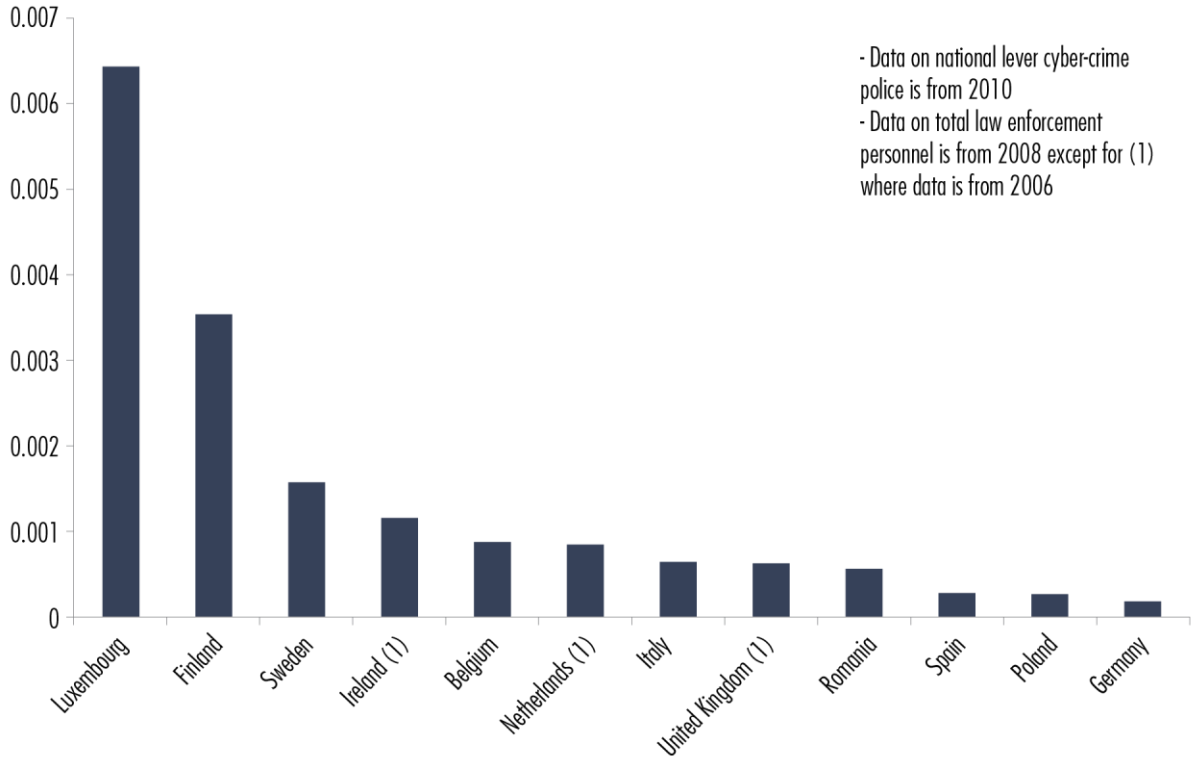
Country	Total in country	Number in national HQ unit
Belgium	249	33
Cyprus		13
Finland	>24	29
France (incl. National Police & Gendarmie)	548	74
Germany	>100	43
Ireland		15
Italy	1,966	144
Luxembourg		10
Netherlands		30
Poland		26
Romania	170	28
Slovenia	45	7

[209] See OECD country profiles: http://www.oecd.org/gov/pem/hrpractices.htm
[209] Report to the French Senate on the public administration: http://www.senat.fr/rap/r11-681/r11-68123.html
[209] German Federal Statistical Service: https://www.destatis.de/EN/FactsFigures/SocietyState/PublicFinanceTaxes/PublicService/PublicServicePersonnel/Tables/FunctionalArea.html
[209] Anonymous interviewee.
[209] DHS Annual Report, 2011; 2012.

Spain (National Police)	182	46
Sweden	250	30
United Kingdom		104

Figure 47 illustrates the diversity in numbers of personnel in the national level high tech crime unit compared against the total numbers of personnel working in the law enforcement according to the UN Office on Drugs and Crime (UNODC). Controlling for the total numbers of staff working in law enforcement, a somewhat fragmented picture emerges. Noting the variations in approaches and numbers laid out above, and assuming this were to be the case with the staffing of CAs, we suggest that it is difficult to predict how many personnel would be needed to perform the tasks of a CA satisfactorily.

Figure 47 National level cyber-crime officers as % of total law enforcement personnel



5.4.4 Administrative burden

The impact assessment accompanying the Directive estimates that around 42,000 market operators and all EU public administrations will be covered. The total administrative burden for this is viewed as €1–2bn.

The proposal for a NIS Directive and its accompanying impact assessment suggest that the administrative burden for those covered entities (public administrations and market operators) complying with the provisions would be between €4,000 and €50,000 per year depending on business size.

These costs are driven by the fact that companies that are either critical infrastructure providers or already classified as data controllers would have risk management systems in place to meet the provisions of:

- Article 11 of Directive 2008/114/EC (the ECI Directive), which makes risk management and mitigation plans mandatory covering all hazards (assumed to include NIS incidents
- Article 17(1) (security of processing) of Directive 95/46/EC covering protection of personal data and as extended into a breach notification regime under the proposed 2012 general data protection regulation.

The impact assessment accompanying the proposal for a NIS Directive[210] states that additional costs for risk management measures necessary to comply with the provisions of the proposal for a NIS Directive would overlap for many covered entities because they are either owner-operators of critical infrastructure or data controllers:

> *Depending on the precise ICT security measures and requirements that will be defined for the implementation of the NIS Regulation, there could be quite some overlap with the measures already foreseen for the Critical Infrastructure (CI) operators and data controllers.*

Furthermore,

> *It can be assumed that an important part of the additional ICT spending required is still needed in order to fully comply with other regulations than the Network and Information Security regulation or would be made 'naturally' (i.e. because of commercial or good governance reasons) by the actors within the scope of this assessment. As such, only part of the additional cost presented in Table 13 will possibly be caused by NIS Regulation and, by consequence, be considered as a compliance cost caused by it.*

This logic exposes a number of concerns regarding the thinking behind the proposals in the Directive:

- Companies likely to be covered, if they are critical infrastructure owner-operators, must already implement security measures under the provisions of the 2008 EU Critical Infrastructure Directive (which may already be a more mature mechanism to obtain the insight into relative status of critical infrastructure that the Directive requires without the necessity of incident reporting).
- The cost assessment of the burden to comply with the provision of dealing with NIS incidents is driven by an appreciation of the risk management measures necessary to address two different types of issue to that of NIS incidents:
    - all types of hazard to critical infrastructures (in which case this may be inefficient because critical infrastructure investment under an all hazards approach to address non-NIS security and safety issues,[211] in addition to covering NIS incidents, may be well in excess of that required to cope with NIS incidents)

[210] ANNEX 3: Assessment of Nis Risk Management Compliance Costs for Public Administrations and Key Private Players.

[211] For example, that associated with preventing or mitigating the effects of a Deepwater Horizon type incident.

  - the security of processing of personal data breaches (in which case, as we have seen, this may only be part of the problem as the risk management measures may not cover incidents not affecting personal data such as DDoS attacks or theft of company intellectual property).
- The cost impact for SMEs is based on an assumption about limited extra NIS spending being required for this segment over and above that being spent to comply with the provisions of EU law concerning critical infrastructure and/or personal data protection. SMEs by their nature are unlikely to be critical infrastructure providers.

In any case, data such as those from Chapter 3 (map of businesses with a security policy in EU27) illustrate that companies do not take security seriously and consistently fail to implement any measures. Purely from a cost perspective it would be futile thus to assume that the additional compliance costs would be based only on those that do not already have to meet obligations either as critical infrastructure providers or data controllers.

The key question then becomes to what extent those risk management measures that a firm might implement already under these two provisions might be effective in managing NIS risks, given as we have seen the proportion of reported incidents that could broadly be conceived as related to breaches of confidentiality (affecting personal data) is low in comparison to either those affecting the integrity of information (malicious code) or the availability of information (DDoS attack).

Table 16 illustrates this gap. It lists categories of incidents collected in a survey into cyber-security practices by Eurobarometer in 2011.

Table 16 Categories of incidents and relevant legal frameworks for reporting

Eurostat defintion	Meaning	Relevant legal framework for reporting of incidents
Enterprises experienced ICT-related security incidents that resulted in unavailability of ICT services, destruction or corruption of data due to hardware or software failures	Loss of availability from accidents, error (we also assume this definition includes possibility of upstream natural disasters, solar flares, hurricane, outage of infrastructure supplying ICT)	ECI Directive 2008
Enterprises experienced ICT-related security incidents that resulted in unavailability of ICT services due to attacks from outside, e.g. denial of service attack	Loss of availability from an external adversary	-
Enterprises experienced ICT-related security incidents that resulted in destruction or corruption of data due to infection or malicious software or unauthorised access	Loss of availability or integrity from external adversary	-

Enterprises experienced ICT-related security incidents that resulted in disclosure of confidential data due to intrusion, pharming, phishing attacks	Loss of confidentiality from external adversary with economic motivation	Data Protection Directive 1995 or proposal for a general data protection regulation 2012
Enterprises experienced any ICT-related security incidents excluding disclosure of confidential data in electronic form by employees	Loss of confidentiality due to external adversary or other reasons	Data Protection Directive 1995 or proposal for a general data protection regulation 2012
Enterprises did not experience any ICT-related security incidents excluding disclosure of confidential data in electronic form by employees	Companies not experiencing ICT-related security incidents (loss of confidentiality) from insiders	
Enterprises experienced ICT-related security incidents resulting in disclosure of confidential data in electronic form by employees whether intentionally or unintentionally	Loss of confidentiality by insiders by accident or deliberately	Data Protection Directive 1995 or proposal for a general data protection regulation 2012

The proposal for the NIS Directive estimates that 28,000 SMEs will be covered (68% of the 42,000 total covered entities in the private sector). The total costs for the private sector to implement risk management measures in accordance with the Directive have been estimated to range from €360 to €720 million. Per small and medium-sized enterprise (SME), this works out between €2,500 and €5,000. According to the European Commission definition of SME as a company with a balance sheet not exceeding €43m, this sum is equivalent of more than 0.005% of the balance sheet of an SME.

Spending on NIS risk management measures is complex. Although, as has been stated, risk management standards describe practices that are regarded as helpful in managing information security,[212] there is no straightforward globally accepted list of what constitute effective security measures that might apply under the provisions of risk management measures.[213] In Table 17 we present some examples where costs might be relatively easily measured.

[212] For example, the UK Information Security Breaches Survey 2013 indicates 10 'steps' that it measured UK large and small firms on: information risk management; user education and training; home and mobile working; incident management; managing user privileges; removable media controls; monitoring; secure configuration; malware protection and network security.

[213] E.g. see NIST Special Publication 800-53 Rev 3, 2010.

Table 17 Example risk management measure and types of cost (Source: RAND Europe)

Risk management measure	Types of cost
Someone responsible for information security in the organisation	FTE costs per annum for a chief information security officer
A management system to set up and monitor the execution of the risk management measures in the organisation	Costs of time to establish, prepare, run and monitor management system FTE time for attendance at meetings Lost opportunity costs for attendance at meetings
Endpoint defence measures (covering real-time protection against anti-virus; malware etc.) on devices used on the network (e.g. desktop, laptops and mobile devices) to mitigate against a range of NIS incidents affecting the confidentiality, availability and integrity of information	Software licensing costs Software support
Network security appliances (e.g. firewall, intrusion detection system or intrusion prevention system to mitigate against incidents affecting the confidentiality and integrity of information	License costs for the software Monitoring and system support Infrastructure costs (e.g. the physical machine to run the software)
Resilient network connections to mitigate against incidents affecting the availability of network	Purchasing internet access from a second Additional internet service provider; additional costs from an ISP
SSL Certificate to secure connections and mitigate against incidents affecting the confidentiality of information	License costs
Backup or disaster recovery systems if there is hardware or software failure affecting the availability of information	Service support from a disaster recovery company; Ongoing maintenance costs to run a backup site
Incident response team (CERT)	Ongoing FTE costs for personnel in a team Upfront and ongoing software and infrastructure costs for an incident response team
Awareness and user training	Costs to license or design in house a training programme FTE costs of employees to attend courses Lost opportunity cost of employees taking the course

Table 17 should be read with great caution as it is very conservative interpretation and does not reflect many nuanced issues regarding how organisations actually buy, license or implement measures. For example, many organisations may be investing in resilience measures (unwittingly or actively) as part of a package offered by a service provider. There may be managed security service providers which offer these services as a whole (in which case the security is bundled together, possibly with other ICT-related services). The advent of cloud computing has somewhat revolutionised this model because firms have no need to implement fewer of these measures (especially regarding confidentiality and availability) because they can access organisational data and applications 'in the cloud'. Indeed, it is fair to say that many SMEs use this model, effectively wholly outsourcing parts of security to their cloud service provider or a managed security service provider. Given the economies of scale possible under such arrangements, it is no surprise and this outsourcing of security to cloud service providers may in a certain sense be considered beneficial from the perspective of security.[214]

