The scale and impact of industrial espionage and theft of trade secrets through cyber

Written by PricewaterhouseCoopers
December – 2018

pwc

EUROPEAN COMMISSION

Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
Directorate F — Innovation and Advanced Manufacturing
Unit GROW-F.5 — Intellectual property and Fight against Counterfeiting

Contact: Jorge NOVAIS GONCALVES

E-mail: Jorge.novais@ec.europa.eu

European Commission
B-1049 Brussels

Europe Direct is a service to help you find answers to your questions about the European Union.

Freephone number (*)**:**

00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Luxembourg: Publications Office of the European Union, 2018

ISBN 978-92-79-77355-6
doi: 10.2873/48055

Printed in Belgium

Table of contents

List of Acronyms	
APT	Advanced Persistent Threat
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CISO	Chief Information and Security Officer
CSIRT	Computer Security Incidents Response Team
CTO	Chief Technology Officer
CYSPA	(European) Cyber Security Protection Alliance
DoD	Department of Defense (United States)
EC	European Commission
EDA	European Union Defence Agency
ENISA	European Union Agency for Network and Information Security
EOS	European Organisation for Security
EU	European Union
EUROPOL EC3	European Union Agency for Law Enforcement Cooperation, European Cybercrime Centre
FSB	Federation of Small Businesses
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
IFSR	International Financial Reporting Standards
IP/IPRs	Intellectual Property/Intellectual Property Rights
ISAC	Information Sharing Analysis Centre
ISO	International Organization for Standardization
IT	Information Technology
LEA	Law Enforcement Agency
NCSC	National Cyber Security Centre (UK)
NIS (directive)	Directive on the security of Network Information Systems
NIST	National Institute of Standards and Technology
PoC	Point of Contact
PPP	Public Private Partnership
R&D	Research and Development
SME	Small and Medium Enterprise

1. EXECUTIVE SUMMARY

The past decade has seen rapid development in the field of information technology and a digital revolution that has provided unprecedented benefits to the European society and economy, facilitating trade and the provision of services, creating new opportunities for businesses and boosting productivity and economic gain. **While a better-connected world offers new opportunities, there are also new risks**.

This study focusses on investigating the impact on European businesses and organisations of a specific type of cyber incident, namely cyber theft of trade secrets. Information represents a pivotal economic asset for businesses, which rely on confidentiality of data as a key for their industrial progress, crucial for the development of their innovation process and their economic growth.

The study is based on an extensive literature review complemented by stakeholder engagement, namely through an online survey, interviews with key stakeholders and a workshop organised in cooperation with the services of the European Commission (EC) in Brussels on 4th October 2018.

Industrial espionage is a method employed throughout history. Europe is particularly vulnerable to this threat. Because of its first class industrial and academic research and development (R&D), Europe attracts interest from emerging countries and competitors. The Tilburg University confirmed this trend in 2015, estimating that "20% of European companies suffered a breach".[1] The study demonstrates that **European businesses are particularly exposed** to this kind of threat, because of their advanced know-how and production development. In fact, national businesses in Italy (36%), France (24%), Germany (20%) and The Netherlands (17%) topped the list as the Europeans who fear cyber espionage the most.[2] Among these countries, the analysis reveals that German companies are most affected with 17% of them declaring sensitive data stolen between 2015 and 2017. Sectors with distinctive industrial expertise are targeted more often, such as luxury manufacturing in Italy or finance in the UK. At European Union (EU) level, manufacturing, information and communication technologies, finance, health and medical technologies are the most impacted sectors, demonstrating that cyber-misappropriation of trade secrets focuses on strategic economic production. As 26 billion personal devices, business and industrial equipment are about to become seamlessly connected in Industry 4.0, the "surface" available for competitors is amplifying, encouraging the multiplication of means and techniques for the fulfillment of cyber intrusions.

