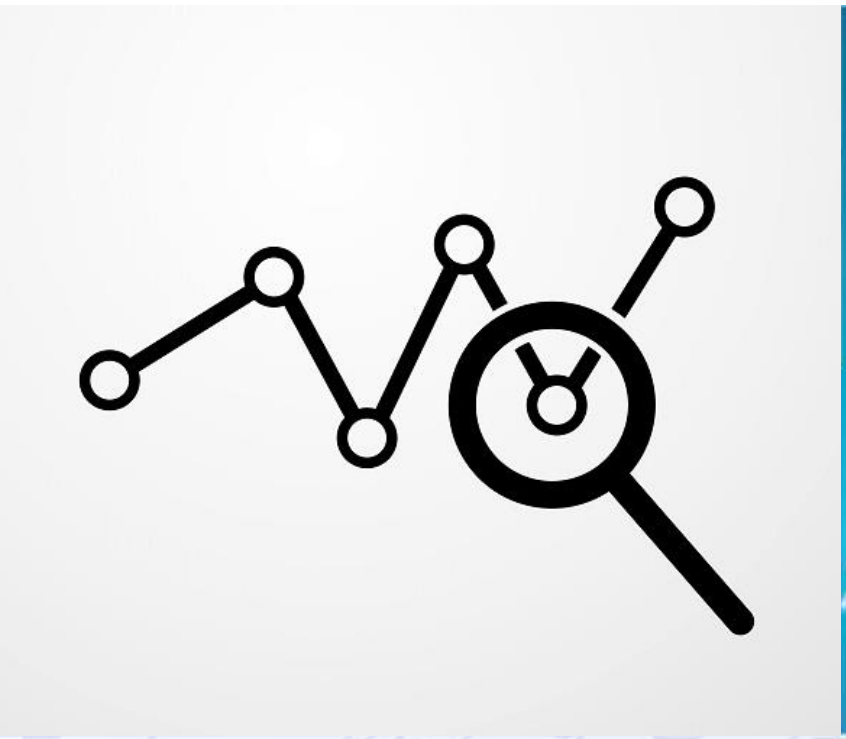


# The cost of incidents affecting CIIs

## Systematic review of studies concerning the economic impact of cyber-security incidents on critical information infrastructures (CII)

AUGUST 2016

# About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

## Authors

Dr. Dan TOFAN (ENISA)
Mr. Theodoros NIKOLAKOPOULOS (ENISA), Ms. Eleni DARRA (ENISA)

## Contact

For contacting the authors please use resilience@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

## Acknowledgements

The analysis in this document was produced in collaboration with EVERIS SPAIN and based on the input of the following experts: Jose VALIENTE ( General Manager and Manager of Coordination and Communication at the Industrial Cybersecurity Centre), Marcos GOMEZ HIDALGO (Operations Deputy Director Spanish National Cybersecurity Institute), Gabriel BASSETT (Senior Information Security Data Scientist Verizon), John MARC SPITLER (Senior Risk Analyst, Verizon), Suzanne WIDUP (Senior Information Security Professional, Verizon).



ISBN: 978-92-9204-173-1 | doi: 10.2824/475621

# Table of Contents

# Executive Summary

Critical Information Infrastructures (CIIs) provide resources upon which several functions of society depend. A potential unavailability of these, would have a debilitating effect on the security, economy and health of society as a whole. Cyber security incidents affecting CIIs are considered nowadays global risks that can have "significant negative impact for several countries or industries within the next 10 years"[1]. As more and more businesses/industries benefit from the advantages of information technology, by witnessing a tighter cyber-physical systems integration, developed under concept like Internet of Things, cyber-attacks or incidents affecting those infrastructures are increasing dramatically, resulting in a new chapter in information security; one that can be called Security of Things. While modern economies rely on the newly developed cyber infrastructures, assuring their security has become the main priority of many actors (governments, companies etc.) as this may have implications for the protection the economies and of business.

A prevalent challenge has been to identify the exact magnitude of incidents in terms of cost required for full recovery, and to determine the national or EU-wide economic impact. The purpose of this document is to take a first step in responding to this challenge, through which we have tried to identify if we currently are able to determine the real impact of incidents and if not what can we do in the future to enable that.

Although there is a plethora of studies addressing the economic impact of incidents, each one of them examines the topic from a different perspective, focusing on certain industries, using different metrics, counting only certain types of incidents etc. The lack of a common approach and criteria for performing such an analysis has allowed the development of rarely comparable standalone studies, often relevant only in a certain context. Despite the lack of relevant studies in EU on this topic, the systematic review undertaken allowed us to identify useful findings for future work in the field, and build an early impression on the current EU and worldwide status.

In this respect, the review revealed that cyber-incidents are a real problem, manifested through a particular set of threats affecting similar types of assets, resulting in financial loss. Among the ***main findings*** are the following:

- ***Finance, ICT and Energy sectors, appear to have the highest incident costs***.
- The most common attack types for Financial sector and ICTs appear to be ***DoS/DDoS and malicious insiders***, with the latter affecting the Public Administration sector as well. It is very important to highlight that these two types on their own, ***collectively constitute approximately half the annualized cost of all cybercrime*** (Figure 9) [16].
- The ***most expensive attacks*** are considered to be insider threats, followed by DDoS and web based attacks [16].
- In terms of ***country loss*** the values provided reach up to 1.6% of GDP in some EU countries [11]. Other studies mention figures like ***425,000 to 20 million euro*** per company per year (Germany) [10]. Another study provides the average cost per company per year that can vary between 2.3 mil. and 15 mil. euro in 2015 [16]. One study also estimates the economic loss for the global economy to be from 330 to 506 billion euro (375 to 575 billion $) [8].
- Data seems to be the ***most affected asset***.

[1] World Economic Forum, The Global Risks Report 2016 - 11th Edition, pg. 11.

Besides the common findings identified above, each study has produced its ***own set of findings***, mostly relevant in their particular context:

- Cybercrime continues to be on the rise, with the cost varying and depending on the organisational size [5][9][16].
- Countries are likely to tolerate malicious activity as long as it stays at acceptable levels, less than 2% of national income [8]; but measuring the exact impact proves to be difficult.
- Business disruption represents the highest external cost, followed by costs associated with information loss [16].
- The urgency to prepare and invest in incident response usually occurs only after an event with a significant impact [2].
- The best data related to cybercrime comes from the financial sector, which is regulated, pays serious attention to cybersecurity, and can easily measure loss [8] being also one of the most targeted industry.
- Companies are in need of qualified personnel, but in some cases they lack completely. Employing under-qualified employees implies a higher risk [1][3].
- Governments need to collect and publish data on cybercrime, and help countries and companies to make better choices about risk and policy [8].
- The most affected CII sectors seem to be financial, ICT and energy.
- A large majority of organisations still have not implemented basic security controls [2].
- Attackers are streamlining and upgrading their techniques, while companies struggle to fight old tactics [15].
- In most cases, attackers are able to compromise an organization within minutes [6][17], while time to recover takes considerably longer [17].
- The large majority of vulnerabilities were exploited one year or more after the vulnerability was revealed; patch management is therefore still one of the weakest links [2][17].

In terms of **conclusions** reached among the most notable one is that the ***measurement of the real impact of incidents in terms of the costs needed for full recovery proved to be quite a challenging task***. Determining cost values that are as close as possible to reality is a key to determining the real economic impact of incidents on EU's economy. Knowing the real impact can help define proper, coherent and cost effective (beneficial) mitigation policies. As a short note, the NIS directive[2] states that "[…] *incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union*", without making any use of figures in support of this. We have also noticed the ***lack of a unified and standardised approach in developing such studies,*** often driven by business factors rather than actual interest of stakeholders or realistic needs.

The importance of the topic along with the gaps identified along our analysis justify the supplying of some **recommendations** specific per type of stakeholder:

- First of all, the development of such studies in the future, should be done throughout a unified analysis, based on a well-structured methodology, and considering all critical variables that define the EU cyber-space. Although there are quite a lot of organisations developing such studies, there is a need for consistent and accurate studies that will reflect as much as possible the real situation. ENISA could be an actor capable of doing such work, but only with suitable resources and a clear mandate in this area.

[2] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

- As regards all types of readers that may be interested in such studies, they would have to place the study in context, prior adopting findings or drawing their own ones. By doing this it is possible to better understand the gaps, or parts uncovered by the study, and better understand the overall findings of the study and their relevance within the actual context. A few details that would assist on this mission are the:
    - number of companies that participated in the study (sample size)
    - geographical area analysed
    - organisations who carried out the study and possible business interests
    - methodology used to extract and collect the data
    - industries affected
    - types of threats / incidents taken into account
- An important category of readers are the ***cyber-security professionals*** (CISOs, security analysts, security engineers, security architects etc.). Beyond understanding the context, they should also focus on extracting useful information for their businesses, such as: major threats, recovery costs, affected industries and assets, best practices etc.
- **Policy makers and corporate management (CEOs and CFOs)** have also something to benefit from these studies in terms of future decision making, policy development, business continuity etc. But again, some filters must be applied to place the study in context and identify the findings that are indeed relevant.
- **Study makers** (organisations that develop such analysis whether being governmental, consultancy companies, cyber-security related companies) can also benefit from this review by improving their frameworks/methodologies, providing more details and transparency on how information was collected and processed, dimension, constituency and representativeness of the sample size, economic sectors covered, types of cyber-threats/incidents covered, challenges identified during the study (that can help understand certain lack of information within the study).