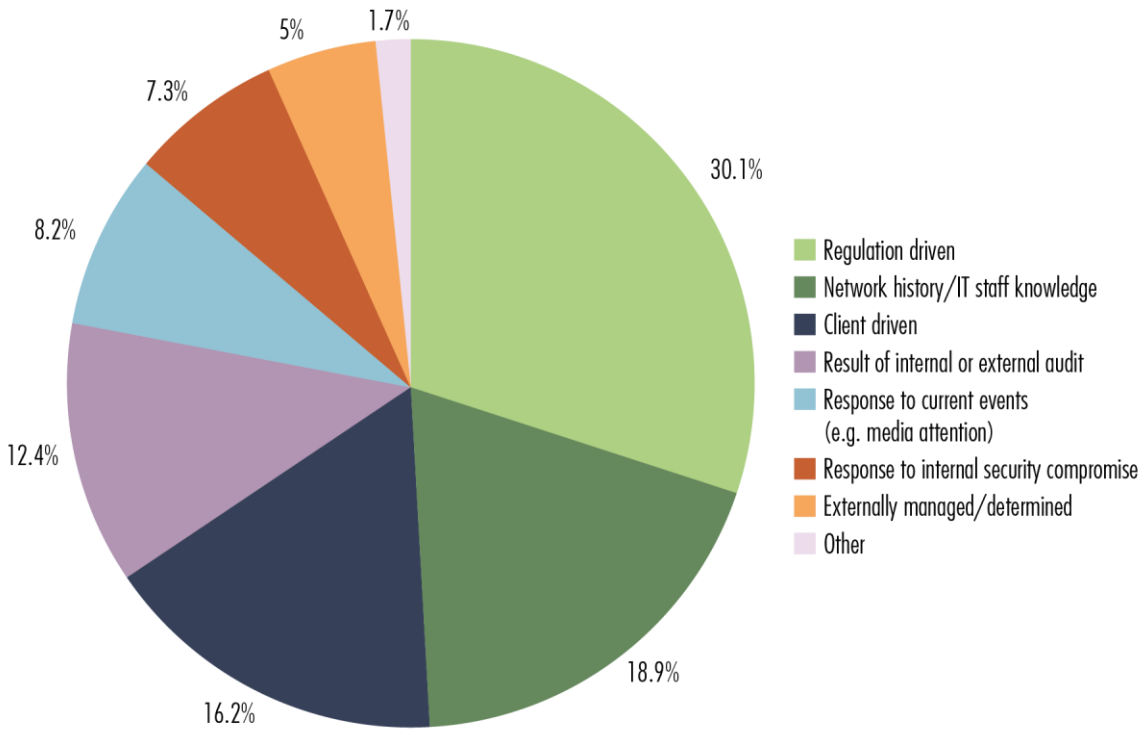
5.5 Supply side factors in the market for cyber security

The IT security services and technologies industry is a fast-growing global industry. As companies continue to expand the technologies they use to improve their overall security, the worldwide information security technology and services market is forecast to reach $67.2 billion (approx. €50.7bn) in 2013, up 8.7% from $61.8bn (approx. €46.6bn) in 2012, according to Gartner, Inc, a global marketing consultancy firm.[215] The market is expected to grow to more than $86 billion (approx. €64.8bn) in 2016. While in 2011 small or mid-size business demand, advanced persistent threats and compliance were among the main drivers of expenditure[216] in 2013 challenges represented by trends in technology use (such as bring your own device or big data analytics) and advanced threats are reported to be important drivers for the market.

Studies conducted on the demand side in US companies suggested that the demand for information security tools and services is driven by various factors, of which regulatory requirements and skills of the staff were the most important, followed by client requirements (suggesting that IT security indeed is incorporated in the competitive strategy of the businesses) and response to audits and recent incidents within the company or reported by the media.[217] Figure 48 outlines some drivers of corporate investment in IT security.

[214] For example, cloud computing service providers may leverage of the law of big numbers with regard to analysing data on incidents from a broader data set than an SME alone to determine trends and patterns thus resulting in 'security benefit'.
[215] Gartner Group, 11 June 2013.
[216] Gartner Group, 26 April 2012.
[217] Rowe and Galagher, 2006.

Figure 48 Drivers of corporate investment in IT security (Source: Rowe and Galagher, 2006)



While surveys report that companies' spending on IT security is growing, it is a widespread opinion that spending is not optimally allocated across effective prevention and protection measures. One survey in 2012 found uneven implementation of cyber-security measures among leading companies and a significant overconfidence in companies' security performance. For instance, while 70% used some kind of malware detection tool, only half of the surveyed companies had automated patch management or used intrusion detection tools.[218] Overall, the survey found a 'diminution of detection technology arsenals' with declines in the use of malware and intrusion detection tools, and tools for vulnerability scanning, security event correlation and data loss prevention.[219]

5.6 Estimating the total costs for investment in cyber security

Comparing the estimates from the impact assessment accompanying the proposal for a NIS Directive to the estimated costs of various risk management methods designed to address cyber crime, extrapolated by a 2012 paper from academics led by a team from the University of Cambridge,[220] is insightful. This paper extrapolated (again with significant caveats) costs from the UK to a global basis controlling for the UK share of GDP. Our analysis for the following countries below reverse engineers that for a number of the comparators covered in this study controlling for share of global GDP.

The costs to implement measures across all the private sector to tackle incidents relating to cyber crime are estimated to be at over €925m for just three EU Member States (Table 18).

[218] Automated patch management tools ensure that updates from software manufacturers regarding newly discovered vulnerabilities are installed on computers running that software.
[219] Lewis, 2013.
[220] Anderson, 2012.

Table 18 Estimate of costs of information security measures in the UK, Italy, Germany, France, Japan and the US (Based on Anderson et al, 2012)

Item ($ converted to €)	Global est.	UK	Italy	Germany	France	Japan	US
Share of GDP	100	0.029%	0.0230%	0.039%	0.0279%	0.057%	0.19%
Risk management measures (mln €)							
Expenditure on anti-virus	2652	76.643	60.996	103.428	73.9908	151.164	503.88
Cost to industry of patching	780	22.542	17.94	30.42	21.762	44.46	148.20
ISP clean-up expenditures	31.2	0.902	0.7176	1.2168	0.87048	1.7784	5.93
Cost to users of clean-up	7800	225.420	179.4	304.2	217.62	444.6	1482.00
Defence costs of firms generally	7800	225.420	179.4	304.2	217.62	444.6	1482.00

5.7 Conclusions

Chapter 5 has shown a number of aspects of the costs of implementing measures to provide cyber security that merit further attention. We focused mainly on costs to the Member States in the form of the establishment of competent authorities and CERTs and the administrative burden. We did not consider in the same level of detail enforcement costs (fines and compliance) and infrastructure costs for connection to the sTESTA network, as the sTESTA network is distinct from the internet and its use is highly restricted.

Many of the costs associated with putting in place measures require careful scrutiny – for example, the numbers of an FTE in a CERT may fluctuate depending on the seriousness of an incident and FTEs responsible for cyber security (as with numbers of law enforcement personnel responsible for tackling cyber crime in national level units) bear little relationship to other dependent variables such as numbers of FTE in central government

While the assumptions underpinning additional estimates for costs to the Member States (e.g. for six additional FTE to perform the functions of the CA and remaining national level CERTs) are not made clear, there is no evidence to suggest that these estimates are unreasonable

The calculated administrative burden placed on covered entities to comply may be based on erroneous assumptions stemming from confusion as to how security risk management assesses the measures that firms may implement under either critical infrastructure or data protection regimes which apply to the sorts of incidents intended to be covered by the proposal for a NIS Directive.
In its conservative understanding of risk management measures, the proposed Directive may have an untoward effect on the competitiveness and innovation of users and providers of cloud computing services and managed security service providers.

6 RELEVANT CYBER SECURITY PRACTICES IN OTHER JURISDICTIONS

KEY FINDINGS

- Many countries have voluntary, closed mechanisms for security incident reporting, especially on critical infrastructure.
- The recent US Executive Order of February 2013 aims to set up a system of voluntary information sharing of cyber-security data between government and critical infrastructure owners.
- The US NIST Cybersecurity Framework will create a set of tools that organisations can use to help meet the goals of the Executive Order.
- The security incident reporting system in India is the closest comparator to the regime described in the proposal for a NIS Directive.
- There is a difference between security incident reporting and data breach notification systems.
- A number of countries have data breach notification systems which are public in nature.
- There is a wealth of non-regulatory systems including technical, operational and grassroots mechanisms.
- Data breach notification laws (specifically covering the notification of losses of personally identifiable information) are common in the US.
- There is no comparable mechanism for security incident notification for sectors like 'enablers of information society services' as identified in the proposal for a NIS Directive Article 38(3).

6.1 Introduction

There are a number of examples of cyber-security practice which it is useful to consider, though determining effectiveness is highly complex. In this chapter we describe some of those that we believe have promise and then compare and analyse them against the proposals in the NIS Directive. It should be noted that our analysis is based on a limited set of data and analysis we were able to perform in the context of this long briefing. Therefore the findings should be taken with great care.

6.2 Incident reporting and notification regimes in selected third countries

6.2.1 The United States

The US has not formally gone down the route of mandating via legislation the notification of security incident data as is detailed in the proposal for a NIS Directive. The sharing of security threat data in the US is planned to be covered under a cyber-threat intelligence scheme in the US Presidential Executive Order[221] 13636 of February 2013. This initiative, which is currently being discussed, aims to resolve the failure of the US Congress to agree on cyber-security legislation.

[221] The White House, 12 February 2013.

The Executive Order is widely regarded to be a revised version of the Cybersecurity Information Sharing and Protection Act (CISPA), which the US Senate was unable to pass in 2012. Crucially the Executive Order does not specify minimum standards for businesses to take. The specification of such standards was seen as placing too much of an administrative burden on industry. These concerns along with those over privacy and civil liberties caused senators to filibuster the debates, killing the legislation.[222]

The 2013 Executive Order will set up a trusted information sharing mechanism between US federal agencies collecting cyber-security data and private sector critical infrastructure owner-operators. It will require federal agencies to produce unclassified reports of threats to US companies and requires that the reports be shared in a timely manner. The Executive Order essentially expands the 2011 Defense Industrial Base (DIB) pilot to non-defence organisations.

The February 2013 Executive Order also goes hand in hand with a cyber-security framework being developed by the US National Institute of Standards and Technology (NIST), which will encompass a set of practices to reduce cyber risks to critical infrastructure.[223] This framework is expected to be technology neutral and enable critical infrastructure owner-operators to benefit from a competitive market for products and services. According to the NIST the framework takes a high level view of how organisations can manage cyber-security risk by focusing on key functions of an organisations approach. These are then broken down into categories. The framework consists of five functions and three implementation levels (senior executive, business process manager and operational manager). Table 19 summarises the NIST framework.

Table 19 NIST framework core draft (Source: NIST[224])

Function	Description
Know	Gaining the institutional understanding to identify what systems need to be protected, assess priority in light of organisational mission, and manage processes to achieve cost effective risk management goals
Prevent	Categories of management, technical and operational activities that enable the organisation to decide on the appropriate outcome-based actions to ensure adequate protection against threats to business systems that support critical infrastructure components
Detect	Activities that identify (through ongoing monitoring or other means of observation) the presence of undesirable cyber risk events, and the processes to assess the potential impact of those events
Respond	Specific risk management decisions and activities enacted based on previously implemented planning (from the prevent function) relative to estimated impact
Recover	Categories of management, technical and operational activities that restore services that have previously been impaired through an undesirable cyber-security risk event

[222] *New York Times*, 13 February 2013.
[223] National Institute of Standards and Technology (NIST), 2013.
[224] NIST Framework Core draft of July 2013.

This framework appears promising because it specifies in a technology neutral way the functions that an organisation needs to perform and will elaborate relative levels of implementation. However, discussions on the framework are still going on; the consultation process is proceeding with further workshops with industry and academia in 2013.

The controversial CISPA was a proposed law introduced in 2011 by the House of Representatives. After much controversy it was stalled in spring 2013. The White House suggested that the bill lacked confidentiality provisions and civil liberties safeguards and despite it being re-introduced and passed in the House of Representatives in April 2013, ultimately it was not voted on by the US Senate.[225]

CISPA was heavily criticised by a number of civil society organisations such as the American Civil Liberties Union (ACLU) and Electronic Frontier Foundation on the grounds that there were not enough limits on how the government might monitor internet browsing habits to order to pursue the bill's objectives of tackling those who misuse cyber space.[226] It was supported by industry associations (such as TechAmerica), telecommunications and information technology companies whose representatives saw its value in sharing important cyber-threat information with the US government. The key challenge with CISPA was in regard to the limits on what the government might do with information received from the private sector and the focus of the legislation on the protection of unauthorised access to networks and systems including unauthorised access aimed at stealing private or government information.

Identification of critical infrastructure in the US Executive Order is under Section 9 and excludes commercial information technology products or consumer information technology services.[227]

The challenge in understanding a definition of an incident in the US is that there is no single definition of a security incident that covers everything. For example (as we have seen, NIST definition is an operational – non-binding one). For example, The US energy sector is governed by regulations that state a cyber-security incident to be:

> *a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communications networks including hardware, software and data that are essential to the Reliable Operation of the Bulk-Power System.*[228]

The Senate Commerce Committee Bill[229] proposed in July 2013 directs NIST to develop voluntary standards for cyber-security best practices. It empowers NIST to develop these standards so they are technology neutral, support cutting edge research, and increase public awareness and improvements to the workforce to better address cyber threats.

The 2013 proposed Deter Cyber Theft Act requires the US Director of National Intelligence (DNI) to compile an annual report on foreign economic and industrial espionage, including a priority watch list on the worst offenders, list of countries and companies engaging in cyber theft and products affected. The bill would set up a system which would block the

[225] The White House Statement, 2013.
[226] ACLU, 2011, and Electronic Frontier Foundation, 2011, statements.
[227] The White House, 19 July 2013.
[228] According to 18 CFR 39.1.
[229] See: Senate Commerce Committee Cybersecurity Bill (July 2013): http://www.scribd.com/doc/153217353/Senate-Commerce-s-cybersecurity-bill

import of products estimated to contain stolen US technology based on the intelligence gathered by the DNI.
The bill also sets up a system for monitoring actions taken by the DNI and other federal agencies with respect to combating industrial or economic espionage in cyber space.

IN 2012 the Electronic Privacy Information Center (EPIC) commented on the 2012 DIB pilot and remarked that the voluntary participation by DIB participants should remain so and that sharing from government towards the DIB of cyber attack information or intelligence should never be on the basis of a quid-pro-quo arrangement (when it is withheld unless DIB agrees to provide information). Another important amendment debated was creating a system of liability on excessive over-exposure of information to reduce over-sharing, especially of personally identifiable information.