There was great consensus among stakeholders interviewed and surveyed on the fact that cyber theft of trade secrets represents a concrete and growing threat for all types and sizes of companies and organisations holding confidential information. Businesses across the EU are constantly cyber-attacked and the cyber threat of trade secrets continues to grow. Stakeholders were of the view that one of the main issues is the lack of accurate and exhaustive data on the issue. The real extent of the problem might therefore be **much larger than what it is currently perceived.**

Estimates on the economic impact of cyber theft of trade secrets can be considerably high and these impacts can have repercussions both for businesses and for society as a whole.[3] The European Centre for International Political Economy (ECIPE), a

---

[1] Tilburg University. (2016). Trade Secret Protection in the U.S. and EU. Available at: http://arno.uvt.nl/show.cgi?fid=141634

[2] Trend Micro. (2017), Challenges and Opportunities for 2017: Trend Micro Global. Available at: https://blog.trendmicro.com/challenges-opportunities-2017-trend-micro-global-research-peels-back-layers/

[3] "Theft of commercial trade secrets, business information and personal data, disruption of services - including essential ones - and of infrastructures result in economic losses of hundreds of billions of euros each year. They can also have consequences for citizens' fundamental rights and for society at large". European Commission, Brussels, 5.7.2016 COM(2016) 410 final, at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0410&from=en

Brussels-based think tank, describes in its latest report on cybercrime an economic impact caused by cyber theft of **€60 billion loss in economic growth** in the EU and a consequential **potential loss of 289,000 jobs**.[4]

There is a **basic problematic issue:** the general **lack of awareness** among European companies on the threat posed by cyber theft of trade secrets and the measures that should be put in place to prevent it. This is especially true for Small and Medium Enterprises (SMEs), because of their limited capacity to invest in advanced cybersecurity defence measures. At the same time, European SMEs, which constitute the vast majority of the entrepreneurial sector, are inadequate in establishing the nature and quantity of stolen data. This translates in a limited availability of data on cyber theft of trade secrets across the EU. Such **scarcity of data** represents a **finding** *per se*. Moreover, if and when detected, **businesses prefer not to disclose** information about suffered misappropriation, due to the subsequent damages, such as impact on stock prices and marketplace reputation. Besides, even when companies report cyber incidents, generally **the information is inexact or incomplete**, making the assessment of the economic impact one of the most challenging features characterising the cyber theft of trade secrets issue. Without information on the nature and mechanics of the threat, sizable technical investments and the elaboration of preventing and mitigating measures may fail to address accurately the issue.[5]

Nevertheless, the literature agrees on four main factors needed to assess the impact: **opportunity costs, negative impacts on innovation, additional costs for security, and reputational damages**. Stakeholders identify **the time delay** in recording the negative impacts and the **difficulty in calculating indirect costs** as the two crucial factors limiting and influencing the possibility to define an accurate economic quantification of the impact of the misappropriation of confidential industrial information.

Considering the broad nature of the threat, an **effective strategy to fight industrial cyber espionage** must rely on a multi-disciplinary approach, derived through coordinated collaboration among businesses, cybersecurity service providers, governments and researchers.

To this end, the study formulates **four main areas of recommendations,** designed to be implemented by the EU, taking into consideration both strategies and legal instruments to tackle cyber theft of trade secrets. The four areas identified are: "Awareness and Training", "Facilitate Businesses in Addressing the Challenge", "Enhance Institutional and Coordination Capabilities" and "Strengthen Law Enforcement".

The first area of focus – Awareness and Training – addresses the core problem of general **unawareness of the threat of cyber theft of trade secrets** among European businesses, especially SMEs, and recommends the organisation of meetings, events, media publications, and dissemination of case studies, to strengthen management-level awareness and ensure continuous training for all levels of staff.

In order to increase awareness of the threat among policy makers and high-level officials case studies, best practice measures and guidelines would be useful – in particular in relation to the identification of internal departments, responsible employees and the role of relevant actors, such as CERTs and ENISA. Increasing awareness of the risks associated with cyber theft of trade secrets leads to greater demand for new **preventive measures within industrial sectors**. A set of incentives at EU level can assist businesses, particularly SMEs, in addressing the challenge and support their technology development and knowledge transfer across all sectors and categories of business. Moreover, the development of new tools and technologies should be advanced by increasing both public and private funding in research and innovation.