# 1. Introduction

## 1.1 Background

Cyber security incidents (incidents) affecting critical information infrastructures (CII) are considered nowadays global risks that can have "significant negative impact for several countries or industries within the next 10 years"[3]. Critical Information Infrastructures (CIIs) are those systems that provide the resources on which all functions of society depend upon, of which a possible incapacitation or destruction, would have a significant effect on the security, economy and/or health of society as a whole. The more businesses benefit from the advantages of information technology, by entering into the era of the also called cyber-physical Systems, Internet of Things and Internet of Services (Industry 4.0), cyber-incidents affecting those infrastructures have increased more than ever. Modern economies rely on the newly developed cyber infrastructures, and assuring their security has become the main priority of many actors (governments, companies etc.) as this may also be similar with protecting the economies or businesses.

To tackle the new risks, the first logical step to do is probably to develop risk assessments, to better understand the challenges. Nevertheless an important step in developing a risk assessment is to identify the economic impact of such incidents, as they may affect large businesses, economies, and the wider population.

Although there are plenty of studies that address this issue, the development standards of these can differ significantly. The lack of a common methodology and criteria, has allowed the development of a number of standalone studies, rarely comparable among themselves. Although we could not identify economic impact values as defined in our methodology, we could derive findings and trends that can be useful for future work, and can form an early view on the general situation in EU and worldwide. We may say that more or less all studies point a common direction; they indicate that cyber-incidents are a real problem, manifesting themselves through particular types of threats, affecting similar types of assets, and having an economic impact. A challenging task is to identify the magnitude of the impact, in relation to the needed cost for a full recovery, and the economic impact for Europe.

A poignant need occurred for the development of a solid analysis framework that would cover all different aspects of the economic impact of cyber incidents, without merely relying upon interview estimations in quantifying actual costs.

Therefore, considering the above and in the context of the upcoming EU NIS Directive, the need for conducting a systematic review of the literature regarding the proposed theme (the objective of this report), has become even more relevant – so to clarify the current situation and provide a general overview on the methodological aspects, had to be considered when drawing up such a study.

## 1.2 Scope of the document

The aim of the study is to assess the economic impact of incidents that affect CIIs in EU, based on existing work done by different parties, and set the proper ground for the future work of ENISA in this area. In detail, our aim is to:

- Identify relevant studies in the field

[3] World Economic Forum, The Global Risks Report 2016 - 11th Edition, pg. 11.

- Define a proper methodology for reviewing the studies
- Extract relevant findings based on the proposed methodology
- Deliver the results in form of a systematic review.

## 1.3 Target audience

The direct beneficiaries of this work are CII owners and operators, and public authorities within member states (MS) dealing with CII protection – as it will help them understand the magnitude of the impact that cyber-attacks can have on economies, businesses and population. Further to these, the study is also of a benefit to security practitioners (CISOs etc.), corporate leadership (CEOs), and organisations developing studies such as the ones reviewed here (study makers).

## 1.4 Project Methodology

This current review has been developed based on the following approach:

- Base choice of studies based on coherent mandatory and optional criteria, as described in the methodology within Annex I;
- Identify relevant studies (Annex II) – 17 studies identified (6 EU and 11 non-EU);
- Extract key findings of the studies (desktop research and interviews);
- Develop conclusions and recommendations.

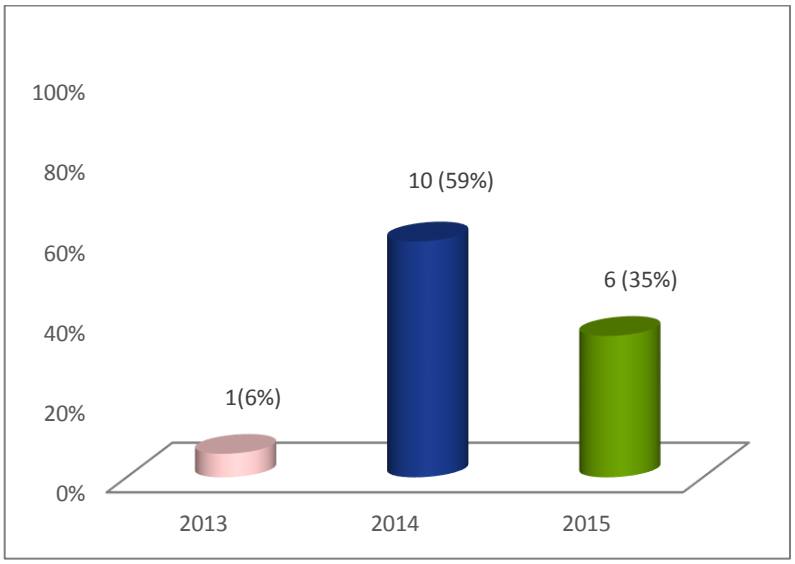
# 2. About the studies analysed

Just a small number of the identified studies have met the defined mandatory criteria. Despite the fact that the primary focus was to locate studies within the EU, this proved quite a challenge since their number is quite low compared to the ones describing the situation with an international focus. The total number of studies that have been taken into consideration for this report was 17, with 6 of them being from the EU, and 11 outside the EU.

## 2.1 Time frame

The timeframe covered by the chosen studies is shown in the figure below (Figure 1). The studies have been covering the calendar year before their publication.

**Figure 1: Data Time Frame**




## 2.2 Data collection (data sources, data selection, data extraction)

Having proper, coherent and accurate data sources is a prerequisite for concrete results. The data extraction method is also important, as the extraction process must enable the identification of meaningful information. The data selection process may assist on improving findings by filtering out any unnecessary information.

### 2.2.1 Data sources

The majority of the studies have engaged experts as the main source of information. The complete set of sources can be found below:

- **EXPERTS**: experts within companies, academia, public institutions, independent experts, or other kind of people that have a connection to the field (**11 studies have followed this approach).**
- **INTERNAL DATA:** used mostly by cyber-security vendors who have the ability to collect data/logs from their clients **(2 studies).**
- **PUBLIC INFORMATION:** publicly available information on incidents (**2 studies).**

- **PARTNERS:** sources such as specialised security companies, CERTs etc. **(2 studies).**

Data sources have been found to be mixed, in the form of internal data and partners, or experts and public information.

Studies that have engaged experts as a source, provide mostly information about countries covered, number of organisations involved and number of incidents studied. The ones that used internal data as a source, provide mostly the number of records analysed (logs), number of countries covered and in some cases the number of partners that have also provided logs. Studies that use public information as a source, provide the number of incidents studied and the geographical coverage (countries).

The number of contributing experts vary between 150 and 2150, depending on the geographical coverage and other factors. The number of organisations covered by the studies are between 24 and 350. A number of studies are also based on data from partners, where the real number of organisations covered cannot be determined. In terms of countries covered the numbers range from 1 to 150. The analysed incidents, are between 140 and 80.000, and some studies mention logs/records analysed with the figure of billions tied to them.

### 2.2.2 Data extraction

The methods utilized for data extraction are the following:

- **Surveys/questionnaires:** are the prevalent tool, mostly in cases where experts were engaged (**11 studies**).
- **LOG/INFO ANALYSIS:** have been used by the specialised security companies that have access to logs and actual cyber-attacks data **(4 studies).**
- **PUBLIC INFORMATION COLLECTION:** public data (media, open sources etc.) is extracted by publishers by different means **(2 studies).**

## 2.3 Geographical coverage

Despite the initial purpose being of analysing the situation at EU level, this turned out to be challenging due to the lack of targeted studies. Although there is a large number of such publications, most of them have an international dimension, and among the ones that are indeed targeting European countries, very few provide all necessary details in order to be considered qualitative. Among the 6 studies covering EU, only 1 has covered all Europe and has results based on only real incidents; with the other 5 covering just regions or countries. The remaining 11 studies, cover other geographic areas (9 international, 1 US, 1 Russia).

Also, an interesting fact is that 14 out of the 17 studies, were carried out by American organisations.

## 2.4 Methodologies used for determining economic impact

Determining the cost of an incident is an essential element, crucial in obtaining a qualitative study. Almost all of the studies that have been taken into account, have based their economic impact determination methodology on the answers they got from the respondents. From the studies, 12 use the surveys as their primary source for costs. There are also 2 other cases, where internal frameworks are used (often based on calculations made by partners/insurance companies) and 3 others that are using public information, or a combination of the methods above.

Regarding the particular techniques to calculate or present the economic data, studies have used different ways to retrieve the incident costs and economic losses:

- **Cost by threat**: calculating the economic losses for a particular threat in a whole country.
- **Cost by country**: calculating the cost for all sectors and for all incidents, and therefore, for the whole country.
- **Cost by sector:** specifying the economic losses for a particular sector (e.g. energy).
- **Cost by region**: calculating the losses for all the sectors and incidents in an entire region.