At the operational level, in the US the Department of Homeland Security and NIST may be considered to be at the forefront of implementation (and the closest organisation comparators to EU with regard to implementation of the cyber-security framework). DHS is given a role in the implementation of Executive Order 13636 to:

- develop a technology neutral cyber-security framework
- promote and incentivise the adoption of cyber-security practices
- increase the volume, timeliness and quality of cyber-threat information sharing
- incorporate strong privacy and civil liberty protections into every initiative
- explore the use of existing regulations to promote cyber security.

PPD-21 replaces PDD-7[230] and directs the executive branch to:

- develop a situational awareness capability that addresses physical and cyber aspects of how infrastructure is functioning in near-real time
- understand the cascading consequences of infrastructure failures
- evaluate and mature the public–private partnership
- update the national infrastructure protection plan
- develop comprehensive research and development plan.

PPD-21 identifies 14 critical infrastructure sectors:

- chemicals
- commercial facilities
- communications
- critical manufacturing
- dams
- the defence industrial base
- emergency services
- energy
- government facilities
- healthcare and public health
- information technology
- nuclear reactors, materials and waste
- transportation systems
- waste and wastewater.

[230] The White House, 12 February 2013.

In 2008 the US Securities and Exchange Commission (SEC) proposed new security and privacy guidelines, including 'requirements for notices to individuals … intended to give investors information that would help them protect themselves against identity theft'.[231]

In 2011, the SEC published non-binding guidance concerning cyber-security disclosures for publicly listed firms.[232] This said that cyber incidents should be disclosed if:

- they are among the most significant factors making an investment risky
- their associated consequences will lead to a material event or trend that is reasonably likely to affect materially the company's financial condition
- they materially affect a company's services, products, competitive conditions or relationships with suppliers or customers
- they result in material legal proceedings
- they pose a threat to the company's ability to report other required disclosures.

Table 20 lists the disclosures that have been made by financial services firms under the SEC 10-K form for filing of company reports according to the law firm Hunton & Williams.

Table 20 Examples of 10-K filings from US financial services according to SEC guidance (Source: Hunton & Williams)[233]

Company	Notification	Date
Citigroup Inc.	'ha[s] been, and will continue to be, subject to an increasing risk of cyber incidents'	1 Mar 2013
Goldman Sachs Group	'regularly the target of attempted cyber attacks'	
JP Morgan Chase & Co.	'continue[s] to experience significant distributed … attacks from technically sophisticated and well-resourced third parties'	28 Feb 2013
Bank of America Corporation	technologies, systems, networks and [its] customers' devices have been subject to, and are likely to continue to be the target of, cyber attacks, computer viruses, malicious code, phishing attacks or information security breaches'	

While these disclosures are public (compared with the closed notifications envisaged in the proposal for a NIS Directive) they give a flavour of how intervention through stock market regulators can contribute to rebalancing of information asymmetries. However, the guidance is non-binding and was seen more as a mechanism to inform enforcement proceedings in cases trying to determine liability between market operators.[234] To understand how this would work in Europe would require extensive further research into whether the market incentives for firms suing each other would be strong enough (the threat of significant damages being awarded) to lead to listed firms disclosing such incidents to defray the costs of possible litigation.

[231] Securities and Exchange Commission, 2008.
[232] Securities and Exchange Commission Division of Corporation Finance Disclosure Guidance, 2011.
[233] Hunton Security and Privacy Blog Disclosure of Cybersecurity Risks on the Rise, March 2013: http://www.huntonprivacyblog.com/2013/03/articles/disclosure-of-cybersecurity-risks-in-sec-filings-on-the-rise/
[234] Hunton Privacy Blog, October 2011.

6.2.2 Japan

The Japanese government implemented a cyber-security strategy in June 2013.[235] This foresees the free flow of information and the National Cyber Security Information Centre (NISC) to be transformed into a cyber-security centre by March 2016. It replaces the Japanese information security plan from 2012.[236]

As of July 2013, it is not clear whether legislation will be implemented to make the free flow of information between public and private sectors a reality.[237] The strategy is interesting in that it mentions tax breaks for small or mid-size businesses (lower taxes as incentives) so they can invest more in cyber security. The strategy also envisages adding categories to critical infrastructure if cyber attacks on them have a significant impact on the lives of citizens and their socio-economic activities.

6.2.3 Australia

The Australian Cyber Security Strategy was published in 2009, with strategic priorities to: 'improve the detection analysis, mitigation and response to sophisticated cyber threats with a focus on government, critical infrastructure and other systems of national interest'.

CERT Australia will be a national co-ordination point within the Australian government. The Cyber Security Operations Centre (CSOC) will provide the Australian government with all source cyber situation awareness and an enhanced ability to facilitate operational responses to cyber-security events of national importance. CSOC will identify and analyse sophisticated cyber attacks and assist in responses to cyber events across government and critical private sector systems and infrastructure.

The Australian Cyber Security Policy and Co-ordination Committee (CSPC) is an interdepartmental committee that co-ordinates the development of cyber-security policy for the Australian government.

The Australian Cyber Security Strategy shows that the Australian government works through trusted information exchange mechanisms to provide critical infrastructure owner-operators with a better understanding of the cyber-threat environment to build a greater shared understanding of threats and vulnerabilities. Participation in such mechanisms comes under the priority of threat awareness and response:

> *actively participating in and facilitating trusted and timely information sharing within and between government and business, nationally and internationally, to ensure the maintenance of situational awareness and a consistent, global response to online threats.*[238]

The Australian Trusted Information Sharing Network (TISN) is an important element of Australia's critical infrastructure protection (CIP) mechanisms. The TISN has seven major sector groups: banking and finance, communications, food, energy, health, transport and water.

---

[235] NISC, 2012, Cybersecurity, http://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf (Japanese) see here for an English summary: http://www.shield.ne.jp/ssrc/topics/SSRC-ER-13-027-en.html

[236] Japan Information Security Policy Council Report, 2012,: http://www.nisc.go.jp/eng/pdf/is2012_eng.pdf

[237] Matsubara, 2013.

[238] Australian Government, Cyber Security Strategy 2009 http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf

TISN is a forum where owner-operators of critical infrastructure work together sharing information on security issues that affect them. The group's role is to allow critical infrastructure owner-operators to work together and share information on threats, vulnerabilities and appropriate measures and strategies to mitigate risks. Government agencies also participate in these inter-agency advisory groups. Of particular relevance to cyber security is the TISN's communications sector inter-agency advisory group, which brings together telecommunications, international submarine cables, postal and broadcasting owners and operators with the aim of enhancing the resilience of the sector to all hazards, including cyber security.

Engagement with the TISN appears to be expanded to cover integrated best practice approaches to cyber security and critical infrastructure protection. Infrastructure advisory groups in the tisn cover nine sectors:

- banking and finance
- communications
- emergency services
- energy
- the food chain
- health (private)
- water services
- mass gatherings
- transport (aviation, maritime and surface).

The Australian government states it will undertake a range of measures using CERT Australia to strengthen trusted partnerships with the private sector for the sharing of sensitive information on cyber threats, vulnerabilities and consequences (including tailored alerts and advisories and intensive information exchange with high risk sectors to share information on sophisticated threats. These exchanges cover the telecommunications, banking and finance industries, and owners and operators of control systems that underpin national critical infrastructure.

6.2.4 South Korea

In South Korea Presidential Directive No. 141 – The National Cyber Security Management Regulation – appears to remain the main policy instrument.[239] This is supported by the National Intelligence Agency Act and the Regulations on Intelligence and Security Affairs Co-ordination (Presidential Decree No.16211). In 2013 it was understood that the South Korean Senate is considering a new broad law that will encompass many different aspects of cyber security.[240] Presidential Directive No. 141 establishes the National Cyber Security Center (NCSC), the central government point for identifying preventing and responding to cyber attacks. The NCSC sits under the National Intelligence Service. The National Cyber Security Strategy Council sits under the president and is aided by a National Cyber Security Countermeasure Committee (effectively a crisis management committee for addressing cyber attacks).[241]

The Act on Information and Communications Infrastructure Protection enacted in 2008 provides a framework for networks used by critical infrastructure such as military, communications and finance sectors.

[239] Woonyon, 2005.
[240] Anonymous interviewee, 26 July 2013.
[241] January 2008.

The government authority responsible for regulating each sector must form an effective information security policy including vulnerability analysis and assessment. The Information and Communications Infrastructure Protection Committee (which directs government organisations responsible for regulating infrastructure) operates under the auspices of the Prime Minister's office.

The Korean Internet Security Center, a division of the Korean Information Security Agency collects information and detects attacks and performs major network monitoring tasks. Its main focus is on non-critical infrastructure private sector and internet service providers. The Korean Information Security Centre and the Korean Information Security Agency are not government bodies but funded in a PPP model (where they draw revenues from the commercialisation of their expertise).

Table 21 gives some statistics on the cyber-security personnel in the Republic of Korea.

Table 21 Statistics on cyber-security personnel in the Republic of Korea (Source: Anonymous interviewee, 25 July 2013)

Organisation	Mandate	Personnel
Military Information Warfare Centre	Military networks and Infrastructure	10,000
National Cyber Security Centre	Government networks	Classified
Korean Information Security Centre	Private	80
Electronics and Telecommunications Research Institute	Private (R&D)	110

6.2.5 India

In 2011 the Department of Information Technology (DoT) in the Indian Ministry of Communications and Information Technology published a discussion draft of its National Cyber Security Policy: For Secure Computing Environment and Adequate Trust and Confidence in Electronic Transactions.[242] The proposal sets out the strategic perspective, threats, processes of governance and actions from government and the private sector to improve cyber security in India. The proposal reflects on the role of a number of stakeholders including the National Cyber Response Centre, Indian Computer Emergency Response Team CERT-In, the National Information Infrastructure Protection Centre (NIIPC) and the National Information Board (or 'apex organisation'). The National Information Board has particular responsibility for enunciating the national policy on information security and co-ordination on all aspects of information security governance. The proposed National Cyber Security Policy of 2011 includes a number of proposals relating to incident reporting placed as priority: 'creation of necessary situational awareness regarding threats to ict infrastructure' and 'proactive preventative and reactive mitigation actions…including…public private partnership arrangements, information sharing'.

Sectoral CERTs covering 'finance; defence; energy; transportation and telecommunication etc' will be set up to counter cyber attacks affecting critical infrastructure.

[242] Department of Information Technology, India, 2011.

Government and critical sector organisations will periodically report cyber-security incidents to CERT-In as and when they occur. The Crisis Management Plan for Countering Cyber Attacks and Cyber Terrorism is a broad framework for dealing with cyber-related incidents and includes sharing of information on focused attacks that would lead to a national crisis affecting critical sectors (defence, energy, finance, space, telecommunications, transport, public essential services and utilities, law enforcement and security). The types of possible crisis include:

- large scale defacement and semantic attacks on websites
- malicious code attacks
- large scale SPAM attacks
- spoofing
- phishing attacks
- social engineering
- denial of service
- distributed denial of service
- attacks on the domain name system, applications infrastructure and routers
- compound attacks
- high energy radio frequency attacks.

6.3 The difference between incident reporting mechanisms and data breach notification regimes

Aside from security incident reporting, a number of countries are considering or have brought into law specific data breach notification regimes covering the loss of personal data.

It should be noted that a distinct difference in these regimes compared with the provisions in the proposal for a NIS Directive is that they cover *notification* to the affected 'data subjects' whereas the notification regime in the proposal for a NIS Directive only covers *reporting* to competent authorities. The difference in the purpose and breadth of recipients is a fundamental one and should be understood before drawing comparisons. Data breach notification systems such as those in articles 30, 31 and 32 of the 2012 Proposal for a general data protection regulation may be characterised as an open 'public' system whereas the security incident reporting mechanism as envisaged in the proposal for a NIS Directive might be considered a 'closed' private system with annual summaries being produced. Table 22 below compares and analyses the characteristics of security incident reporting mechanisms and data breach notification regimes in current and proposed European regulatory frameworks.

In summer 2013 a majority of US states[243] had passed data breach notification legislation requiring those organisations processing personally identifiable information to notify individuals if their data had been compromised. These laws are very different in each state and differ with the content of the notification (e.g. the threshold for an organisation to notify affected individuals only on suspicion or with definite proof) and on the exempted entities (e.g. in some medical entities are excluded).[244]

[243] Forty-six states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information – National Conference of State Legislatures (see: http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx).

[244] Sophos Naked Security Blog, 9 July 2013.

Data breach notification rules in the US may be thought of as a patchwork with the requirements of the Health Insurance Portability and Accountability Act (HIPAA) and Gramm Leach Bliley Act (financial services) and the US SEC also being relevant. Empirical research from panel data in 2011 suggests that data breach notification laws in the US reduce identity theft by on average 6.1%,[245] but it would be naïve to consider this would also be the case in Europe if the same regime were to be adopted. One of the main drivers for the differences is the possibility of the threat of private litigation by affected consumers, frequently in large scale class actions.[246] Such an identical possibility does not currently exist in the European legal system. Furthermore, there is the different firm demographics of the ratio of listed to unlisted companies to account for.

In 2007 the UK Science and Technology Committee claimed that 'data security breach notification law would be among the most important advances that the UK could make in promoting personal internet security'.[247]

As has been described earlier, personal data breach notification law is a key part of the revisions proposed in 2012 to the European legal framework governing privacy and data protection, namely articles 30, 31 and 32 of the proposals for a general data protection regulation. Table 22 compares and analyses the characteristics of security incident reporting mechanisms and data breach notification regimes in current and proposed European regulatory frameworks.