---

[4] ECIPE. (2018). Stealing thunder, Cloud, IoT and 5G paradigm for protecting European commercial interests. Will Cyber espionage be allowed to hold Europe Back in the global race for industrial competitiveness? http://ecipe.org/publications/stealing-thunder/?chapter=all

[5] Brooking institution - Cyber Theft of Competitive Data: Asking the Right Questions. Available at: https://www.brookings.edu/wp-content/uploads/2016/06/BrookingsCyberTech_Revised.pdf

The EU should act as a coordinator to bring about political momentum on the issue and could do so by providing **a concerted solution to a shared problem. The EU should foster** international cooperation among sectoral key players, for the adoption and implementation of effective countermeasures. The EU could reinforce the resources and competences of the ENISA with a view to improving coordination among national authorities.

Finally, aiming at ensuring certainty and predictability of **law enforcement**, more stringent laws will be fundamental at EU level. The creation of a specific investigation law enforcement body for the prosecution of cyber theft of trade secrets can foster European monitoring and intervention operations. Since there is not a single reporting system for the notification of cyber theft of trade secrets, overlapping of the reporting systems using different taxonomies and methodologies for data collection across countries limits the possibility of building accurate aggregate data. A **common and coordinated reporting system** at EU level would be helpful for **timely response interventions.**

However there seems to be little appetite from industry for the setting up of a brand new and horizontal reporting mechanism at EU level. The mere prospect of having a more solid factual basis for policy making at EU and national levels is not considered a sufficient incentive for individual companies to report incidents or attempts of trade secret theft by cyber means in a systematic way. A more feasible approach could be the promotion of sector-based and industry-led reporting systems that could function as rapid alert systems between peers and which would progressively increase awareness and expertise and improve preparedness and resilience. Therefore, a **pilot reporting system** tested by users to gather feedback, could be a starting point for a future roadmap.

2. INTRODUCTION AND SCOPE OF THE STUDY

Nowadays, digital connectivity and pervasive integration are introducing a wide array of security risks for all types and sizes of organisation. As a result, everything is connected, and flexibility, mobility and speed of communication are examples of essential variables required for efficient and effective operations, especially for businesses.

A substantial number of intrusions target valuable knowledge and information, such as details about the business, know-how, and technology that companies treat as confidential. This study refers to such information as trade secrets.[6]

More specifically, trade secrets can include formulae, manufacturing processes, methodologies to improve decision-making (e.g. algorithms or calculations), a unique design of a product or service, pivotal results from surveys or studies (e.g. geological survey of shale oil deposits), tools that improve work results, merger plans, or information regarding business negotiations and strategies. Trade secrets comprise any type of confidential information that allows a business to offer better products, be faster or cheaper, to be the first in introducing innovative products and solutions and outpace competitors.

In a digital world, trade secrets can be stolen from any location globally, with perpetrators often remaining anonymous and unidentified for long periods. The problem in defining a clear impact on companies is that in many cases these companies are unable to detect or report the incidents. Additionally, the majority of data available in the literature refers to cyber incidents rather than cyber theft of trade secrets specifically. Hence, there is a general lack of both qualitative and quantitative data on the threat.

In this scenario, EU industrial and research sectors emerge as one of the main targets of theft of trade secrets through cyber means. As examined in this study, several Member States reported cyber theft of trade secrets in recent years; indeed, all Member States, industries and organisations are at risk. The issue has also been recognised at the highest level by the EC, which adopted a directive on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.[7] Effective design and implementation of cybersecurity, as well as the protection of trade secrets do have the interrelated and compatible goals of protecting organisations' value, the economic competitiveness of Member States, and reducing monetary and reputation risks.