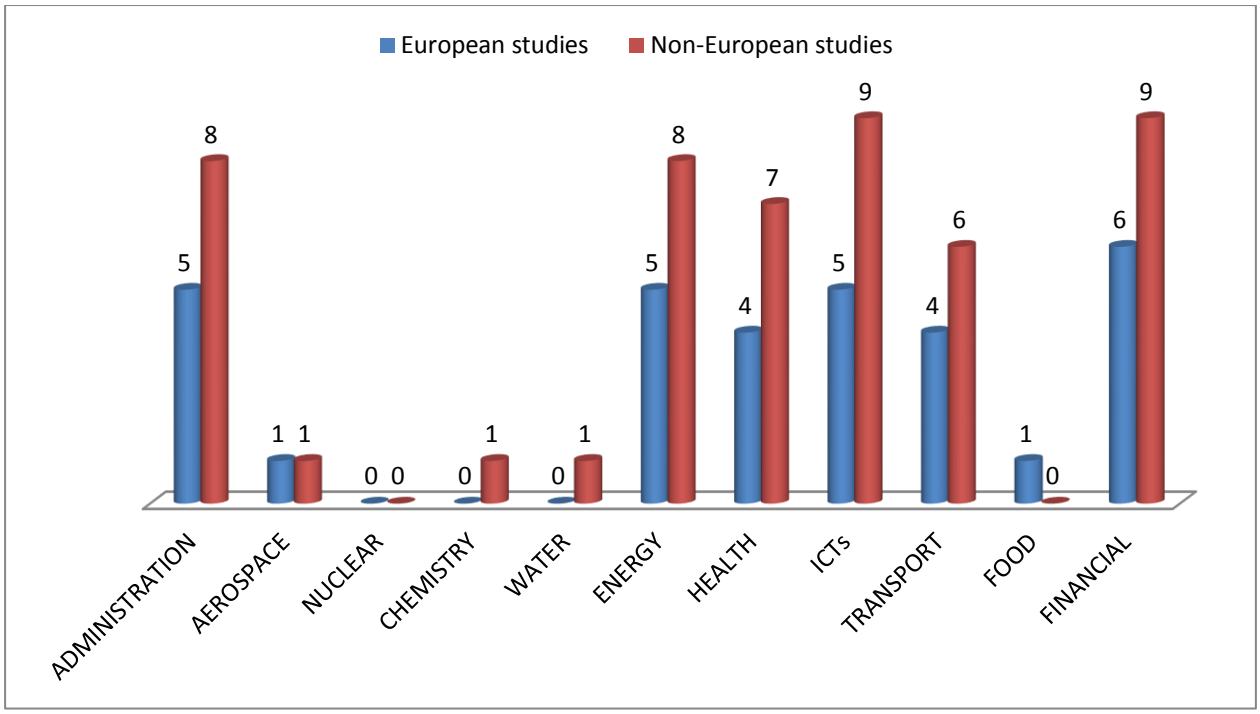
Besides this, some of the studies provide the exact costs and others use the range technique. Chapter 3 includes the findings regarding this.

## 2.5 CII sectors affected

One of the mandatory quality criteria that we have defined within our methodology, was that the studies should address at least one of the CII sectors identified within EU (see Annex I – Methodology description). Out of 12 sectors defined within the methodology, 9 were addressed by the selected studies.

It is worth noting that none of these studies provide economic impact data related to the nuclear sector for example. Conversely, the financial sector is included in 15 out of the 17 studies (Figure 2).

**Figure 2: CII sectors affected**

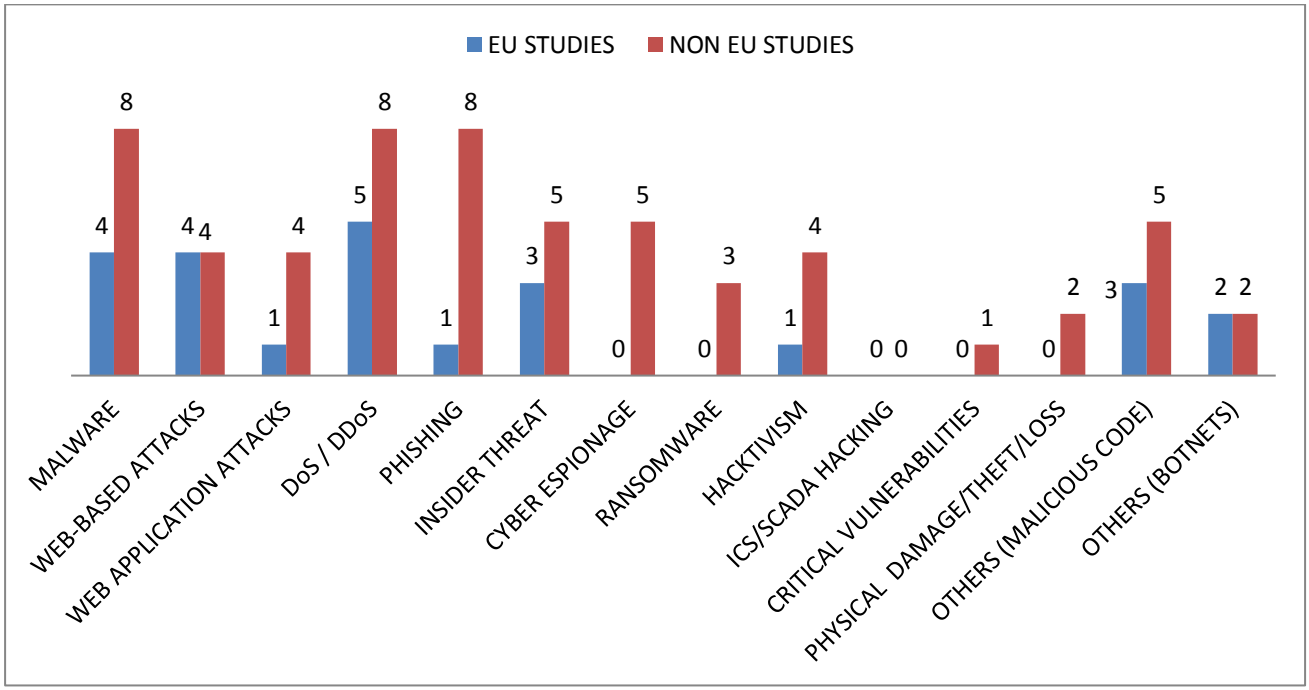


## 2.6 Types of incidents (taxonomy)

A specific incident taxonomy was defined in the methodology so that we can capture studies that contain information about specific types of incidents.

None of the studies provides data related to ICS/SCADA Hacking and Physical Damage/Theft/Loss threats. Conversely, DoS/DDoS is the most common threat, mentioned in 13 out of 17 studies (Figure 3).

**Figure 3: Incident taxonomy**



# 3. Findings based on the content of the studies

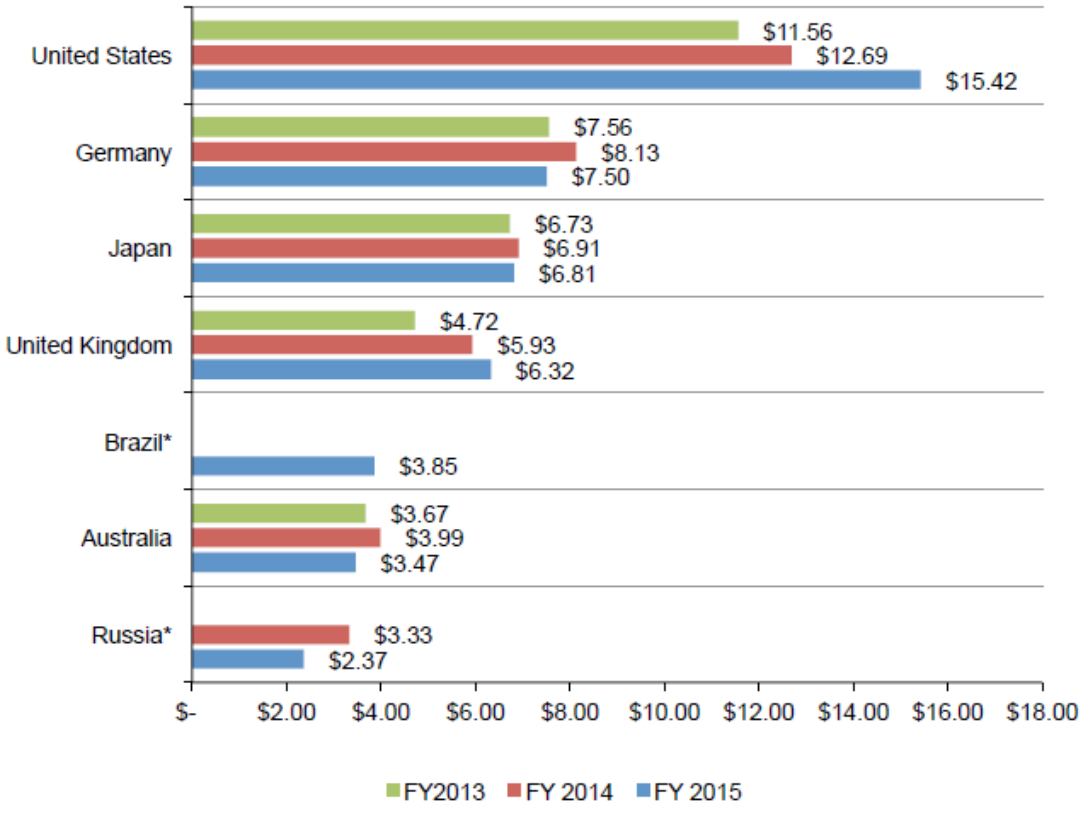
The objective of this section is to analyse in detail the content of the studies, and identify common findings and future trends.

## 3.1 Findings related to the economic impact

After analysing various studies it was found that each study expresses economic impact in a different way. While some studies show annual economic impact per country, other studies provide cost per incident or per organisation. Besides this, some of them use real cost but others use approximations based on different techniques or internal frameworks. On top of that, cost were expressed in different currencies, for which we have converted all figures to a common currency[4]. Given the above, the task of identifying common denominators for those studies becomes almost impossible.

The following table within Ponemon's "*2015 Cost of Cyber Crime Study: Global*" report, summarises the average economic impact of cybercrime per organisation in 7 developed countries worldwide (Figure 4).