Table 22 Comparison of security incident reporting mechanisms to data breach notification mechanisms (Source: RAND Europe)

Type of system	Examples	Purpose	Who sends the information?	Who receives the information?
Security incident reporting regime	2008/114 ECI Directive; Article 13a FWD	Gain a better understanding of threats, trends and patterns in incidents	Covered entities (e.g. critical infrastructure)	Competent authorities European Commission ENISA
Data breach notification regime	Proposal for a general data protection regulation (articles 30,31, 32) National data breach notification laws	Inform affected citizens about compromise of their personal data Encourage better stewardship of personal data by data controllers	Data controllers or organisations using personal data	Affected data subjects; regulatory bodies

6.4 Comparison of notification regimes covering losses of personal data in selected jurisdictions

Table 23 summarises and updates research from ENISA published in 2011 and the Privacy Association on data breach notification systems. These systems can operate via guidance or legislative intervention and be mandatory or voluntary.

[245] Romanosky et al., 2011.
[246] ENISA, 2009.
[247] UK House of Lords, 2007.

Table 23 Overview of national level data breach notification systems (Source: ENISA and the Privacy Association)

Country	Date	Instrument	Originator	Binding	Comment
Australia	2013	Guidance on personally identifiable information (PII) security breaches	Australian Privacy Commissioner	No	A new PII breaches bill is pending before Parliament
Germany	2009	Federal Data Protection Act (BDSG) Section 42a	Legislature	Yes	Modelled on US breach notification law
Ireland	2011	Personal Data Security Breach Code of Practice under Section 13 (2) (b) of the Data protection Acts 1988 and 2003	Office of the Data Protection Commissioner	No	
Japan		Guidance	Guidance from Financial Service Agency	No	No specific notification regime in the Japanese Data Protection Law
Mexico	2012	Data Protection Law	Legislature	Yes	
Qatar		Consumer protection law	Legislature	Yes	
Russia		Amendment to data protection law	Legislature	Yes	
Spain	2007	Royal Decree 1720/2007 implementing Organic Law 15/1999 Article 90	Legislature	No	
United Kingdom	2008	Guidance note	Information Commissioner's Office	No	Advised that it should be notified of 'serious' breaches
United States	Since 2002	Legislation	State Legislatures	Yes	

Other countries have implemented similar mechanisms but are not directly comparable to those above since they either concern security incidents or are closed loop reporting systems. For example, in the Chilean Consumer Protection Law, service providers must promptly report 'risks or dangers to the authorities'.

India and the Republic of Korea are two exceptions where more complex incident notification systems have been developed.

In the Republic of Korea, although the framework covers any data security incidents affecting Koreans, there appears to be no requirement for the affected individuals to be informed of such incidents.

Rather, the requirements state that the Korean Information Security Agency or the Korean Communications Commission must be informed immediately with details on the security breach and other relevant information. In this respect it might be considered a hybrid framework, since there is no obligation to inform affected citizens (those in Europe who might be considered data subjects) but the type of breaches that need to be reported to the authorities appear to be those involving personal data.[248]

A second example of the development of more complex incident notification systems is the Indian reporting system for cyber-security incidents. This may be thought of as another type of hybrid regime. In India, intermediaries are required to report certain types of cyber-security incident to the authorities. An intermediary is defined as anyone who:

> *with respect to any particular electronic records […] who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.*

The types of cyber-security incident to be reported are defined as:

> *any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorized access, denial of service or disruption, unauthorized use of a computer resource for processing or storage of information, or changes to data or information without authorization.*

The mandatory notification is thus only to the CERT-In at the national level within the DoT (not to affected individuals). Therefore, in comparison, we might see that this Indian reporting mechanism is the closest comparator to that envisaged in the proposal for a NIS Directive by virtue of the topic of the reports ('any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy') and the closed nature of the reporting (to the national level CERT-In).

Table 24 compares important aspects of security incident and data breach notification regimes across a number of countries.

[248] Wiet and Hengesbaugh, 2012.

Table 24 Security incident and data breach notification regimes in selected third countries (Source: RAND Europe)

	Breaches of personal data	Breaches of online personal data	Security incidents (incl. cyber) on critical infrastructure	Security incidents (incl. cyber) specifically on public tele-communications networks	All types of security incidents
Australia			Informal through TISN		
EU	*2012 proposal for a data protection regulation* Member State laws (e.g. DE)	2002 e-Privacy Directive	2008/114 ECI Directive (energy and transport only) Informal at Member State level (e.g. the Centre for the Protection of the National Infrastructure) and pan-European (EuroSCSIE)	2009 Telecommunications Regulatory Framework	*2013 Proposal for a NIS Directive*
Japan			Informal Jan 2011 Initiative for Cyber Security Information Sharing Partnership Japan (J-CISP) and Council for Advanced Analysis of Cyber Attacks CEPTOR Council	Informal Telecom–ISAC	
South Korea	Personal Information Protection Act (PIPA)		Information and Telecommunication Infrastructure Protection Act	Information and Telecommunication Infrastructure Protection Act	
US	State level PII Breach Notification laws HIPAA Final Notification Rule	State level PII Breach Notification laws	Informal through sector-specific plans (e.g. Defence Industrial Base Pilot) with sector-specific agencies (e.g. DHS) 2013 Executive Order 2013 PPD-21		Informal US SEC Guidance

(Italics indicates regimes in progress).

6.5 Non-regulatory information sharing mechanisms

Aside from national reporting mechanisms listed above there are numerous types of cross cutting or non-policy information exchange and sharing mechanisms. Table 25 lists some of relevance.

Table 25 Examples of non-regulatory information sharing mechanisms (Source: RAND Europe)

Mechanism	Focus	Summary	Examples
Information exchanges	Usually critical infrastructure	Information exchanges are a trusted information sharing mechanism among peers. Threats, incidents and mitigation information is exchanged. Government usually plays a facilitating not chairing role. The agenda is determined by consensus. There is no membership fee.	EuroSCSIE; IEs in the UK; NL
Information sharing and analysis centres	Critical infrastructure	Information sharing and analysis centres (ISACs) are a trusted information exchange mechanism. There can be a membership fee. The secretariat of an ISAC may produce abridged or synthesised reports to the members. There is usually no government involvement.	IT-ISAC[249] in the US; FI-ISAC[250]
WARP[251]	Any community	WARPs are a community based model for like-minded members to receive and share information on threats, vulnerabilities and solutions. Services provided by a WARP can include filtered warnings, advice brokering and reporting.	IE1WARP;[252] LCWARP[253]
Informal technical standards based mechanisms	Technical incident descriptors	Standards based initiatives to permit the rapid and/or autonomous sharing of cyber-security information between different stakeholders.	RfC 5070 Incident Object Description Exchange Format (IODEF)[254] Common Attack Pattern and Enumeration (CAPEC)[255]

[249] Danyliw and Meijer, 2007.
[250] Hafkamp, 2010.
[251] Centre for the Protection of the National Infrastructure, 2013, WARP Directory: http://www.warp.gov.uk/directory.html
[252] Irish Reporting and Information Security Service: http://www.iriss.ie
[253] London Connects WARP; http://www.isfl.org.uk
[254] Danyliw and Meijer, 2007, 'RfC 5070 The Incident Object Description Exchange Format', http://www.ietf.org/rfc/rfc5070.txt
[255] Mitre, 2013, Common Attack Pattern Enumeration and Classification Release 2.1, http://capec.mitre.org/

Vulnerability listings or malware repositories	Security researchers	Grassroots-based technical listings of vulnerabilities or databases of malicious code and exploits.	Bugtraq[256]
Botnet mitigation	Home users	Automated reporting and monitoring of compromised machines on an ISPs network.	Botfrei.de ;[257] ACDC; CyberClean Center[258]

6.6 Approaches in other sectors

It can also be informative to briefly consider approaches to incident reporting in other sectors. In particular we focus on mixed voluntary or mandatory approaches which are increasingly being reviewed as a step forward to mitigate the problems of under-reporting in mandatory systems. Reporting systems are thought to be fundamental in preventing incidents in several domains, in particular those involving complex adaptive systems.

Mixed voluntary or mandatory approaches to address the widespread under-reporting of incidents that characterise many industries despite the presence of mandatory reporting regimes have been successfully adopted in sectors including healthcare and aviation. These sectors offer some useful parallels in the reporting of sentinel events (healthcare) and 'near misses' (aviation).

In the healthcare sector, several jurisdictions have in place systems for the reporting and investigation of 'sentinel events' – events that resulted in death or serious physical or psychological injury to a patient, not related to the patient's illness. However, these reporting systems often face problems of under-reporting of incidents, a problem that will likely surface in any voluntary breach reporting scheme.[259] An empirical study on the Swedish mandatory reporting system for sentinel events, which has been in place for more than 70 years, has suggested that mixed approaches can be more effective in gaining a more complete picture of the incident landscape.[260] In the healthcare sector this portfolio of tools could include incident reporting, medical record review and analysis of patient claims.

The experience gained in aviation safety systems has demonstrated that an accident is usually preceded by weak signals, such as 'near misses' – a term used for situations where incidents arise but adverse consequences do not occur or are prevented.[261] These incident precursors are often not related to the technical or non-technical skills of the operators, but to the overall organisational context surrounding them. Mixed approaches also offer the possibility of including 'near misses' in the scope of the reporting procedure.[262] Furthermore, mixed approaches may often offer better systems to provide incentives for voluntary reporting, maximising confidentiality while maintaining accountability, and emphasise the importance of system-level views in data collection, analysis and improvement.

[256] Security Focus log of vulnerabilities, http://www.securityfocus.com/archive/1
[257] Botfrei Europe website, http://www.Botfrei.de
[258] Japan Cyber Clean Center, https://www.ccc.go.jp/en_ccc/
[259] For instance, the French mandatory data breach reporting scheme has resulted in only 10 reported incidents over the course of its first year of operation (source: CNIL, 2013, CNIL Annual report of activities 2012, http://www.cnil.fr).
[260] Ohrn et al., 2011.
[261] Kessels-Habraken et al., 2010.
[262] Ferroli et al., 2012.

Furthermore, near misses have the advantage of being more numerous than actual grave incidents, thus enabling better data analysis; avoiding legal liability, which is an important barrier to reporting; and offering the possibility to capture and learn from recovery patterns.[263] Such systems require the presence of additional characteristics requiring public policy intervention, which might include provisions for immunity and anonymity of data sources and the availability of rapid and meaningful feedback.[264]

6.7 Conclusions

Within the evidence gathering we were able to conduct for this study, the proposal for a NIS Directive is thus the only regime encompassing a broad security incident reporting mechanism, with the exception of that in India. There are four unique features in the proposal for a NIS Directive compared with the regimes discussed above:

- its inclusion of internet enablers as a sector
- the extension of security incident reporting for cyber-security incidents to critical infrastructure sectors that so far remain generally unaffected by EU critical infrastructure legislation (a small minority from two sectors are defined as ECI under the 2008 ECI Directive)
- its broader understanding of security incidents when considering the types of phenomena to be reported
- most importantly, it has a mandatory reporting nature unlike the voluntary informal or mixed systems in three of our other comparators (US, Japan and Australia) for critical infrastructure and other sectors.

In conclusion, given the unique institutional complexity of the EU, 'like for like' comparisons with national regimes are undoubtedly difficult and so care should be taken with them. The institutional mechanisms of EU policy making are somewhat unique, which makes it difficult to identify best practices from other national contexts that might be fruitful to consider. The learning process therefore could benefit from guidelines to identify best practice. For instance, a recent report published by the multinational Cyber Defence Centre of Excellence in Tallinn proposed three overall strategic factors relevant to cyber-security strategies.[265] These may be useful when considering cyber security at the EU level. These are broadly defined as three characteristics; five mandates and five challenges.

The three characteristics are:

- government
- national
- international.

The five mandates are:

- military cyber
- countering cyber crime
- intelligence and counter-intelligence
- CIP and crisis management
- internet governance and cyber diplomacy.

[263] Barach and Small, 2000.
[264] Idem.
[265] Klimburg, 2012, Chap. 5.

The five challenges are:

- economic growth vs national security
- infrastructure protection vs infrastructure modernisation
- private vs public sector
- data protection vs information sharing
- freedom of expression vs political stability.

Notwithstanding the security orientated context of this report, these characteristics or 'axes of analysis' provide at least a useful framework for analysing how best the proposal for a NIS Directive should be scoped in order to fit with the objectives of the EU Cyber-Security Strategy.

7 WHAT ARE THE POTENTIAL PITFALLS WITH THE PROPOSALS FOR A NIS DIRECTIVE?

KEY FINDINGS

- The proposals for a NIS Directive do not cover the utility of private reporting versus public notification for security incidents, attacks and data breaches clearly.
- There is a vague understanding of the term public–private partnership.
- The centralising effects may cause divergence in implementation.
- There is a risk of regulatory duplication.
- The proposed mandates of CAs and CERTs could encourage a reactive approach to cyber security.
- Additional reporting requirements might lead to fragmentation.
- There is a conservative understanding of current approaches to implementation.
- Little attention is given to other stakeholders that collect and process incident information.
- Multiple reporting mechanisms create additional burdens.
- Obligations fall on those actors (large companies) that are more likely to be doing something already.
- The regulation of internet economy enablers is without precedent.

In the penultimate chapter we present a critique of the proposal for a NIS Directive as a whole, taking into account the previous analysis and described practice from other countries. We find that in some aspects the proposal for a NIS Directive is very ambitious, while paradoxically in others it is rather unambitious.

7.1 Analysis from the Impact Assessment Board (IAB)

The impact assessment accompanying the proposal for a NIS Directive was criticised by the IAB on first submission over its remarks on the version of the impact assessment supporting the proposals of the 13 June 2012. It was originally rejected for four reasons:

- Justification of costs was poorly explained (across a wide range of sectors and Member States).
- There were unclear obligations.
- It was unclear how the preferred option would address the problem.
- Impacts on SMEs and micro entities were poorly elaborated.

On receipt of the revised version, the IAB commented on the impact assessment of 18 October 2012 that the justification for imposing mandatory measures was lacking. The added value of the proposals was not explained (especially in regard to gaps in current measures). The IAB asked the Commission to further justify the proportionality of imposing measures across sectors including SMEs, explain why co-operation between Member States is best achieved by regulatory intervention, and expand the analysis of social and employment considerations, competitiveness, innovation and data protection.