The rising threat of cybersecurity breaches for European organisations and companies puts confidential business information at greater risk from theft and loss. According to the Global Fraud & Risk Report,[8] an astounding 85% of surveyed executives reported that their company experienced a cyber intrusion, or theft or loss of information in 2016. 36% of respondents reported that their networks were infested with viruses or worms, 33% reported being subject to email-based phishing attacks, 27% reported data breaches resulting in loss of customer or employee data, Intellectual Property (IP) or Research & Design (R&D), while 25% reported incidents resulting in the deletion of data. In the age of big data, the survey demonstrated extensive loss or theft of data via cyber-related incidents that include, among other types, data breach, data deletion, and loss of equipment with sensitive data.

[6] In order to provide a EU-based legal definition of trade secrets, the Directive 2016/943 states as follows: trade secret is defined as an "information [that] is secret, has commercial value because it is secret, and has been subject to reasonable steps […] to keep it secret".

[7] European Commission. (2016). Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

[8] Kroll (2017), Global Fraud & Risk Report, available at: http://www.kroll.com/en-us/intelligence-center/reports/global-fraud-risk-report

Scope and Purpose of the Study

The scope of this study involved the collection and analysis of data regarding the estimated volume and impact of **industrial espionage and theft of trade secrets through cyber**, culminating in the formulation of recommendations on appropriate policy responses.

The study also addressed the issue of a **lack of information on cyber theft of trade secrets**, exploring possible ways of collecting data through voluntary reporting of volumes and impacts of cyber theft of trade secrets.

In line with the scope described above, the specific objectives of the study were to:

- Collect and analyse qualitative and quantitative data and information through a review of the most relevant literature on cyber theft of trade secrets and industrial cyber espionage;
- Collect and analyse qualitative and quantitative data and information **through consultation with a variety of stakeholders, in particular the European business community,** from as many Member States of the EU as possible;
- **Assess the estimated volume and impact** of cyber theft of trade secrets within the EU;
- **Report all information gathered and analysed** though the literature review and consultation including key statements from stakeholders (which can be presented in an anonymised manner, if necessary), including examples, figures, graphics and conclusions;
- **Assess the extent to which** the theft of trade secrets through cyber is recognised as a relevant issue worthy of policy intervention at EU level;
- Suggest appropriate **policy recommendations** to mitigate the issue;
- Assess whether, and under what conditions a system of voluntary reporting could be set up for regular data collection at EU level.

As far as the final report is concerned, the study team provided a response to the following questions (posed in the Terms of Reference) by means of literature review:

- What organisations have addressed the topic of cyber theft of trade secrets through publications, reports, position papers and conference reports since 2012?
- Is cyber theft of trade secrets a real threat to businesses operating in the EU?
- How often and with what intensity are European companies and research institutions experiencing cyber theft of trade secrets?
- What is the impact of such cyber incidents on companies or organisations that suffer intrusions?
- Is there a perceived impact, or a risk of an impact, on the innovation, economic performance and competitiveness of European industry?
- Is there a growing trend regarding the number and impact of incidents?
- Are there economic sectors, or specific areas of scientific research particularly targeted by cyber intruders wanting to get access to undisclosed information?
- Is there a lack of publicly available data on incidents of cyber theft of trade secrets, their magnitude and impact? If so, why?
- Are Small Medium Enterprises (SMEs) also victims of cyber theft of trade secrets?
- Are there systems and mechanisms that companies are using, or may use, to prevent, react to and report on cyber intrusion (that is focussed on attempting to access confidential/proprietary information), provided either by themselves or third parties?

- How can the EU and national authorities help businesses and research institutions face the challenges posed by cyber theft of trade secrets?

The study collated data from Austria, France, Denmark, Finland, Germany, Italy, Ireland, the Netherlands, Slovenia, Sweden, United Kingdom, Belgium, Estonia, Poland and Spain.