**Figure 4: Average economic impact of cybercrime per organisation (millions) [16]**




[4] 1 Pound = 1.3871 €; 1 Dollar = 0.90503 € and 1 Rubble = 0.01422 € Exchange rate date as of 27/10/15

In June 2014 the McAfee study "*Net Losses: Estimating the Global Cost of Cybercrime*" [8] depicts an estimation of the economic impact of cybercrime for some countries, as a GDP percentage. This study finds that the most affected countries are Germany, Netherlands and Norway (Table 1).

**Table 1: Cybercrime as a percent of GDP [8]**

| COUNTRY | % | COUNTRY | % |
|---|---|---|---|
| Germany | 1.60% | United Kingdom | 0.16% |
| Netherlands | 1.50% | Colombia | 0.14% |
| Norway | 0.64% | South Africa | 0.14% |
| United States | 0.64% | Vietnam | 0.13% |
| China | 0.63% | France | 0.11% |
| European Union | 0.41% | United Arab Emirates | 0.11% |
| Singapore | 0.41% | Russia | 0.10% |
| Brazil | 0.32% | New Zealand | 0.09% |
| India | 0.21% | Australia | 0.08% |
| Ireland | 0.20% | Nigeria | 0.08% |
| Zambia | 0.19% | Turkey | 0.07% |
| Malaysia | 0.18% | Italy | 0.04% |
| Canada | 0.17% | Japan | 0.02% |
| Mexico | 0.17% | Kenya | 0.01% |
| Saudi Arabia | 0.17% | | |

### 3.1.1 Overall losses recorded in European Union

UK was the most studied country in EU, as we have identified in 3 studies. According to one study ***UK companies*** losses reach up to ***37 billion euro per year*** (27 billion pounds) [1]. As a comparison, this was approximately the investment of the European Commission in Innovation, Research and Development during a three-year period for the entire H2020 program. Another study underlines that the economic impact can vary between ***1.01 (£544,000) to 26.19 million euro (£14 million) annual cost per company***. Cost from ***104,000 (£75,000) to 4.35 million euro (£3.1 million)*** per affected company are also mentioned [3]. Germany is also in the focus of one of the studies with losses varying from ***425,000 to 20 million euro*** per company per year [10]. France is also affected by losses from ***445,000 to 18,9 million euro*** economic impact per company per year [11].

### 3.1.2 Overall losses recorded by international studies

Among the international studies, 8 examine the worldwide situation, with 1 of them focusing on the United States [14], and 1 more on the Russian Federation [12]. The majority of the studies provide an estimated economic loss range. However, some of them detail data for specific threats, and global economic impact on specific sectors or countries.

The most comprehensive estimation regarding economic loss is presented in the McAfee study [8]. Estimated economic loss for the global economy varies from 330 to 506 billion euro (375 to 575 billion $), with focus on three different types of attacks: hacktivism, malware and cyber espionage.

The study "*Energy Market Review"* by Willis Limited [13] focused only on the energy sector, and presents an impressive highlight about the economic losses: around 545 million euro (400 million GBP) in the United Kingdom's energy sector. Globally, it is estimated that cyber-attacks against oil and gas infrastructures will cost 1.69 billion euro (1.87 billion $) by 2018.

Another report [5] offers a range estimation for economic loss for 257 companies worldwide. The lowest cost for a company would be 0.45 million euro (0.56 million $), and the highest loss 55.2 million euro (61 million $).

The study *2015 Data Breach Investigations Report [7],* by Verizon, shows a different approach to the economic loss estimation. They introduce the term "record" to refer to a set of valuable information and it builds the economic loss based on the number of records compromised plus other relevant aspects ("multiple contributing factors"). This report presents a range of economic impacts depending on the number of records compromised, with the lowest average impact of 16.400 euro (18.120 $) for 100 records and the highest average impact of 14.1 million euro (15.6 million $) for 100 million records. The most sectors affected are Public Administration, Finance, Health and ICTs.

The study *2015 Internet Security Threat Report [15],* by Symantec, shows the value of stolen data in the black market. Symantec affirms that there are 317 million new malware variants being sold in the black market and used to steal information. Information – such as e-mails, credit cards, and passport copies – is sold in the black market, with the price varying from 0.45 euro cent (0.50 $) to 3,168 euro (3,500 $).

The study *2013 Cost of Cyber Crime Study: United States [14]* by Ponemon, shows that the average annualised cost of cybercrime for 60 US-based organisations is 10.4 million euro (11.6 million $) per year, with a range from 1.7 to 52 million euro (1.3 to 58 million $). In the previous year, the average annualised cost had been 8 million euro. This represents an increase of 26%, or 2.3 million euro (2.6 million $).

The average annualised cost for 24 Russian organisations is 1.7 million euro (120.2 million rubbles) per year, with a range from 334,000 euro (25 million rubbles) to 6.3 million euro (442 million rubbles) per company each year [12].

## 3.2 Findings related to CII sectors

For performing the current review, we have taken into consideration certain types of critical information infrastructures (CII) that exist in the context of the EU legislation – making their presence mandatory.

### 3.2.1 Most affected CII sectors

The following figure, shows the affected sectors in Europe, as reported by the European studies.