7.2 General considerations

The overall impression from analysis of the proposal for a NIS Directive is that policy-makers have largely rejected the use of soft measures or self-regulation to encourage private co-operation, preferring to devise formal reporting mechanisms.

Information sharing mechanisms although still immature are at least in some areas seen as trusted by private sector participants. The proposal for a NIS Directive suggests that these should be replaced by a structured form of incident reporting without fully clarifying the benefits for business (apart from indicating the expected efficiencies on the part of Member States).

Many of the proposals to tackle cyber security are based on an unclear definition of the supposed root cause of incidents, security breaches or data breaches.

The economic analysis accompanying the Directive uses assumptions on investment in risk management measures to tackle critical infrastructure and data protection as proxies, which when analysed against the nuanced types of incidents appear somewhat weak. This is possibly because there is a strategic need to demonstrate that the administrative burden of the proposals on enterprises will be minimal. However, this has the result that a message is sent to the market that relatively little additional investment in security by firms is required.

At the same time, the fact that the proposal for a NIS Directive assumes a 'gold standard' level of precaution can result in these measures being disproportionately and inefficiently costly for companies, in particular SMEs. The NIS conceptualisation of risk management procedures risks assuming – and therefore imposing – a much higher level of security than would be appropriate or efficient for many SMEs, essentially displacing the liability for the security of all involved parties onto one designated party.

This solution does not appear to take into account aspects such as the distribution of risk aversion, opportunities for diversification, possibilities to allocate risks through contracts and other factors contributing to an efficient allocation of risks.

If this is the case, these requirements could have a number of effects on SMEs. First, the requirement to invest in security could deter SMEs that cannot bear the risk of failure from entering relevant markets. At the same time, if security products constitute a fixed cost, this requirement will also deter the market entry of SMEs that will not have a large enough installed base over which to spread their liabilities and/or the development cost of efficient security measures.

More particularly, owing to the relatively small scale of their systems, SMEs will have to use the kinds of precautions (e.g. security tools) that can be afforded at small scale (and may be less effective and not viable in the market) or will have to outsource protection from managed security service providers or platform providers, e.g. cloud platform providers. Under such conditions, SMEs would have difficulty in abiding by provisions of incident notification envisaged in the proposal for a NIS Directive for reasons discussed in Section 5.4 (for example many cloud computing service providers are based outside the EU and would have difficulty in disaggregating incidents in order to decide what to report).

The former solution (purchasing protection from specialist cyber-security providers) may lead to vertical foreclosure in the Single Market, because the security-as-a-service providers will probably be more concentrated than the SME end-user-service providers. In any case, the security-as-a-service providers will have a different set of risks and incentives to provide adequate services as they will not bear the existential reputational risk facing SMEs.

Purchasing security services from platform providers may also create foreclosure in the market, and allow for a stealth form of discrimination[266] between platform providers and developers of NIS products. This is because it would let platform providers discriminate between large and small or affiliated and unaffiliated NIS providers, eventually operating in a 'lock-in' and ultimately resulting in a less competitive, less resilient and less diverse ecosystem of NIS products and services. .

The definition of standard levels of security might also have effects on innovation: as they have a larger customer base than SMEs (and therefore better ability to recoup security innovation through product bundles), the ability to protect innovation in 'predatory ways' (e.g. through patents) and more robust resilience to reputational damage, large firms might be able to better affront the costs of security innovation.

In contrast, smaller firms would need to generate the innovation and recoup the costs by appearing more reliable and trustworthy to customers who will not be reassured by the benefits of continuity and size. This asymmetry could be particularly discriminating against the most innovative small firms, which would also be more exposed to the combination of risks from innovative new products and risks of failures related to to cyber security.

We now turn to a deeper analysis of some of the potential major pitfalls.

7.3 Uncertainty over public disclosure versus private notification with regard to security incidents and data breaches

A further criticism of the proposals for a NIS Directive concerns the proportionality of the way in which the envisaged incident notification regime links to the objectives. The objective of the Directive does not primarily appear to be to name and shame companies with poor cyber-security practices (as with regimes discussed above in the context of data breaches or SEC guidance) in order to incentivise better security practices. The proposal for a NIS Directive envisages mainly a *private* notification (not disclosure) framework for reporting of security incidents to CAs, which depending on the public interest may then disclose them publicly. The objectives thus appear to focus on obtaining a better picture of trends and encouraging co-operation in incident response. Transparency for the consumer must be thus regarded as a secondary objective (if at all).

However, as has been shown, public notification may have beneficial (albeit short-term[267]) effects on security practices. Given that:

- critical infrastructure owner-operators already have marginally more mature channels to communicate security levels to regulators under the 2008 ECI Directive
- data controllers will have to meet a breach disclosure obligations under articles 30, 31 and 31 of the proposed general data protection regulation

[266] This could also be termed a form of 'non-net neutrality' – a similar argumentation as applies in net-neutrality applying to the provision of cyber security products and services.
[267] For example, Acquisti et al., 2006.

- the types of internet enabling industries noted in the definition of market operators are under limited regulation and hence difficult to regulate.

It would thus appear that the provisions in the NIS Directive constitute additional mechanisms, which might have only limited benefit in contributing toward achievement of the objectives.

7.4 Vague understanding of public–private partnerships

The standard definition of a PPP is where government makes an investment (either in capital or via subsides on revenue in the form of tax breaks, for example) to incentivise the private sector to offer a public service, which normally would not be attractive. It may be observed that despite extensive discussion of the importance of PPPs for cyber security, governments remain reluctant to provide capital investment or revenue subsidies to encourage firms to invest in it. This might be because policy-makers think that the ICT sector is responsible for the problem in the first place and therefore paying out more money to encourage them to fix it is encouraging the wrong behaviour. The proposal for a NIS Directive does not clarify this, discussing PPPs in general terms as a shared responsibility to tackle cyber security. From an industry perspective, this could cause uncertainty, especially with global firms, which might be more familiar with a PPP as an instrument with financial implications.

7.5 Centralising effects may cause divergence in implementation

The proposal for a NIS Directive may be understood as a centralising policy initiative. Little emphasis is given to allocating responsibility to those regulatory bodies closest to the subjects of the regulation that operate the process as we have seen with the different actors in the US (the SEC, Dept of Health and Human Services under HIPAA etc.) according to a common framework that could be organised at EU level. This may be because there is incomplete understanding of who the actors are and how they co-ordinate and co-operate.

There is definitive view of who deals with what with regard to cyber security in Europe. We have provided our overview in Figure 42 but this is no means conclusive and does not explain the nature of connections between the different stakeholders. This may be because there is no single stakeholder with such an overview. It is understood discussions have taken place concerning the appointment of a EU cyber-security czar.

7.6 Regulatory duplication

Many of the market operators discussed operating in already highly regulated sectors (energy, transport, health, finance) may thus find themselves regulated twice – or, in certain sectors that fall under the scope of the ECI Directive, three times.[268] They will have to keep sector regulators appraised of safety and security issues affecting their licence conditions and also report NIS incidents to national level competent authorities. They may thus be on the horns of a dilemma that the broader release of breach data may put them at risk of not meeting their own licence conditions by disclosing incident information to third parties. The existence of other similar organisations to the EFMS is not clear (e.g. in the maritime transport area, the Committee on Maritime Security – MARSEC – operates as a peer group of Member States).

[268] Opinion of the European Central Bank, 13 April 2007.

According to anecdotal evidence,[269] telecommunications regulators were critical in devising reporting standards for Article 13a under EFMS. This was regarded as a key success of EFMS.

The proposal for a NIS Directive does not explain the relationship between its provisions and EFMS peers (assuming they exist) in the different sectors such as transport, healthcare, finance and energy. There is little detail on how these would be engaged assuming (as with the EFMS) that they would play a key role in implementing the notification regime within their respective sectors.

7.7 Proposed mandates of CAs and CERTS encourages a reactive and technical focus

The proposal for a NIS Directive appears primarily designed to guide reaction rather than prevention: the language used links CERTs to CAs in respect of reacting to incidents. Furthermore, CERTs are given a role to run training awareness and education activities, which if followed could result in a overly detailed technical orientation of such campaigns. The NIS Directive provides more detail on expectations of national governmental CERTs than of competent authorities.

7.8 Additional reporting requirements might lead to fragmentation of consideration of risk and poor outcomes for cyber security

Under the proposal, an additional regulatory layer concerning incidents has been established for the NIS. However, big businesses regard many types of incidents as unremarkable, which feeds into an overall risk appetite for the organisation. For example, this is covered in Basel II agreements regarding capital controls and operational risk for financial services. Practice from industry suggests that cyber security therefore should feed into a *whole* view of operational risk. Therefore, asking critical infrastructure industry to separate those operational incidents which materially affect their licence conditions from NIS incidents (which need to reported to competent authorities and then ENISA) could add complexity, further encouraging less reporting since industry might calculate that it is inefficient to de-conflict incident reports compared. The costs of doing nothing (accepting the consequence from an incident) or simply burying them in existing reporting of operational risk are lower than reporting incidents.

Paradoxically, the provisions of the proposal for a NIS Directive may end up undermining chances of succeeding in reaching the very objectives it seeks to achieve. By effectively setting up a system for treating NIS incidents as separate from other types of risk that affect the operational risk profile of critical infrastructure providers (by establishing a mechanism to require separate reporting), the Directive establishes a framework to encourage CEOs and chief information security officers to treat cyber-security incidents not as part of their overall risk appetite but rather as something unique. This might well result in behaviours that shift responsibility further away from the chief executive level of management. This has the outcome that the management of cyber security and incidents is allocated to the IT department rather than being the responsibility of the board. So the regulatory architecture proposed actually works in opposition to the objectives of the Directive (to get NIS on the board level).

[269] Anonymous interviewee.

7.9 Conservative understanding of current approaches to implementing cyber security in SMEs would cause inefficiencies

Many SMEs currently contract out security either willingly or unwillingly from cloud service providers or managed security service providers. Such entities can leverage the power of 'big data' through security incident and event management to help analyse patterns in data and predict trends. The bigger the dataset the more accurate statistical analysis of patterns and possible future trends becomes, allowing more efficient and effective security. Requiring entities that use these services to try and break out incident reports risks causing confusion and fragmentation in this market, potentially hampering the ability of managed security service providers and cloud service providers to carry out analysis. For example, a cloud service provider may suffer an incident that its customers deem 'significant' but it regards as trivial. The proposed NIS Directive is silent on how either cloud service providers or their customers might decide who should report an incident. Furthermore, by the time the notification has been prepared the incident may have been resolved.

7.10 Little attention given to other stakeholders that collect and process incident information on behalf of customers

The proposal for a NIS Directive places little emphasis on those organisations that collect incident information on behalf of customers. Such organisations include managed security service providers and cloud service providers. The data these actors collect would help inform the sorts of trend analysis in the objectives of the Directive. Similarly, the exemption of telecommunications services providers could lead to blind spots in incident reporting because of the imperfect alignment of the legislation applying to different service providers.

7.11 Multiple reporting mechanisms create additional burdens

The proposal for a NIS Directive acknowledges that some companies may face obligations to report under the proposed regime and that of the Data Protection Regulation. The solution is a common template, which would be provided to minimise the burden. However, this does not take account the realities of cyber-security incidents (especially in real time) where because of the difficulty of attribution understanding whether a security incident was motivated by an attacker trying to steal confidential business intellectual property or confidential personal data of customers.

Furthermore additional burden may result in regulated actors making efforts to understand and separate out reporting requirements under (under articles 30, 31 and 32 of the proposed Data Protection; Article 14 of the NIS Directive or Article 8 of the e-Privacy Regulation). This gives industry another reason to limit sharing.

Finally, within the policy architecture (as Chapter 4 shows) there is complexity that could cause uncertainty within Member States charged with implementing the system and those subject to it.

As we have seen, Member States have various ways of formulating policies to deal with incidents and cyber security, and this can lead to significant risk of duplication (e.g. EC3 incident reporting) and obligations under the CIP Directive. There is a further question about capacity and capabilities of Member States to process such incident reports and the question of capacity building in competent authorities has not been covered.

It is also far from clear how co-ordination between data protection authorities and those responsible for cyber security would work in practice. Many data protection authorities take their obligations for independence very seriously and it remains to be seen whether they would actively co-ordinate with competent authorities whose representatives may need to adopt a more collaborative approach with the private sector. For example, in 2013 the level of maturity of co-operative channels between ENISA and Europol remains emergent despite ENISA being established several years ago and there being a high tech crime unit within Europol's Operations Department before the creation of the EC3.

7.12 Obligations fall on those more likely to be doing something already

The provisions of the proposal for a NIS directive may be regarded as unnecessarily disproportionate since they impose costs on organisations most able to bear the costs and report. Most large companies (which are likely to be critical infrastructure providers) are probably already talking to regulators and perhaps already sharing certain types of cyber-security information as part of their obligations toward sector-specific regulators. Furthermore, anecdotal evidence suggests that firms may prefer to talk to regulators off the record; placing specific legal obligations on them would result in the firm taking legal advice. This would have the effect of potentially making the process more efficient and prone to under-reporting since through a process of regulatory compliance, companies would want to make sure all notifications are checked for possible adverse legal implications.

7.13 Regulation of internet economy enablers is without precedent

The proposal for a NIS Directive mentions internet economy enablers, but this sector is presently not very regulated and many such enabling companies are based overseas, specifically in the US. The proposal for a NIS Directive does not address how regulatory purchase might be achieved for this market segment; European legal requirements on notification will probably cause such firms to challenge such requirements against those imposed on them in the country where their headquarters are. Such a debate is being seen now with respect to the EU's proposed data protection regime of 2012. Nonetheless, the proposal for a NIS Directive scarcely discusses the need for a mechanism or forum for internet economy facilitators to share information on promising practices for risk management measures needed to ensure compliance.

7.14 Conclusions

Our limited assessment of the policy interventions in the proposal for a NIS Directive suggests there is a disproportionate interplay between its costs and benefits and other issues. The proposal is unambitious and unbalanced in its focus on the public rather than the private sector (for example failing to acknowledge the role of managed security service providers in collecting incident data) possibly stemming from the perception of the unwillingness of the private sector to address cyber security in the last few years of policy development.

Finally, establishing mandatory reporting while encouraging firms to take up risk analysis in the context of an instrument concerned with incident reporting appears paradoxical because risk analysis for cyber security is highly context dependent and what may be a significant risk for one organisation (thus passing a threshold for notification) could be trivial for another.

8 RECOMMENDATIONS

KEY FINDINGS

- Strive for transparency in the EU policy framework for cyber security.
- Make reporting voluntary rather than mandatory.
- Build up and exploit existing information sharing channels.
- Elaborate what role sector-specific regulators should play.
- Consider the use of guidance as part of stock market listings to encourage good security behaviour by publicly listed firms.
- Formulate a trusted information sharing mechanism for internet enablers.
- Adapt Article 13a to cover critical infrastructure and broaden its scope (to include security incidents other than those that result in outages).
- Engage SMEs though chambers of commerce and grassroots initiatives like WARPs.
- Leverage international practice in implementation guidance.

In this final chapter we present several recommendations aimed at addressing the challenges with the proposal for a NIS Directive as it stands. Like the findings, our recommendations are based on a limited set of data and analysis we were able to perform in the context of this long briefing and conclusions should be drawn with great care. First we list high level substantive recommendations, followed by those relating to sectors and those concerning implementation.

8.1 Strive for transparency in the EU policy framework for cyber security

As Chapter 4 shows, the cyber-security framework at the European level is highly complex with a mix of actors at the macro, meso and micro levels. The idea that this can be simplfiied and radically streamlined is somewhat naïve because there are long standing institutional mandates. Such a streamlining (to create one entity responsible for all cyber-security policy across resilience; cyber crime and national security) would be unrealistic. There is no single accessible overview that captures what the links are between each actor and how these links should and do work. The impact assessment, for example, describes these actors in narrative form but does not adequately reflect the interplay between these different entities and how co-ordination occurs in practice. Creating and maintaining this (using Figure 42 in Chapter 4 as a starting point) would greatly assist in reducing confusion and helping transparency and accessibility. This would be relatively easy to implement.

8.2 Make reporting voluntary rather than mandatory

Overall we recommend that a voluntary rather than required approach be pursued. As has been shown in Chapter 6, many other reporting mechanisms (including those relating to critical infrastructure and complex adaptive systems such as healthcare and aviation) are based on voluntary mechanisms or use a mixture of mandatory and voluntary instruments having regard for the sub-optimal nature of purely mandatory systems. As the objective of the proposal for a NIS Directive appears to be the better understanding of trends and patterns in incidents, the rationale for mandating reporting (as is more common in a public data breach notification regime) is unclear. In the main sectors (critical infrastructure providers and practice from elsewhere) voluntary mechanisms are the norm. The variety of

horizontal mechanisms described in Chapter 6 suggests that an added mandatory reporting mechanism for the covered entities would cause further unnecessary multiplication of the types of mechanism confronting covered entities. This recommendation would involve negotiation on the text of the proposal for a NIS Directive itself.

8.3 Exploit and strengthen existing information sharing channels

Following on from the last recommendation, a more suitable approach to achieve the objectives specified in the Directive may lie in more effectively exploiting *existing* trusted channels for the exchange of security information and data on incidents. Such an approach might take the form of a common internal framework between the different EU-level actors (see Figure 42 in Chapter 4) and Member State level actors (e.g. nationally relevant CERTs and Member critical infrastructure regulators) elaborating a kind of common intelligence collection model, which would define what information was needed but leave the specifics of how that is collected up to the unique conditions of the type of incident (accident, technical failure, natural cause, deliberate attack), sector and Member State. Although such subsidiarity is implied in the choice of legal instrument (a Directive) this only seems to imply vertical flexibility between the provisions of a Directive and its implementation in a Member State. This is not necessary horizontally across sectors or according to the characteristic of the incident. Such a revised approach could well have the benefit of a possible higher quality of information on NIS incidents provided to sector regulators (as companies would be less likely to withhold data on the basis of possible onward legal liability). The European Commission (DG CNECT and ENISA) would be able to develop this recommendation.

8.4 Elaborate a larger role for existing sector-specific regulators

In support of the principle of establishing a regulatory framework where the regulations take effect closest to the regulated, existing sector regulators in the energy, transport, finance and healthcare sectors with responsibility for critical infrastructure would be better placed to receive and process incident information. They should be given the responsibility and made accountable for doing so. The processing and management of such incident notifications could be framed by suitable guidance from ENISA. The benefit of this would be clarity and a potentially reduced administrative burden for firms as they could interact with one regulator. It would also encourage firms to take an all hazards approach to risk as they would need to consider how NIS incidents affect safety and broader provision of security. Similarly, aligning the legislation applicable to telecommunications with the proposal for a NIS Directive could mean that it would either include these actors (effectively withdrawing Article 13a) or maintain the current framework and leave them excluded (but ensure that there is consistency in the types of security incidents reported). This would need to be developed by DG CNECT and other relevant DGs (e.g. DG HOME, DG MOVE) in the European Commission.

8.5 Consider the use of guidance as part of stock market listings to encourage good security behaviour by publicly listed firms

Utilise MS equivalents of the SEC (market regulators for publicly listed firms) such as Consob (IT), LSE (UK), Deutsche Bourse (DE) and so on to guide or require firms seeking public listing to report incidents (that materially affect share price) as part of operational risk. Given most critical infrastructure operators are likely to be publicly owned and listed this might be an effective route to encouraging good cyber-security practices if some kind of public reporting system were envisaged. Such a recommendation would have to be mindful of the changing demography of public firms and differences in company

demography between state owned enterprises (which might be more prevalent in Europe), private firms and family owned conglomerates.[270] This would be beneficial in acting as a incentive for publicly listed firms to improve security practices based on evidence about the impact of breach notification regimes on stock valuations of listed firms. This recommendation would need to be implemented by the European Commission (DG MARKT, DG CNECT) and the European Central Bank.

8.6 Facilitate creation of an informal trusted information sharing mechanism for internet enablers

The logic of including market operators such as internet enabling industries is not clear but if these were to be included, a more proportionate approach would be to try and establish a trusted information exchange mechanism for such a sector along the lines of an information exchange model. This would be beneficial in bringing in internet enablers to the debate especially as the degree of European regulatory purchase over them with regards to security incidents is currently relatively limited. This recommendation should be implemented by ENISA.

8.7 Adapt Article 13a to cover critical infrastructure owners only and broaden its scope to include security incidents not resulting in outages

Given the proportionality of the scale of market operators affected (estimated to be 42,000), a more efficient approach to security might lie in investing and strengthening existing trusted mechanisms with critical infrastructure providers generally, e.g. by allowing access to a secured network (without the legal obligation of reporting), facilitated by the EU. as critical infrastructure companies are likely to be large, multinational firms, they would have the resources to participate. Another approach would be to create legislation which extends Article 13a only to internet enablers, expanding the focus more broadly from incidents resulting in an outage (its current scope under voluntary conditions) and toward all types of incidents (e.g. including security breaches and other types of incident not covered as outages or personal data breaches). This would be beneficial by targeting the intervention and improving the quality of incident reports given the breadth identified in this domain.

8.8 Create an informal trusted information sharing mechanism for public administrations

As we have seen in Chapter 3 with regard to understanding patterns in public administrations, there is little available data on incidents affecting public administration in Member States. As this is popularly defined as a critical infrastructure, this blind spot may be a risk, especially given the extensive e-government initiatives being planned at European level and the measures in the proposal for a NIS Directive to connect competent authorities and CERTs up together in a secured network as described in Chapter 5. As with internet enablers above, we recommend the further investigation of levels of cyber security in public administrations in Member States with the possibility of establishing an informal community of interest as with our recommendation on internet enablers. This recommendation could be implemented by the European Commission and Council.

[270] *The Economist*, 12 March 2012.

8.9 Engage SMEs through Chambers of Commerce and grassroots cyber-security initiatives

To address notoriously difficult to reach SMEs, informal approaches might be taken. One such approach is a grassroots-based model such as a WARP, discussed in Chapter 6. As of 2013 there were 21 active WARPs in existence across public, private and community sectors globally. WARPs might be built up at the same time as links are fostered with cloud computing service providers and managed security service providers. Since these providers collect data on incidents automatically (and most SMEs do not have their own information security programs but contract them as a service from a managed security service provider), they could provide summary insights for regulatory authorities avoiding the need to go via the SME. Chambers of commerce in each Member State, accessed via pan-European bodies such as EUROCHAMBRES, might be engaged to support this activity.[271] The benefits of this would be cost effectiveness and better engagement with SMEs through proxies in which they see value. This recommendation could be implemented by the ENISA and SME representative organisations like EUROCHAMBRES.

8.10 Leverage international practice in implementation guidance for ENISA to take forward for implementation

As has been noted, the proposal for a NIS Directive does not contain implementation guidance and this is welcome. While the obvious candidate for taking forward the details of implementation is ENISA (assuming Article 13a and NISTs cyber-security framework as a parallel), ENISA should aim to provide technology neutral guidance about what measures would be suitable for organisations to adopt to help meet the objectives of the NIS Directive. In line with the proposals, these will need to be suitable for both public and private sectors. ENISA could make use of the NIST Cybersecurity Framework as a possible model to base its guidance on. Ideally ENISA would implement this recommendation.

[271] Chambers of Commerce are useful because they are often provide a platform for SMEs to speak with a collective voice, and share insights and information on common issues. For example see: EuroChambres: http://www.eurochambres.eu/content/default.asp?PageID=29

REFERENCES

- 2013 Cyber attack master index. As of 19 July 2013: http://hackmageddon.com/2013-cyber-attacks-timeline-master-index/

- ACLU (2011). *Opposition to H.R. 3523, the Cyber Intelligence Sharing and Protection Act of 2011*. As of 27 August: https://www.aclu.org/technology-and-liberty/aclu-opposition-hr-3523-cyber-intelligence-sharing-and-protection-act-2011

- Acquisti, A., & Grossklags, J. (May 2003). Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. In *2nd Annual Workshop on Economics and Information Security-WEIS* (Vol. 3).

- Acquisti, A., Friedman, A., and Telang, R., (2006). 'Is there a cost to privacy breaches? An event study', Paper presented at the Fifth Workshop on the Economics of Information Security, *University of Cambridge*, England.

- Alberts, Christopher, Dorofee, Audrey; Killcrece, Georgia; Ruefle, Robin & Zajicek, Mark., (2004). 'Defining Incident Management Processes for CSIRTs: A Work in Progress (CMU/SEI-2004-TR-015)', *Software Engineering Institute, Carnegie Mellon University*. As of 31 July 2013: http://www.sei.cmu.edu/library/abstracts/reports/04tr015.cfm

- Anderson, R. et al., (2012). 'Measuring the Cost of Cybercrime', *WEIS 2012*. As of 19 July: http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

- Anderson, R. and Tyler Moore, (2006). 'The Economics of Information Security', *Science,* Vol. 314 no. 5799 pp. 610-613.

- Article 29 Data Protection Working Party (2011). Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments, 00683/11/EN WP 184

- Australian government, (2010). *Critical Infrastructure Resilience Strategy*. As of 19 July: http://www.tisn.gov.au/Pages/default.aspx

- Barach, P., Small, S. D. (2000). Reporting and preventing medical mishaps: lessons from non-medical near miss reporting systems. *BMJ: British Medical Journal*, 320(7237), 759.

- Bsi Group, (2013). 'Upcoming revision of the ISO/IEC 27001 standard'. As of 31 July 2013: http://www.bsigroup.co.uk/en-GB/iso-27001-information-security/ISOIEC-27001-Revision/

- Böhme, R., (2006). 'A comparison of market approaches to software vulnerability disclosure', In *Emerging Trends in Information and Communication Security*, pp. 298-311. Springer Berlin Heidelberg, 2006.

- Brownlee, N., Guttman. E (1998) *Expectations for Computer Security Incident Response.* June 1998. RFC 2350

- Buncefield Major Incident Investigation Board, (2005). 'The Buncefield Incident, 11 December 2005'. As of 31 July 2013: http://www.buncefieldinvestigation.gov.uk/reports/volume1.pdf

- Campbell, K., L.A., G., Loeb, M. P. and Zhou, L., (2003). 'The economic cost of publicly announced information security breaches: Empircal evidence from the stock market' *Journal of Computer Security*, 11(3), pp 431-438.

- Carter, L., Burnett, D., Drew, S., Marle, G., Hagadorn, L., Bartlett-McNeil, D., and Irvine, N. (2009). Submarine Cables and the Oceans – Connecting the World, *UNEP-WCMC Biodiversity*, Series No. 31. ICPC/UNEP/UNEP-WCMC. As of 19 July 2013: http://www.iscpc.org/publications/ICPC-UNEP_Report.pdf

- Cavusoglu, H., Mishra, B., & Raghunathan, S., (2004). 'The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers', *International Journal of Electronic Commerce*, 9, 70–104.

- Cencini, A., (2005). 'Software Vulnerabilities, a working paper', *University of Washington*. As of 31 July 2013: http://www.cs.washington.edu/education/courses/csep590/05au/whitepaper_turnin/software_vulnerabilities_by_cencini_yu_chan.pdf

- Committee on National Security Systems. (2010). *National Information Assurance Glossary Instruction No. 4009*. As of 31 July 2013: http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

- Connection Management (2013). 'The Visible Effects and Hidden Sources of Internet Latency'. As of 31 July 2013: http://connectionmanagement.org/2013/06/21/the-visible-effects-and-hidden-sources-of-internet-latency

- Council of Europe, (2013). *Convention on Cybercrime,* 23.XI.2001 ETS Treaty series No. 185. As of 19 July 2013: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG

- CSIS (2013). 'Significant Cyber Incidents since 2006', CSIS working paper. As of 21 August: http://csis.org/files/publication/130711_Significant_Cyber_Incidents_Since_2006.pdf

- Danyliw, R. and Meijer, J. (2007). 'RfC 5070: The Incident Object Description Exchange Format'. As of 31 July 2013: http://www.ietf.org/rfc/rfc5070.txt

- Data Protection Working Party, (2012). Opinion 06/2012 on the draft Commission Decision on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC on privacy and electronic communications, 01119/13/EN. As of 31 July 2013: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp197_en.pdf

- Department of Information Technology, India (2011). National Cyber Security Policy draft: 'For secure computing environment and adequate trust & confidence in electronic transactions', New Delhi. As of 31 July 2013: http://deity.gov.in/hindi/sites/upload_files/dithindi/files/ncsp_060411.pdf

- DG Justice & Home Affairs, (2012). 'The new EU agency for management of large-scale IT systems up and running'. As of 31 July 2013: http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2012/20121129_en.htm

- DK CERT (2012). *DK CERT Trendrapport* 2012.