**Figure 5: CII sectors affected (same as 2)**

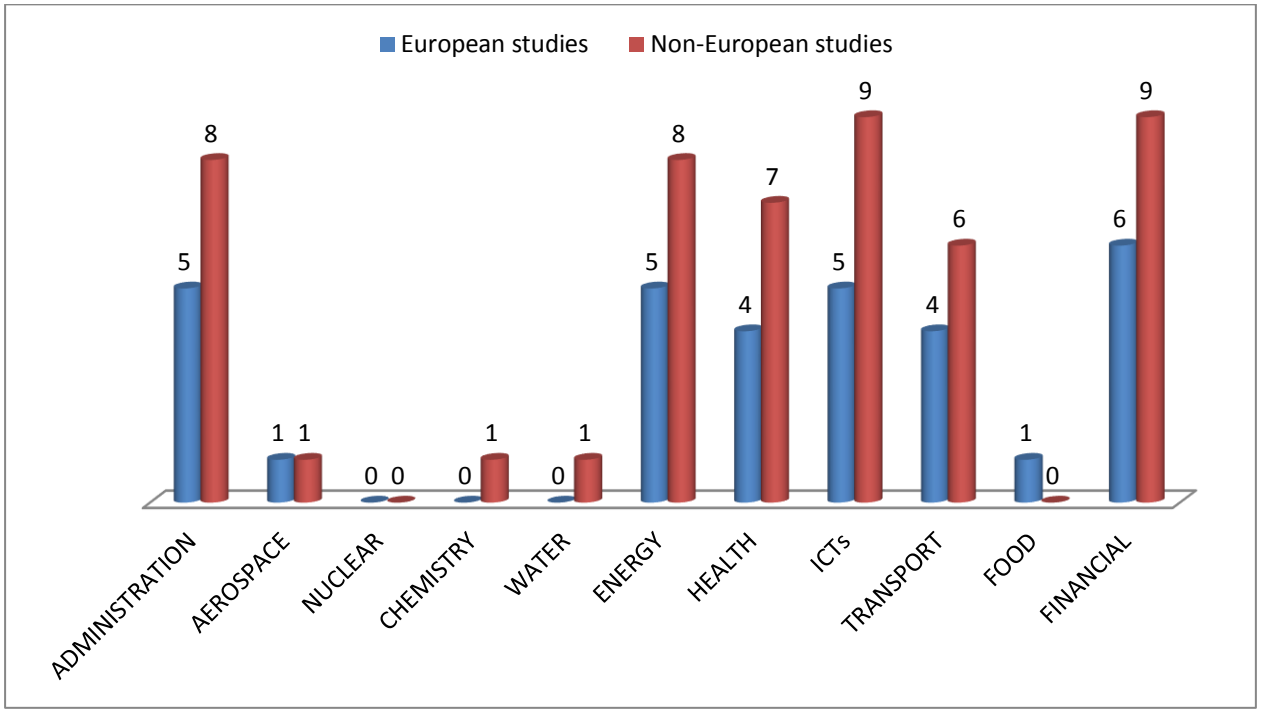


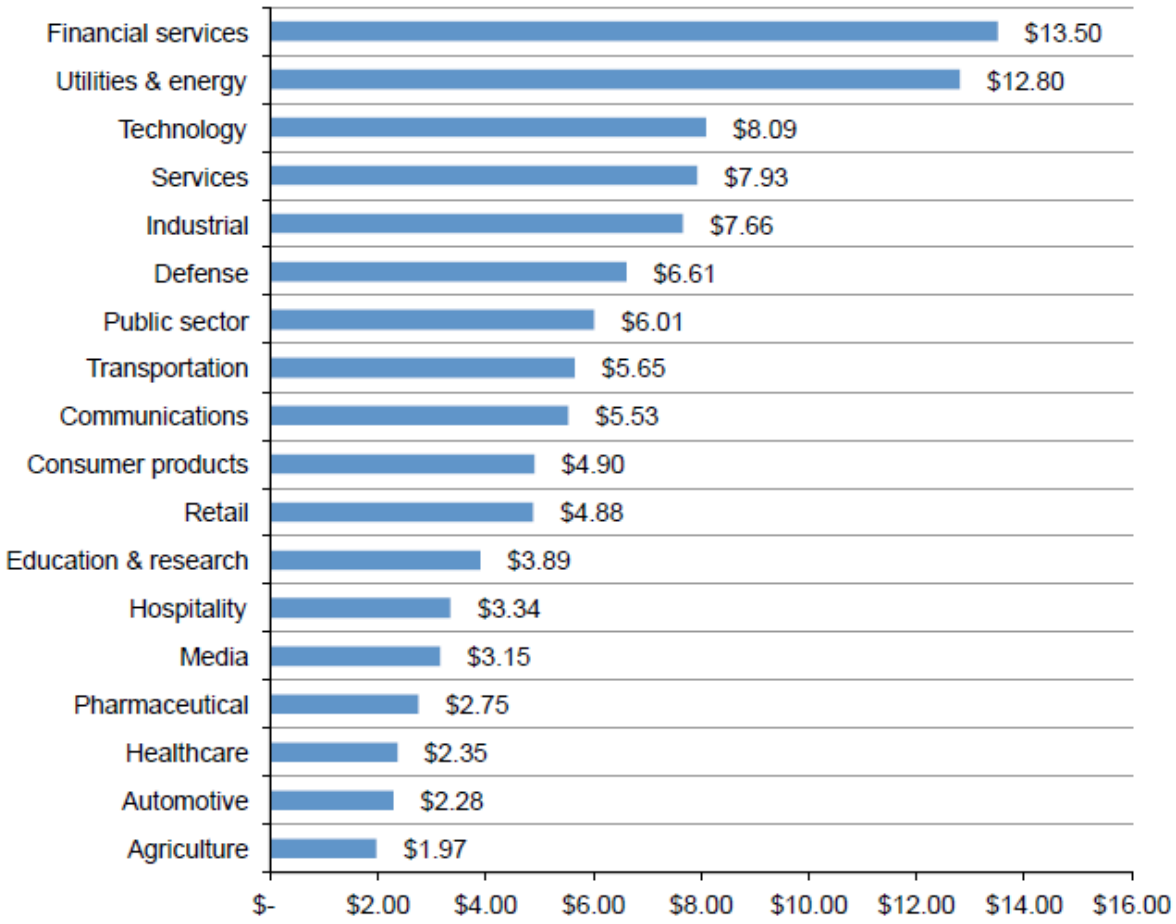

Figure 5 shows the number of studies that covered each specific sector. The financial sector seems to be the most examined, by being mentioned in 14 studies (2 were sector specific), followed by ICT and Energy. Other affected sectors are: Public Administration, Health and Transport.

The sectors with rather poor coverage within the studies are: Aerospace, Nuclear, Chemistry, Research and Development, and Water.

### 3.2.2 Overall losses per CII sector

The Ponemon's "*2015 Cost of Cyber Crime Study: Global*" [16] gives us an average annualized cost by industry sector from 252 companies worldwide (Figure 6).

**Figure 6: Average annualized cost by industry sector (millions) [16]**




The data shows that financial services and energy related sectors suffered the strongest economic impact due to cybercrime.

Another study oriented towards one specific sector, "*Energy market review" [13]*, by Willis Limited have found that UK economic loss in the energy sector for 2014, was 545 million euro (400 million GBP).

The Ponemon "*2015 Cost of Data Breach Study: Global Analysis" [6]* have examined the worldwide cost per capita in different sectors in 2015, and concluded that the average cost is approximately *154 $.* The study covers only data breaches, and it has found that heavily regulated areas have a substantially higher per capita data breach cost, than less regulated or no regulated areas.

The Ponemon "*2014 Cost of Cyber Crime Study: Germany" [10]*, shows the average annualised cost by industry sector in Germany, comparing data from three different fiscal years. Financial services and utilities & energy experience higher costs in all three annual studies. In addition, the education & research and public

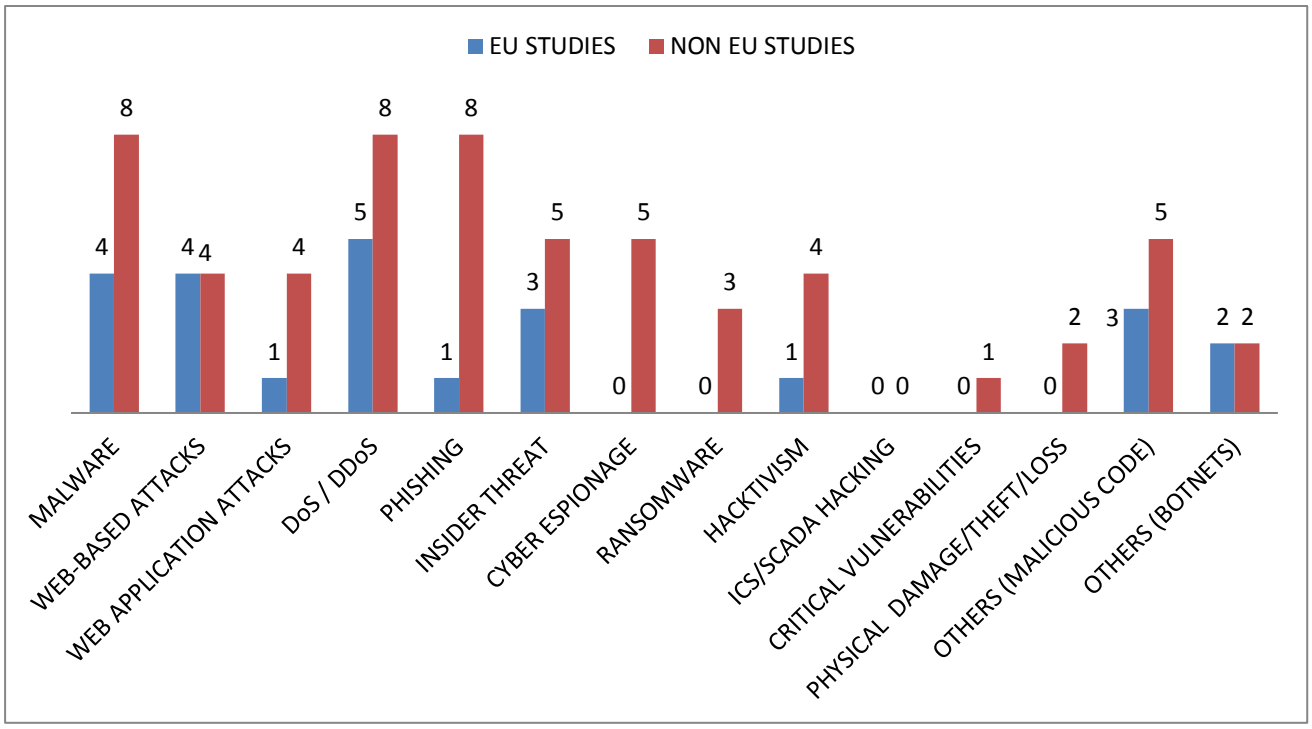
sectors have experienced a significant cost increase in the last year. On the other hand organisations in hospitality, media and retail appear to have a lower overall economic impact over the last three years (2012-2014).

## 3.3 Findings related to incident types

This section describes the overall common incident types, the specific incidents per sector, and an average cost per incident type. In most cases the incident types can be considered as threats.

### 3.3.1 Overall common threat

**Figure 7: Threats identified within the studies (same as Fig. 3)**




DoS/DDoS seems to be the most common type of threat, mentioned in 13 out of 17 studies. The second most frequent threats are: Malware (12), Insider threat (8), Phishing (9), Web-based attacks (8), and cyber-espionage (5) (Figure 7).

Surprisingly the studies do not contain information about ICS/SCADA, although it has been in the public focus in the last years. Physical damage/theft/loss has also recorder 0 references within the studies.

### 3.3.2 Specific threat per CII sector

Within this section incident types are mapped to CII sectors, visualising the specific threats reported per sector (Table 2).