- Electronic Frontier Foundation (2011) 'CISPA Amendments Passed Out of Committee—Here's Why The New Version Still Threatens Online Privacy' Electronic Frontier Foundation Position Paper. As of 27 August: https://www.eff.org/deeplinks/2013/04/cispa-amendment-and-passed-out-committee-heres-why-new-version-still-threatens

- ENISA, (2013a). *Technical Guideline on Incident Reporting*. As of 19 July 2013: https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/technical-guideline-on-incident-reporting-v-2-0

- ENISA, (2013b). Press Release: New Regulation for EU cybersecurity agency ENISA, with new duties. As of 19 July: https://www.enisa.europa.eu/media/press-releases/new-regulation-for-eu-cybersecurity-agency-enisa-with-new-duties

- ENISA (2013c). *Annual Incident Reports 2012, Analysis of Article 13a annual incident reports*, August 2013.

- ENISA (2012a). *Threat Landscape Responding to the Evolving Threat Environment.* As of 29 July 2013: http://www.enisa.europa.eu/activities/risk.../ENISA...download/fullReport

- ENISA, (2012b). *Good Practices in Resilient Internet Interconnection*. As of 19 July 2013: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x/resilience-of-interconnections/report

- ENISA, (2012c). *General Report 2012.* As of 19 July 2013: http://www.enisa.europa.eu/publications/programmes-reports/general-report-2012

- ENISA, (2012d). *Deployment of Baseline Capabilities of National/Governmental CERTs*. As of 31 July 2013: http://www.enisa.europa.eu/activities/cert/support/files/...2012/at.../fullReport

- ENISA, (2012e). *Cyber Incident Reporting in the EU*. As of 19 July: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu

- ENISA (2012f). *Roadmap to provide more proactive and efficient. Computer Emergency. Response Team training.* As of 31 July 2013: http://www.enisa.europa.eu/activities/cert/support/exercise/roadmap-to-provide-more-proactive-and-efficient-cert-training

- ENISA, (2011a). *Annual Incident Report 2011*. As of 19 July 2013: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports

- ENISA, (2011b). *Technical Guideline on Reporting Incidents Guidance on the incident reporting scheme in Article 13a*. As of 19 July 2013: https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/technical-guideline-for-incident-reporting-v1.0

- ENISA, (2009a). *Barriers and Incentives for Information Sharing for Critical Information Infrastructure Protection*. As of 19 July 2013: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/incentives-and-barriers-to-information-sharing

- ENISA (2009b). *Benefits, risks and recommendations for information security.* As of 19 July 2013: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

- Eurobarometer 390, (2012). *Cyber Security Special Report*. As of 19 July: http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf

- European Commission, (2013a). 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, 2013/0027 (COD). As of 19 July 2013: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:EN:PDF

- European Commission, (2013b), Press Release: European Cybercrime Centre (EC3) opens on 11 January, Reference: IP/13/13. As of 19 July 2013: http://europa.eu/rapid/press-release_IP-13-13_en.htm?locale=en

- European Commission, (2012). Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final. As of 19 July 2013: http://www.europarl.europa.eu/document/activities/cont/201305/20130508ATT65776/20130508ATT65776EN.pdf

- European Commission Staff Working Document, (2012). Review of the European Programme for Critical Infrastructure Protection (EPCIP0, SWD(2012) 190 Final. As of 31 July 2013: http://ec.europa.eu/dgs/home-affairs/pdf/policies/crisis_and_terrorism/epcip_swd_2012_190_final.pdf

- European Commission, (2011a). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection 'Achievements And Next Steps: Towards Global Cyber-Security', COM(2011) 163 final. As of 19 July 2013: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52011DC0163:EN:NOT

- European Commission, (2011b). Press Release: Cyber security: EU prepares to set up Computer Emergency Response Team for EU Institutions, Reference: IP/11/694. As of 19 July 2013: http://europa.eu/rapid/press-release_IP-11-694_en.htm

- European Council, (2010). *Internal security strategy for the European Union: Towards a European security model*. As of 31 July 2013: http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313ENC.pdf

- European Council, (2008). Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, 23.12.2008, *Official Journal of the European Union*, L 345/75.

- European Council, (2005). Council Decision 2005/681/JHA of 20 September 2005 establishing the European Police College (CEPOL) and repealing Decision 2000/820/JHA. As of 19 July 2013: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:256:0063:01:EN:HTML

- European Parliament, (2013a). Science and Technology Options Assessment Workshop: Security of e-Government systems. As of 31 July 2013: http://www.europarl.europa.eu/stoa/cms/home/events/workshops/egovernment

- European Parliament, (2013b). Legislative resolution of 4 July 2013 on the proposal for a directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA. As of 31 July 2013: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0321+0+DOC+XML+V0//EN

- European Parliament, Directorate General for Internal Policies, Policy Department A Economic and Scientific Policy, 'The Role of ENISA in Contributing to a Coherent and Enhanced Structure of Network and Information Security in the EU and Internationally', 2011 http://www.europarl.europa.eu/committees/en/itre/studiesdownload.html?languageDocument=EN&file=42251"

- European Parliament & the Council, (2013). Regulation (EU) no 526/2013 of the European Parliament and of the Council concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004. As of 19 July 2013: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF

- European Parliament & the Council, (2012). Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final. As of 31 July 2013: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

- European Parliament & the Council, (2011). Regulation (EU) No 580/2011 of the European Parliament and of the Council amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration. As of 19 July 2013: http://www.enisa.europa.eu/media/news-items/extension-of-enisa2019s-mandate-published-1

- European Parliament & the Council, (2010). Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA. 2010/0273 (COD). As of 19 July: http://ec.europa.eu/dgs/home-affairs/policies/crime/1_en_act_part1_v101.pdf

- European Parliament & the Council, (2009). Directive 2009/140/EC of the European Parliament and of the Council amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services. As of 19 July 2013: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF

- European Parliament & the Council, (2004). Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. As of 19 July: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

- European Parliament & the Council, (2002a). Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services (Framework Directive). As of 19 July 2013: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0033:0033:EN:PDF

- European Parliament & the Council of the European Union, (2002b). Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector as amended by Directive 2006/24/EC and Directive 2009/136/EC. As of 19 July: http://ec.europa.eu/information_society/policy/ecomm/doc/24eprivacy.pdf

- European Parliament & the Council, (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. As of 19 July: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

- Europol, (2013a). Terms of Reference and mandate of the Advisory Group on Financial Services. As of 31 July 2013: https://www.europol.europa.eu/sites/default/files/publications/ec3_-_programme_board_-_tor_-_terms_of_reference_and_mandate_of_the_advisory_group_on_retail_and_financial_services.pdf

- Europol, (2013b). Terms of Reference and mandate of the Advisory Group on Industry Cross-Sector Developments. As of 31 July 2013: https://www.europol.europa.eu/sites/default/files/publications/ec3_-_programme_board_-tor_-_terms_of_reference_and_mandate_of_the_advisory_group_on_industry_cross-sector_developments.pdf

- Europol, (2013c). Terms of Reference and mandate of the Advisory Group on Internet Security. As of 31 July 2013: https://www.europol.europa.eu/sites/default/files/publications/ec3_programme_board_-_tor_-_terms_of_reference_and_mandate_of_the_advisory_group_on_internet_security.pdf

- Eurostat, (2013). Security incidents and consequences. As of 19 July 2013: http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_cisce_ic&lang=en

- Federal Computer Week DHS Hearing, (2010). As of 19 July: http://fcw.com/articles/2010/06/16/web-dhs-cyber-hearing-ig.aspx

- Federal Information Security Amendments Act, (2013). H.R. 1163. As of 31 July 2013: http://www.gop.gov/bill/113/1/hr1163

- Federal Ministry of the Interior, Germany, (2008). Protecting Critical Infrastructures – Risk and Crisis Management: A guide for companies and government authorities. As of 31 July 2013: http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/Leitfaden_Schutz_kritischer_Infrastrukturen_en.pdf?__blob=publicationFile

- Federal Statistical Office of Germany (Destatis). Public service personnel by functional area, 30 June 2012. As of 19 July 2013: https://www.destatis.de/EN/FactsFigures/SocietyState/PublicFinanceTaxes/PublicService/PublicServicePersonnel/Tables/FunctionalArea.html

- Ferroli, P., Caldiroli, D., Acerbi, F., Scholtze, M., Piro, A., Schiariti, M., DiMeco, F. (2012). Application of an aviation model of incident reporting and investigation to the neurosurgical scenario: method and preliminary data. Neurosurgical focus, 33(5), E7.

- Fitsanakis, J., (2011). 'German government admits using Trojan to spy on private computers', Intelnews, 11 October 2011. As of 31 July 2013: http://intelnews.org/2011/10/11/01-842

- Gannes, L., (2008). 'Pakistan Block Accidentally Takes YouTube Down Globally'. As of 31 July 2013: http://gigaom.com/2008/02/24/pakistan-block-accidentally-takes-youtube-down-globally/)

- Gartner Group (22 June 2013). 'Gartner Says Worldwide Security Market to Grow 8.7 Percent in 2013'. As of 31 July 2013: http://www.gartner.com/newsroom/id/2512215

- Gartner Group, (26 April 2012). 'Gartner Says Security Software Market Grew 7.5 Percent in 2011'. As of 31 July 2013: http://www.gartner.com/newsroom/id/1996415

- Gazzetta Ufficiale, (2013). Decreto Del Presidente Del Consiglio Dei Ministri Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, 13A02504GU Serie Generale, n.66 del 19-3-2013

- Greisiger, M., (2012). *Cyber Liability & Data Breach Insurance Claims – A Study of Actual Payouts for Covered Data Breaches' 2nd Edition*: http://www.netdiligence.com/files/CyberClaimsStudy-2012sh.pdf

- Greisiger, M., (2011). *Cyber Liability & Data Breach Insurance Claims – A Study of Actual Payouts for Covered Data Breaches*: http://www.immersionltd.com/Immersion/documents/CyberLiability-0711sh.pdf

- Hafkamp, W. (2010). 'Information Sharing: Does it really work?' Presentation given at ENISA Workshop on Information Exchanges, Amsterdam 17th March 2010. As of 31 July 2013: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2010/information-sharing-workshop/presentations/wim

- Howard, D., Longstaff, J., Longstaff, Thomas A., (1998). 'A Common Language for Computer Security Incidents', *Sandia National Laboratories*. SAND98-8667. As of 19 July 2013: http://prod.sandia.gov/techlib/access-control.cgi/1998/988667.pdf

- House of Lords. Session 2009-2010: European Union Committee – *Fifth Report Protecting Europe against large-scale cyber-attacks*. As of 19 July 2013: http://www.publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/6802.htm

- Hunton Privacy Blog, (October 2011). SEC Issues Disclosure Guidance on Cybersecurity Matters and Cyber Incidents. As of 31 July 2013: http://www.huntonprivacyblog.com/wp-content/uploads/2013/03/sec_issues_disclosure_guidance_on_cybersecurity.pdf

- Irion, C., (2013). *The Governance of Network and Information Security in the European Union: The European Public–Private Partnership for Resilience (EP3R)*. As of 19 July: http://link.springer.com/chapter/10.1007%2F978-1-4471-4763-3_4

- ISO/IEC, (2011). 'Information technology – Security techniques – Information security risk management' ISO/IEC FIDIS 27005:2011. As of 31 July 2013: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=56742

- Jan, J., (2008). 'The Current Situation and Countermeasures to Cybercrime and Cyber-terror in the Republic of Korea', Visiting Papers, *Resource Material Series,* No. 79. As of 31 July 2013: http://www.unafei.or.jp/english/pdf/RS_No79/No79_08VE_Jang1.pdf

- Jensen, T (2008). 'Net-tyvene går amok i Danmark', *ComputerWorld*, 4 April 2008. As of 21 August: http://www.computerworld.dk/art/45162/net-tyvene-gaar-amok-i-danmark

- JP-CERT Co-ordination Center, (2008). Presentation: Organizational internal computer security incident responding structure: CSIRT. As of 31 July 2013: http://www.cicc.or.jp/japanese/kouenkai/pdf_ppt/afit/12_Mr.Keisuke%20Kamata.pdf

- Kessels-Habraken, M., Van der Schaaf, T., De Jonge, J., & Rutte, C. (2010). Defining near misses: Towards a sharpened definition based on empirical data about error handling processes. *Social science & medicine*, 70(9), 1301-1308.

- Klimburg, A. ed (2012) *National Cyber Security Framework Manual* NATO Co-operative Centre of Excellence for Cyber Defence, Tallinn, Estonia Ch 5

- Ko, M., & Dorantes, C. (2006). 'The impact of information security breaches on financial performance of the breached firms: An empirical investigation', *Journal of Information Technology Management*, 17, 13–22.

- Kraft, T., (2012), Presentation given at ENISA http://www.inteco.es/file/9IT5TiusKBJQ7ms3m2eDeA

- Kuner, Christopher, Pateraki, Anna, (2012). 'European Data Protection Law: Breach Notification Requirements – A Global Approach', WSGR. As of 19 July: http://www.wsgr.com/publications/PDFSearch/eye-on-privacy/Nov2012/index.html#1

- Lee, B. Cynthia, Chris Roedel & Elena Silenok, (2001). 'Detection and Characterization of Port Scan Attack', *University of California.* As of 31 July 2013: http://cseweb.ucsd.edu/~clbailey/PortScans.pdf

- Lewis, James A., (2013). 'Raising the Bar for Cybersecurity', *Center for Strategic and International Studies*. As of 19 July: http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf

- Limell, J (2013). 'Facing up to the cyber-espionage battle ahead 3/7/2012', *Public Service Online*. As of 31 July 2013: http://www.publicserviceeurope.com/article/3672/facing-up-to-the-cyber-espionage-battle-ahead

- M. boyd, Danah, N. Ellison., (2008), Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, 13 (2008), pp. 210–230.

- Mandiant Intelligence Center Report, (2012). *APT1: Exposing One of China's Cyber Espionage Units*. As of 19 July 2013: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

- Marcus, S. et al. (2011). *The role of ENISA in contributing to a coherent and enhanced structure of network and information security in the EU and internationally*, Report prepared for the European Parliament. As of 21 August: http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=42251

- Matsubara, M., (2013). 'Japan's New Cybersecurity Strategy: Implications for the Alliance?', As of 31 July 2013: http://www.forbes.com/sites/jonathanmiller/2013/06/13/japans-new-cybersecurity-strategy-implications-for-the-alliance/

- McAfee (2011). Global Energy Cyberattacks: 'Night Dragon'. As of 31 July 2013: http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf

- Microsoft, (2013a). TechNet: Definition of a Security Vulnerability. As of 31 July 2013 : http://technet.microsoft.com/en-us/library/cc751383.aspx

- Microsoft, (2013b). Safety & Security Center. As of 31 July 2013: http://www.microsoft.com/security/resources/botnet-whatis.aspx

- Microsoft, (2012). *Microsoft Security Intelligence Report Volume 14*. As of 19 July: http://www.microsoft.com/security/sir/default.aspx

- Microsoft, (2010). *Microsoft Security Intelligence Report Volume 10*. As of 19 July: http://www.microsoft.com/en-us/download/details.aspx?id=17030

- Mitnick, K. (2000) Testimony before the US Senate Governmental Affairs Committee, March 2, 2000. As of 21 August: http://mitnicksecurity.com/media/SGAC-Testimony-20000302.pdf

- National Council of ISACs, Information sharing and analysis center. As of 19 July 2013: http://www.isaccouncil.org/memberisacs.html

- National Institute of Standards and Technology (NIST), (2013). Cybersecurity Framework Preliminary version. As of 19 July: http://www.nist.gov/itl/cyberframework.cfm

- National Institute of Standards and Technology (NIST), (2012). Computer Security Incident Handling Guide. As of 31 July 2013: http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

- National Institute of Standards and Technology (NIST), (2010). Recommended Security Controls for Federal Information Systems and Organizations. As of 19 July: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

- National Research Council of the National Academies (2003). *The Internet under Crisis Conditions*. The National Academies Press: Washington. As of 19 July: http://www.nap.edu/openbook.php?isbn=0309087023

- National Response Team (2011). 'On Scene Coordinator Report on Deepwater Horizon Oil Spill'. As of 31 July 2013: http://www.uscg.mil/foia/docs/dwh/fosc_dwh_report.pdf

- NCircle, (2006). *Top 10 Tangible Measures for Effective Security Risk Management*. As of 19 July: http://www.ncircle.com/downloads/pdfs/Top_10_Tangible_Measures_for_Effective_Information_Risk_Management-US.pdf

- North American Electric Reliability Corporation (2013). *Glossary of Terms Used in NERC Reliability Standards*. As of 31 July 2013: http://www.nerc.com/files/Glossary_of_Terms.pdf

- NIST 800-61, (2012). Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology.

- Ohrn, A., Elfstrom, J., Liedgren, C., & Rutberg, H. (2011). Reporting of sentinel events in Swedish hospitals: a comparison of severe adverse events reported by patients and providers. Joint Commission Journal on Quality and Patient Safety, 37(11), 495-501.

- Opinion of the European Central Bank, (13 April 2007). Proposal for Council Directive on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection, (CON/2007/11).

- Opinion of the European Data Protection Supervisor on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a 'Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace', and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union. As of 19th July 2013: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-06-14_Cyber_security_EN.pdf

- Opinion of 14 June 2013 on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a 'Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace', and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union. As of 31 July 2013: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-06-14_Cyber_security_EN.pdf

- Organisation for Economic Co-operation and Development (OECD), (2012). *Cybersecurity Policy Making at a Turning Point: Analysing a new generation of national cybersecurity strategies for the Internet Economy*. DSTI/ICCP/REG(2011)12/FINAL. As of 19 July 2013: http://search.oecd.org/officialdocuments/displaydocumentpdf/?cote=dsti/iccp/reg(2011)12/final&doclanguage=en

- Privacy and Information Security law blog, (2013). 'Disclosure of Cyber security risks in SEC filings on the rise'. As of 19 July 2013: http://www.huntonprivacyblog.com/2013/03/articles/disclosure-of-cybersecurity-risks-in-sec-filings-on-the-rise/

- Privacy and Information Security law blog, (2011). 'SEC issues disclosure guidance on cybersecurity matters and cyber incidents'. As of 19 July 2013: http://www.huntonprivacyblog.com/wp-content/uploads/2013/03/sec_issues_disclosure_guidance_on_cybersecurity.pdf

- Pollitt, Christopher and Bouckaert, G, (2011). *Public Management Reform: A Comparative Analysis: New Public Management, Governance and the Neo-Weberian State* (3rd Edition). Oxford University Press. pp 50-51.

- Ponemon Institute, (2013). *2013 Global Cost of a Data Breach*. As of 19 July: https://symantec-corporation.com/servlet/formlink/f?kPugHuQYCDB&ACTIVITYCODE=164216&inid=GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382_aid164216&om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2013Jun_worldwide_CostofaDataBreach

- PwC (2012). *UK Information Security Breaches Survey.* As of 31 July 2013: http://www.pwc.co.uk/audit-assurance/publications/uk-information-security-breaches-survey-results-2012.jhtml

- Richards, K., (2009). 'The Australian business assessment of computer user security: a national survey', *Australian Institute of Criminology*. As of 31 July 2013: http://www.aic.gov.au/documents/3/B/3/%7b3B3117DE-635A-4A0D-B1D3-FB1005D53832%7drpp102.pdf

- Robinson, Neil, (2013). 'Information Sharing for CIP: Between Policy, Theory, and Practice.' In *Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection,* ed. Christopher Laing, Atta Badii and Paul Vickers, 324-351 (2013).

- Robinson, Neil, Luke Gribbon, Veronika Horvath and Kate Robertson, (2013). Cyber-security threat characterisation: A rapid comparative analysis, Santa Monica, CA: RAND Corporation, 2013. As of 19 July 2013: http://www.rand.org/pubs/research_reports/RR235

- Robinson, Neil, Disley, Emma, Potoglou, Dimitris, Reding, Anais, Culley, Deirdre May, Penny, Maryse, Botterman, Maarten, Carpenter, Gwendolyn, Blackman, Colin and Millard, Jeremy, (2012). Feasibility Study for a European Cybercrime Centre, Santa Monica, CA: RAND Corporation, http://www.rand.org/pubs/technical_reports/TR1218

- Robinson, Neil, Lorenzo Valeri, Jonathan Cave, Tony G. Thompson-Starkey, Hans Graux, Sadie Creese and Paul Hopkins, (2011), The Cloud: Understanding the Security, Privacy and Trust Challenges. Santa Monica, CA: RAND Corporation, 2011. As of 19 July 2013: http://www.rand.org/pubs/technical_reports/TR933

- Romanosky, S., Telang, R. and Acquisti, A, (2011) 'Do data breach disclosure laws reduce identity theft?'. *Journal of Policy Analysis and Management*. 30: 256–286.

- Rowe, B., Galagher, M., (2006). Private Sector Cyber Security Investment Strategies: An Empirical Analysis. As of 19 July 2013: http://weis2006.econinfosec.org/docs/18.pdf

- Securities and Exchange Commission, (2011). *Division of Corporation Finance Disclosure Guidance: Topic No.2 Cybersecurity. As of 19 July 2013:* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm
- Sharme, V., (2012). Analysis of Different Vulnerabilities in Auto Teller Machine Transactions, *Journal of Global Research in Computer Science,* Vol 3(3), pp. 38-40.

- Sommer, Peter and Ian Brown, (2011). *Reducing Systemic Cybersecurity Risk*. Organisation for Economic Co-operation and Development (OECD). IFP/WKP/FGS(2011)3. As of 19 July 2013: http://www.oecd.org/gov/risk/46889922.pdf

- Sophos Naked Security Blog, (9th July 2013). As of 31 July 2013: http://nakedsecurity.sophos.com/2013/07/09/some-us-states-strengthen-data-breach-notification-laws-others-ignore-them/

- Susanto, H., Almunawar, M. N., and Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five, *International Journal of Electrical & Computer Sciences IJECS-IJENS* Vol 11 (5) pp 23-29.

- Symantec, (2009). *Symantec Global Internet Security report trends for 2009 Volume XV*. As of 19 July: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf

- Telecompaper, (2013). 'Belgian minister wants more investment in cyber security'. As of 19 July: http://www.telecompaper.com/news/belgian-minister-wants-more-investment-in-cyber-security–938778

- Telang, R., & Wattal, S. (2007). 'An empirical analysis of the impact of software vulnerability announcements on firm stock price', *IEEE Transactions on Software Engineering*, 33, 544–557.

- Tetri, P. and Vuokkinnen, J., (2013). 'Dissecting social engineering', *Behaviour & Information Technology*. As of 31 July 2013: http://www.tandfonline.com/doi/abs/10.1080/0144929X.2013.763860#.UflBG9Iwc-8

- The Department for Business, Innovation and Skills (BIS), *2013 Information Security Breaches Survey*. As of 19 July: http://www.pwc.co.uk/assets/pdf/cyber-security-2013-technical-report.pdf

- The Economist, (2012). 'The big engine that couldn't'. no author named. As of 19 July 2013: http://www.economist.com/node/21555552

- The European Voice, (15 November 2012). 'European Commission Computers Hacked at Web Event' As of 31 July 2013: http://www.europeanvoice.com/article/imported/computers-hacked-at-web-event/75682.aspx

- The Financial Times (20 January 2011). 'Carbon trade cyber-theft hits €30m'. As of 31 July 2013: http://www.ft.com/cms/s/0/cdb788e8-24df-11e0-895d-00144feab49a.html

- The Guardian (25 December 2012). 'Car pollution, noise and accidents 'cost every EU citizen £600 a year'. As of 19 July: http://www.guardian.co.uk/world/2012/dec/25/car-pollution-noise-accidents-eu

- The Guardian (25 November 2011). 'The £650m cyber security blanket'. As of 31 July 2013: http://www.theguardian.com/global/2011/nov/25/governments-650m-cyber-security-blanket

- The Guardian (2011). 'Elderly Georgian Woman cuts off web access to whole of Armenia'. As of 19 July: http://www.guardian.co.uk/world/2011/apr/06/georgian-woman-cuts-web-access

- The New York Times (13 February 2013). 'Obama Order Gives Firms Cyberthreat Information'. As of 19 July: http://www.nytimes.com/2013/02/13/us/executive-order-on-cybersecurity-is-issued.html?_r=0

- The White House, Office of the Press Secretary, (2013). *Executive Order – Improving Critical Infrastructure Cybersecurity*. As of 19 July: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

- UK House of Lords, (2007). Science and Technology Committee, Personal Internet Security, 5th Report of Session 2006–07, HL Paper 165

- US Computer Emergency Readiness Team (US-CERT), (2009). 'Understanding Denial-of-Service Attacks', *Security Tip (ST04-015).* As of 31 July 2013: http://www.us-cert.gov/ncas/tips/ST04-015

- US Department of Defense (DOD), (2012). Fact Sheet: Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance. As of 31 July 2013: http://www.defense.gov/news/d20120511dib.pdf

- Valeri, Lorenzo, Somers, Geert, Robinson, Neil, Graux, Hans, and Dumortier, Jos (2006). Handbook of Legal Procedures of Computer and Network Misuse in EU Countries. Santa Monica, CA: RAND Corporation, 2006. http://www.rand.org/pubs/technical_reports/TR337

- Verizon, (2012). *Data Breach Investigations Report.* As of 19 July: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

- Wiet, F and Hengesbaugh, B (2012). 'International Developments in Data Breach Laws', *Practical Privacy Series*, As of 31 July 2013:

https://www.privacyassociation.org/media/presentations/12PPS-Chicago/4%20%20PPS12_International_Developments.pdf

- Woonyon, K., (2005). Protection of Critical Information Infrastructure in Korea, Presentation given to 13th ASEAN Regional Forum. As of 31 July 2013: http://aseanregionalforum.asean.org/files/Archive/13th/2nd%20ARF%20Seminar%20on%20Cyber%20Terrorism%20Cebu%20City,%20Philippines,%203-5%20October%202005/Annex%20H-Republic%20of%20Korea%20Country%20Report.pdf

- ZDNet, (2002). 'Arsonist Brings down BT network in Manchester'. As of 19 July: http://www.zdnet.com/arsonist-brings-down-bt-network-in-manchester-3040144070

NOTES

EUROPEAN PARLIAMENT

CATALOGUE BA-03-13-454-EN-C

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT A
ECONOMIC AND SCIENTIFIC POLICY

Role

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

Policy Areas

- Economic and Monetary Affairs
- Employment and Social Affairs
- Environment, Public Health and Food Safety
- Industry, Research and Energy
- Internal Market and Consumer Protection

Documents

Visit the European Parliament website: **http://www.europarl.europa.eu/studies**

PHOTO CREDIT: iStock International Inc.

ISBN 978-92-823-4698-3
doi: 10.2861/32110

Publications Office

Data and Security Breaches and Cybersecurity Strategies in the EU and its international counterparts