**Figure 8: Attack/Threat types per CII sector (graphical view of Table 2)**

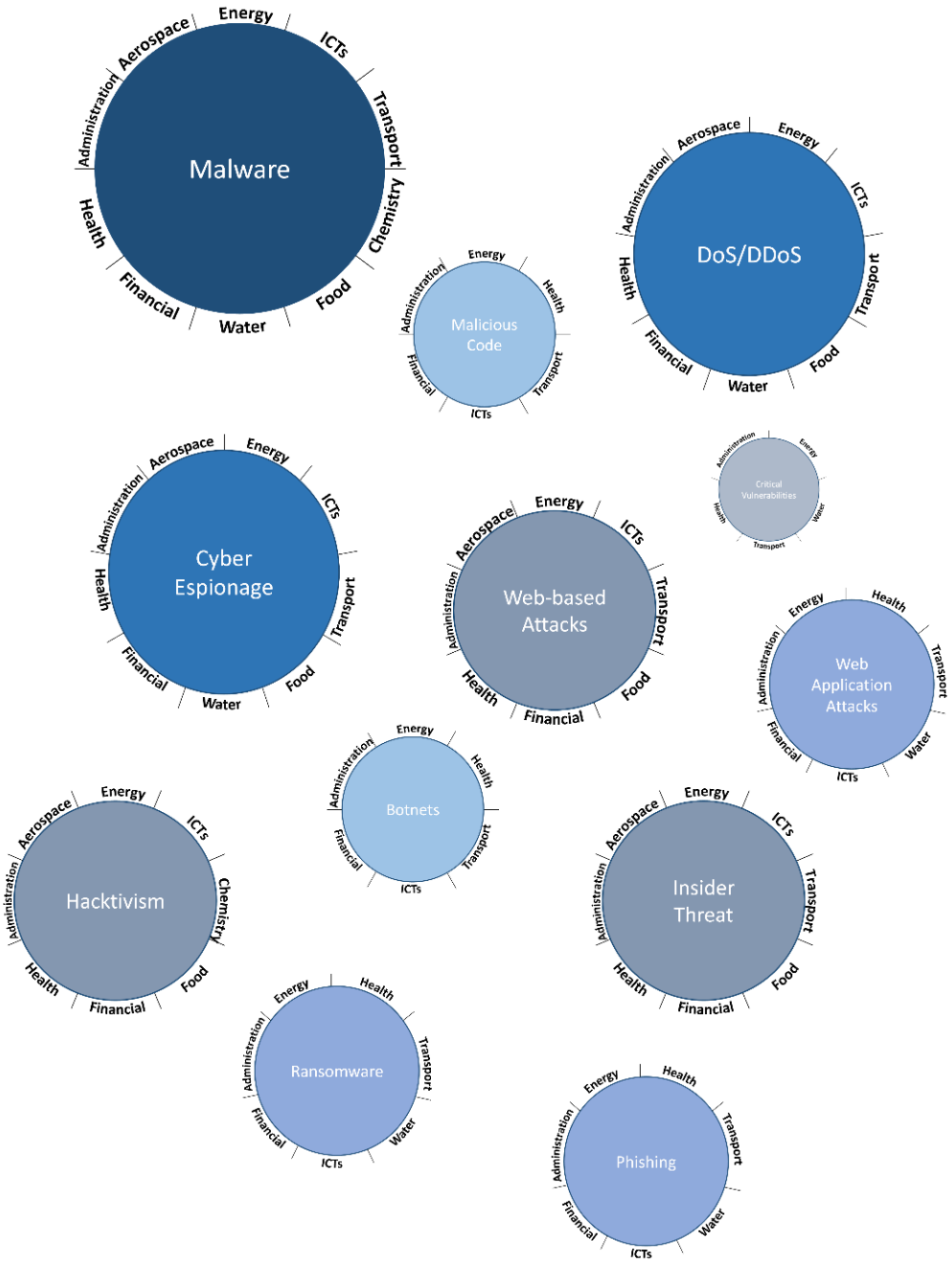


**Table 2: Attack/Threat types per CII sector**

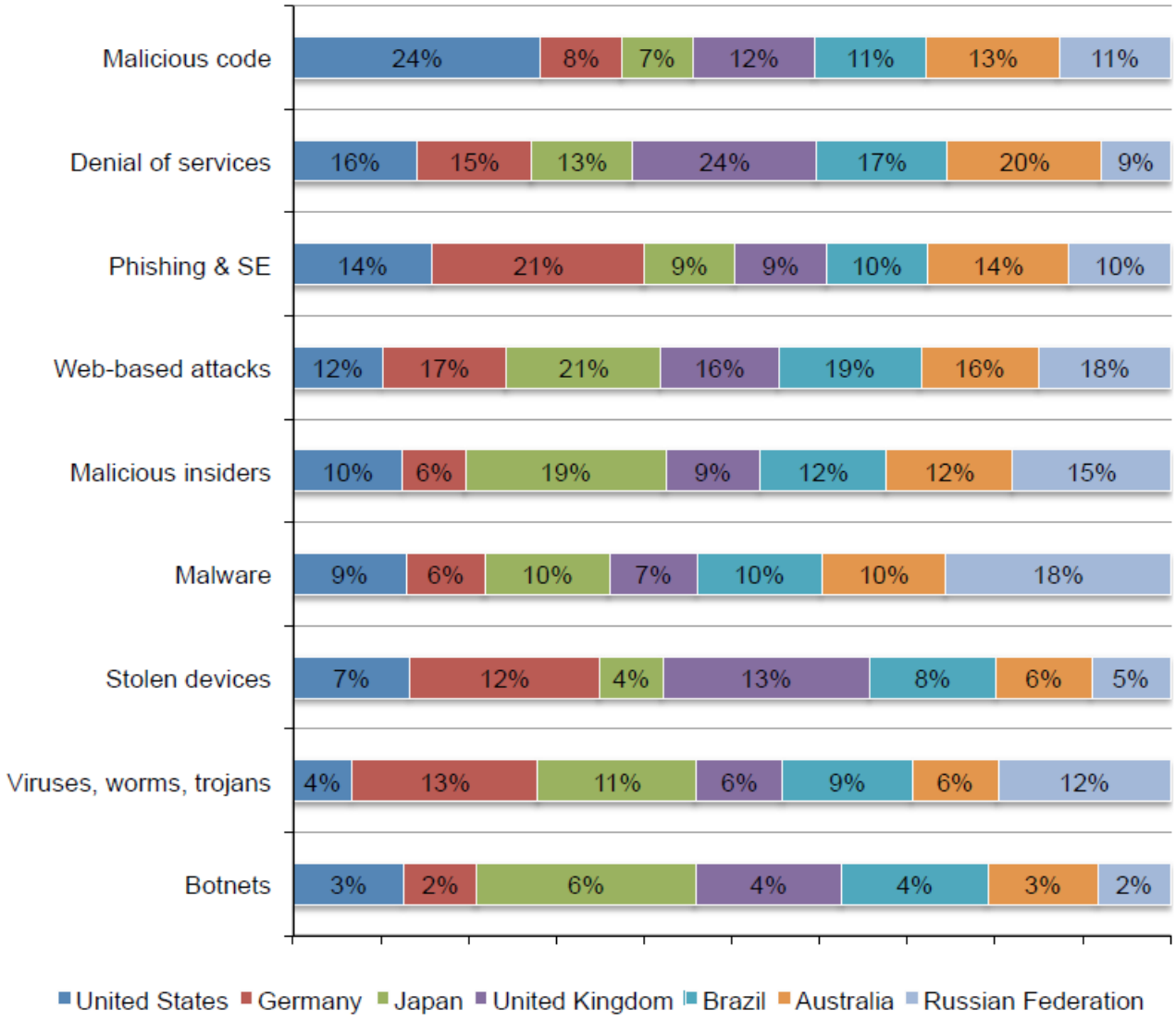
| | | Number of studies per sector | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Nr. | Attack / Threat | Public Administration | Energy | Health | Financial | ICTs | Transport | Water | Aerospace | Food | Chemistry |
| 1 | Malware | 7 | 10 | 7 | 9 | 9 | 7 | 1 | 1 | 1 | 1 |
| 2 | DoS/DDoS | 10 | 8 | 8 | 11 | 11 | 8 | 1 | 1 | 1 | – |
| 3 | Cyber Espionage | 2 | 3 | 3 | 3 | 2 | 1 | 1 | 1 | – | 1 |
| 4 | Web-Based Attacks | 5 | 7 | 4 | 7 | 7 | 6 | – | 1 | 1 | – |
| 5 | Insider Threat | 7 | 4 | 6 | 8 | 7 | 3 | – | 1 | 1 | – |
| 6 | Hacktivism | 3 | 3 | 3 | 5 | 4 | – | – | 1 | 1 | 1 |
| 7 | Malicious Code | 5 | 6 | 5 | 7 | 7 | 6 | – | – | – | – |
| 8 | Phishing | 6 | 4 | 4 | 6 | 6 | 4 | 1 | – | – | – |
| 9 | Web Application Attacks | 5 | 2 | 4 | 4 | 4 | 2 | 1 | – | – | – |
| 10 | Ransomware | 3 | 1 | 3 | 2 | 2 | 1 | 1 | – | – | – |
| 11 | Botnets | 1 | 2 | 2 | 2 | 2 | 2 | – | – | – | – |
| 12 | Critical Vulnerabilities | 1 | 1 | 1 | – | – | 1 | 1 | – | – | – |

### 3.3.3 Average cost per threat type

To identify the incidents having the greatest financial impact that may affect an organization, it is necessary to calculate the average cost per threat. It is imperative to understand that the economic impact is highly associated to the industry type of each company; information that was difficult to source, since most studies would not provide this. An exception to this rule is Ponemon's "*2015 Cost of Cyber Crime Study: Global*" [16], that has covered this area.

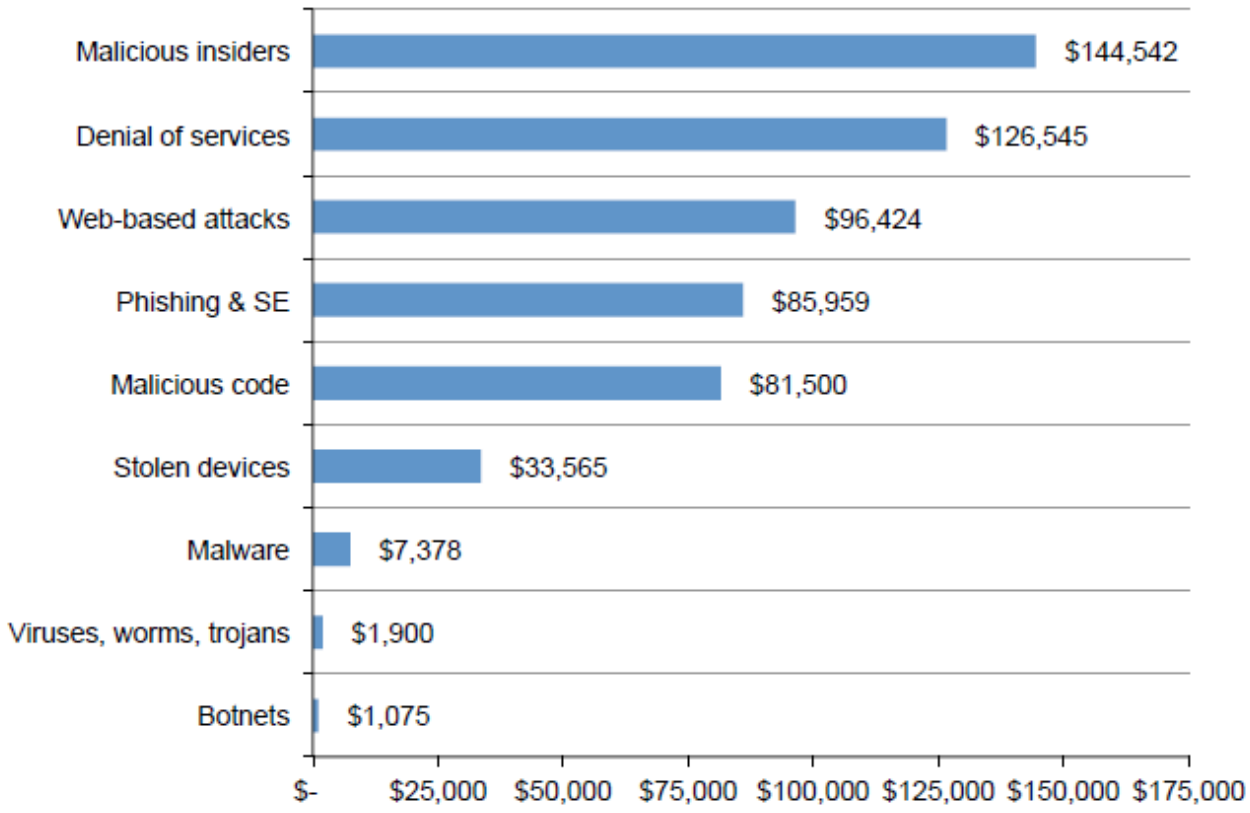
The following figure shows the percentages of annualized cybercrime cost by attack type, across several countries (Figure 8).

Figure 8: Percentage of annualized cybercrime cost, by attack type [16]




The same study also gives an overview on the worldwide average annual cost of attacks, weighted by attack frequency (Figure 9).

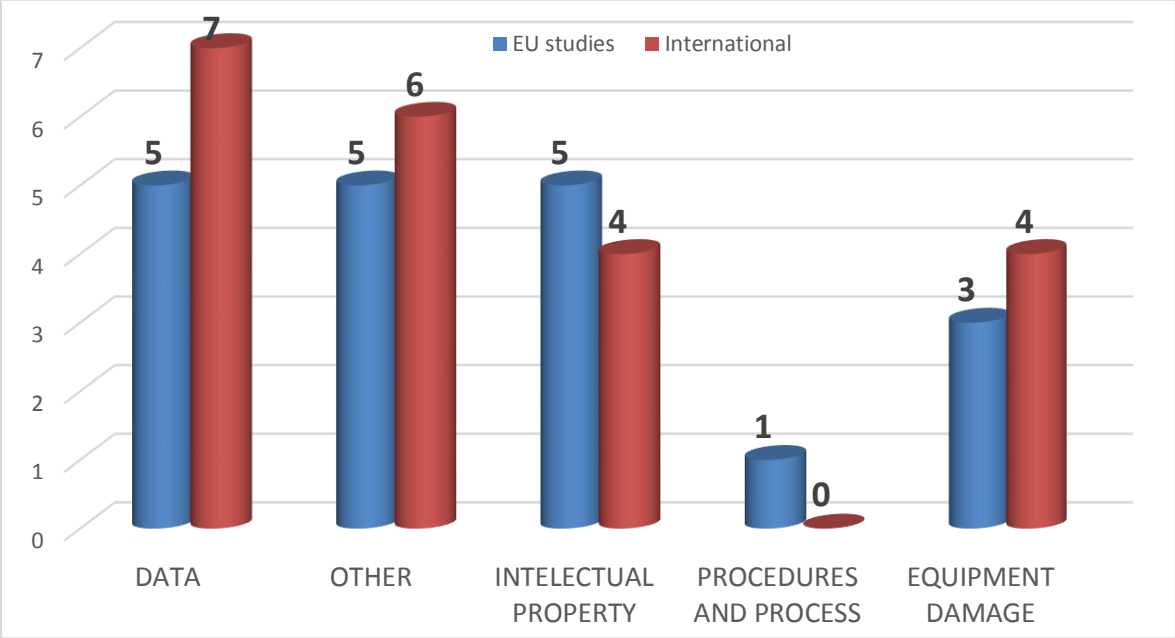
Figure 9: Percentage annualized cybercrime cost, by attack type [16]



## 3.4 Findings related to affected assets

There was an effort to identify assets that are affected by incidents, which again was a challenge, considering that not all studies provided such information (Figure 10).

**Figure 10: Assets affected**




Data appears to be the most affected asset; where data may mean any kind of information, e.g. confidential information, personal identifiable data, logs and other types. Data is usually considered one of the most important assets of a company, so this finding is not surprising. Another affected asset category seems to be intellectual property, which can be considered also data in some circumstances. Equipment was also found to be affected in 6 of the analysed studies. Of course there could be more asset types within an organisation, but those were the only ones mentioned within the studies.

## 3.5 Conclusions from the studies

Based on the overall findings and the prospective audience, most of the studies have developed a number of conclusions. Below is a grouped summary of these conclusions, some of them taken "as is" from the studies analysed.

**Economic**

- The highest economic impact is produced by malicious insiders, denial of services and web-based attacks.
- Cybercrime continues to be on the rise for organisations, with the cost varying and being depended to the organisational size [5][9][16].
- Cost of cybercrime can reach values as high as 15 mil. euro per organisation/year, or 1.6% of the GDP for some countries [16].
- Countries will tolerate malicious activity as long as it stays at acceptable levels, less than 2% of national income [8].

- Business disruption represents the highest external cost, followed by the costs associated with information loss [16].
- Cybercrime slows down the pace of global innovation by reducing the rate of return to innovators and investors [8]. Those types of costs are often not taken into account when assessing the economic impact.
- The urgency to prepare and invest in incident response usually occurs only after an event with a significant impact [2].
- The cost of cybercrime will continue to increase as more business functions move to online platforms, and more companies and consumers around the world connect to the Internet [8].
- Incident detection is the most costly internal activity followed by recovery [16]. Cleaning up in the aftermath of cybercrime is expensive, often more expensive than the crime itself [8].
- Deployment of enterprise security governance practices moderates the cost of cybercrime [16].
- The incentives in cybercrime encourage attack and discourage defence. Cybercrime produces high returns at low risk and low cost for the hackers [8].
- The best data related to cybercrime comes from the financial sector, which is regulated, pays serious attention to cybersecurity, can easily measure loss [8] being also one of the most targeted industry.
- The time taken to identify and contain a data breach directly affects the cost [5].

**Organisational**

- Companies are in need of qualified personnel, but in some cases they lack completely. Employing under-qualified employees implies a higher risk [1][3].
- Companies that fail to adequately protect their networks will be at an increasing competitive disadvantage [8].

**Policy**

- Board involvement, the purchase of cyber-insurance, and business continuity management policies, can reduce the cost of a data breach [5].
- Governments need to collect and publish data on cybercrime, and help countries and companies to make better choices about risk and policy [8].

**Technical**

- The most affected CII sectors seem to be financial, ICT and energy.
- A large majority of organisations still don't have implemented basic security controls [2].
- Attackers are streamlining and upgrading their techniques, while companies struggle to fight old tactics [15].
- The incident discovery phase (time to discover) takes longer than the time to compromise [17].
- In most of cases, attackers are able to compromise an organization within minutes [6][17].
- Hackers and criminal insiders cause most of the data breaches [5].
- Exploiting browser, OS, and other third-party software (e.g., Flash and Java) vulnerabilities to infect end-user systems is a common first step for attackers [7].
- Deploying security/threat intelligence sharing systems seems to be efficient [15][16][17].
- The large majority of vulnerabilities were exploited one year or more after the vulnerability was revealed; patch management still one of the weakest links [2][17].
- Short-life malware: 95% of malware types showed up for less than a month, and four out of five didn't last beyond a week [17]. A vast majority of the malware samples are unique to an organisations.

# 4. Conclusions and recommendations

Despite the abundance of studies that attempt to address the economic impact of cyber incidents, it was found that the lack of common approach, objectives and thematic areas, cannot effectively contribute to an EU wide study. However, it has been possible to identify trends that can be useful for giving a general impression on EU and international level, and assist on future work.

Study **findings** agree that cyber-incidents are a real problem, manifest through a particular set of threats, to an extend affect similar types of assets, resulting to a financial loss. Among the main findings we can find:

- ***Finance, ICT and Energy sectors, appear to have a much higher incident cost***, in comparison with the rest of sectors.
- The most common attack types for Financial sector and ICTs appear to be ***DoS/DDoS and malicious insiders***, with the later one affecting the Public Administration sector as well. It is very important to highlight that these two types on their own, ***make approximately half the annualized cost of all cybercrime*** (Figure 9) [16].
- The ***most expensive attacks*** are considered to be insider threats, followed by DDoS and web based attacks [16]. The ranking slightly changes when it comes to different countries, as you will see later in the document.
- In terms of ***country loss*** the values provided reach up to 1.6% of GDP in some EU countries [11]. Other studies mention losses reaching up to 37 billion euro (27 Billion pounds) per year (UK) [1], while for Germany figures like ***425,000 to 20 million euro*** per company per year [10]. Another study provides the average cost per company per year that can vary between 2.3 mil. and 15 mil. euro in 2015 [16]. One study also estimates the economic loss for the global economy to be from 330 to 506 billion euro (375 to 575 billion $) [8].
- Data seems to be the ***most affected asset***. In this context data may mean any kind of information – from confidential information and personal identifiable data, to logs and other types.

In terms of **conclusions** reached among the most notable is that the ***measurement of the real impact of incidents in terms of the costs needed for full recovery proved to be quite a challenging task***. Determining cost values that are as close as possible to reality is a key to determining the real economic impact of incidents on EU's economy. Knowing the real impact can help define proper, coherent and cost effective (beneficial) mitigation policies. As a short note, the current draft of the NIS directive[5] states that "[…] *incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union*", without making any use of figures in support of this. We have also noticed the ***lack of a unified and standardised approach in developing such studies,*** often driven by business factors rather than actual interest of stakeholders or realistic needs.

The importance of the topic along with the gaps identified along our analysis justify the supplying of some **recommendations** specific per type of stakeholder:

- First of all, the development of such studies in the future, should be done throughout a unified analysis, based on a well-structured methodology, and considering all critical variables that define the EU cyber-space. Although there are quite a lot of organisations developing such studies, there is a need for consistent and accurate studies that will reflect as much as possible the real situation.

[5] http://data.consilium.europa.eu/doc/document/ST-5581-2016-INIT/en/pdf

ENISA could be an actor capable of doing such work, but only with suitable resources and a clear mandate in this area.

- As regards all types of readers that may be interested in such studies, they would have to place the study in context, prior adopting findings or drawing their own ones. By doing this it is possible to better understand the gaps, or parts uncovered by the study, and better understand the overall findings of the study and their relevance within the actual context. A few details that would assist on this mission are the:
    - number of companies that participated in the study (sample size)
    - geographical area analysed
    - organisations who carried out the study and possible business interests
    - methodology used to extract and collect the data
    - industries affected
    - types of threats / incidents taken into account
- An important category of readers are the ***cyber-security professionals*** (CISOs, security analysts, security engineers, security architects etc.). Beyond understanding the context, they should also focus on extracting useful information for their businesses, such as: major threats, recovery costs, affected industries and assets, best practices etc.
- **Policy makers and corporate management (CEOs and CFOs)** have also something to benefit from these studies in terms of future decision making, policy development, business continuity etc. But again, some filters must be applied to place the study in context and identify the findings that are indeed relevant.
- **Study makers** (organisations that develop such analysis whether being governmental, consultancy companies, cyber-security related companies) can also benefit from this review by improving their frameworks/methodologies, providing more details and transparency on how information was collected and processed, dimension, constituency and representativeness of the sample size, economic sectors covered, types of cyber-threats/incidents covered, challenges identified during the study (that can help understand certain lack of information within the study).

# Annex I – Methodology description

To properly carry out the systematic review a methodology was defined in terms of steps and criteria that must be followed in order to collect accurate and coherent data. The methodology is based on previous work of ENISA in terms of incident reporting, CIIs, threat landscapes and other relevant fields.

As previously mentioned, there are a number of studies publicly available that cover different types of statistics about cyber incidents, but not all of them are relevant to ENISA's work. In order to select the suitable studies to be analysed some quality criteria had to be applied. In the table below you will find 12 defined criteria, of which 5 are mandatory and 7 are non-mandatory. For a study to be taken into account all 5 mandatory criteria should have been accomplished.

**Table 3: List of qualitative mandatory and non-mandatory criteria**

| Nr. | Type | Name | DESCRIPTION |
|---|---|---|---|
| 1 | Mandatory | Time Frame | Only studies ranging from 2013 to 2015 will be considered. |
| 2 | Mandatory | CIIs Sector | At least one of the following CII sectors must be included in the study:<br>1. Energy<br>2. Information, Communication Technologies (ICT)<br>3. Water<br>4. Food<br>5. Health<br>6. Financial<br>7. Public & Legal Order and Safety<br>8. Public Administration<br>9. Transport<br>10. Chemical and Nuclear Industry<br>11. Space Industry<br>The above list inspired by ENISA's document Methodologies for the identification of Critical Information Infrastructure assets and services. |
| 3 | Mandatory | Economic Data/Costs | The study had to contain details on the economic impact of cyber-security incidents, including details related to the cost of incidents. |
| 4 | Mandatory | Incident type/Attack/Threat | The study must contain information on at least one of the incident types below, inspired by ENISA's 2015 Threat Landscape:<br>1. Malware (Worms / Trojans).<br>2. Web-based attacks (drive by downloads).<br>3. Web application attacks / injection attacks.<br>4. Denial of Service (DoS) or Distributed Denial of Service (DDoS).<br>5. Phishing.<br>6. Insider threat.<br>7. Cyber espionage.<br>8. Ransoware / Rogueware / Scareware / Crimeware.<br>9. Hacktivism.<br>10. ICS/SCADA hacking.<br>11. Critical vulnerabilities (heartbleed, SS7, SSL, shellshock).<br>12. Physical damage/ theft / loss. |

| | | | |
|---|---|---|---|
| 5 | Mandatory | Incident Result | The study must provide details on what the incidents have affected in terms of confidentiality (ex. data breaches), integrity (ex: physical damage) or availability (ex: DDoS). |
| 6 | Non-mandatory | Geographical coverage | Focus on Europe would be most welcomed, but other international studies were also accepted. |
| 7 | Non-mandatory | Assets affected | Details about types of assets affected would be most welcomed. |
| 8 | Non-mandatory | Cost Computing Methodology | Details on how incident costs were determined would be most welcomed. |
| 9 | Non-mandatory | Type of cost | Details on types of costs taken into account would be most welcomed. |
| 10 | Non-mandatory | Staff Profile | Details about incident response specialised staff (level of training etc.) would be most welcomed. |
| 11 | Non-mandatory | Policies/Procedures/Measures | Details regarding the security measures in place within the participating organisations would be most welcomed. |
| 12 | Non-mandatory | Data collection methodology (sources, selection, extraction) | Details about how data was collected would be most welcomed. |

# Annex II – Analysed studies

| No. | Name of study | Source | Year | Geographical coverage | Responders | Country in which the study was developed |
|---|---|---|---|---|---|---|
| 1 | CYBER-ATTACKS: EFFECTS ON UK COMPANIES | OXFORD ECONOMICS | 2014 | United Kingdom | 427 | United Kingdom |
| 2 | GLOBAL THREAT INTELLIGENCE REPORT | NTT GROUP | 2015 | Worldwide | - | Japan |
| 3 | INFORMATION SECURITY BREACHES SURVEY | PWC AND INFOSECURITY EUROPE | 2015 | United Kingdom | 664 | United States |
| 4 | DATA BREACHES IN EUROPE | CEU SCHOOL OF PUBLIC POLICY | 2014 | Europe | - | Hungary |
| 5 | 2014 GLOBAL REPORT ON THE COST OF CYBER CRIME | PONEMON INSTITUTE BY HP | 2014 | Worldwide | 257 | United States |
| 6 | 2015 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS | PONEMON INSTITUTE BY IBM | 2015 | Worldwide | 350 | United States |
| 7 | 2014 DATA BREACH INVESTIGATIONS REPORT | VERIZON | 2014 | Worldwide | 50 | United States |
| 8 | NET LOSSES: ESTIMATING THE GLOBAL COST OF CYBERCRIME | MCAFEE | 2014 | Worldwide | - | United States |
| 9 | 2014 COST OF CYBER CRIME STUDY: UK | PONEMON INSTITUTE | 2014 | United Kingdom | 38 | United States |
| 10 | 2014 COST OF CYBER CRIME STUDY: GERMANY | PONEMON INSTITUTE | 2014 | Germany | 46 | United States |
| 11 | 2014 COST OF CYBER CRIME STUDY: FRANCE | PONEMON INSTITUTE | 2014 | France | 29 | United States |
| 12 | 2014 COST OF CYBER CRIME STUDY: RUSSIAN FEDERATION | PONEMON INSTITUTE | 2014 | Russian Federation | 24 | United States |
| 13 | ENERGY MARKET REVIEW | WILLIS LIMITED | 2014 | Worldwide | 557 | United Kingdom |

| | | | | | | |
|---|---|---|---|---|---|---|
| 14 | 2013 COST OF CYBER CRIME STUDY: UNITED STATES | PONEMON INSTITUTE | 2013 | United States | 60 | United States |
| 15 | ISTR20 INTERNET SECURITY THREAT REPORT | SYMANTEC | 2015 | Worldwide | 157 | United States |
| 16 | 2015 COST OF CYBER CRIME STUDY: Global | PONEMON INSTITUTE BY HP | 2015 | Worldwide | 252 | United States |
| 17 | 2015 DATA BREACH INVESTIGATIONS REPORT | VERIZON | 2015 | Worldwide | 70 | United States |

# Annex III - References and bibliography

[1] Cyber-Attacks: Effects on UK companies, Oxford Economics, 2014

[2] Global Threat Intelligence Report, NTT Group, 2015

[3] Information Security Breaches Survey, PWC and Infosecurity Europe, 2015

[4] Data Breaches in Europe, CEU School of Public Policy, 2014

[5] Global Report on the Cost of Cyber Crime, Ponemon Institute, 2014

[6] Cost of Data Breach Study: Global Analysis, Ponemon Institute, 2015

[7] Data Breach Investigations Report, Verizon, 2014

[8] Net Losses: Estimating the Global Cost of Cybercrime, McAfee, 2014

[9] Cost of Cyber Crime Study: UK, Ponemon Institute, 2014

[10] Cost of Cyber Crime Study: Germany, Ponemon Institute, 2014

[11] Cost of Cyber Crime Study: France, Ponemon Institute, 2014

[12] Cost of Cyber Crime Study: Russian Federation, Ponemon Institute, 2014

[13] Energy Market Review, Willis Limited, 2014

[14] Cost of Cyber Crime Study: United States, Ponemon Institute, 2013

[15] ISTR20 Internet Security Threat Report, Symantec, 2015

[16] Global Report on the Cost of Cyber Crime, Ponemon Institute, 2015

[17] Data Breach Investigations Report, Verizon, 2015


## ENISA

European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

## Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece



TP-04-16-479-EN-N



PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu



ISBN: 978-92-9204-173-1
doi: 10.2824/475621