Structure of the report

This report consists of five main sections:

- A literature review examining the topic in a selected list of documents from a variety of disciplines. While the literature review focuses on cyber theft of trade secrets, publications on cybersecurity in general were also analysed inasmuch as information was valuable to the subject of the study;
- Overview of stakeholder consultation. The section provides a synopsis of all information gathered through the interviews and survey, which involved 79 experts. Experts were selected from specific fields so as to ensure sufficient coverage of the topic, namely four main categories: business, research laboratories, cybersecurity providers and governmental bodies;
- An assessment of the main findings of the study, based on both the literature review and outcome of the stakeholder consultation. This section identifies four areas of findings:
    - the main threats and trends regarding the cyber theft of trade secrets, along with growing levels of risk and concern in the EU;
    - the prevalence of obstacles impeding the assessment of the impact of cyber theft of trace secrets on the European businesses;
    - data regarding the most affected industrial sectors in Europe;
    - the consequences for SMEs, which deserve special attention, as they represent the majority of the European industrial sector and are generally more vulnerable to cyber threats;
- Recommendations addressed to EU institutions and national governments, in order to foster the implementation of mid- and long-term policies, as well as practical solutions able to mitigate cyber theft of trade secrets;
- A list of Annexes comprising the following:
    - Annex A describing in detail the methodology used for the preparation of the study;
    - Annex B providing the Case Study Protocol, employed in order to gather data from businesses on possible cyber theft of trade secrets endured;
    - Annex C presenting two case studies identified through literature review and comprehensive research where cyber theft of trade secrets occurred to a business based in the EU;
    - Annex D reporting the results of the online survey which was used as a complementary tool to interviews;
    - Annex E providing a summary report of the workshop "Industrial Espionage In A Digital World";
    - Annex F providing a small description of the EU Directive on Security of Network and Information System (NIS Directive);
    - Annex G detailing the structure and functions of the European Union Agency for Network and Information Security (ENISA);
    - Annex H summarising the United States policy and strategy for cyber theft of trade secrets;
    - Annex I presenting a comprehensive bibliography.

3. METHODOLOGY FOR THE PREPARATION OF THE STUDY

The preparation of the final study report was carried out between January 2018 and October 2018, with **methodological triangulation** a fundamental element of the methodology employed to analyse the current state of the art, the existing literature, stakeholder perception of the threat and the estimated volume and impact of cyber theft of trade secrets to expand the body of knowledge with qualitative and quantitative data on this issue.

In the methodological triangulation different sources, design and forms of analysis are used. The triangulation approach is a particular form mixing methodology methods that pursue: a) convergent validity, that is combining qualitative and quantitative methods to study the same phenomenon in order to gain convergence and increase validity; b) compensation: use strengths of each method/source to overcome the weaknesses of the other and, thus, enrich the study of a phenomenon; and c) expansion: use each method/source to obtain a fuller picture of a phenomenon. For instance, perceptions and opinions can be contrasted against evidence from statistics or documents and vice versa.

3.1. Desk Research

Desk research activities were conducted throughout the preparation of the final report. The study team collected and examined all publicly available data on the topic, analysing almost **200 publicly available documents**, including reports, surveys, publications, conference papers, etc.

With a more targeted approach, the team analysed documents from a variety of sources likely to provide valuable results, such as:

- Governmental bodies;
- International organisations;
- Academia and research bodies;
- Think tanks;
- Cybersecurity experts;
- Cybersecurity service/product providers;
- Business associations;
- Private Service providers.

On the basis of the most authoritative sources, the team identified additional and more detailed publications and dossiers, including also referenced blogs. This phase enabled the team to ensure that any relevant publications were not missed, while acquiring an understanding of the most recurring and valuable sources to be further analysed.

3.2. Interviews

Another fundamental step of the triangulation methodology was the interview process. A programme of interviews and an online survey targeted stakeholders across all relevant sectors and countries within the scope of the study. Desk research activities were of primary importance in identifying relevant stakeholders for participation in the interview programme. Interviews were conducted with stakeholders across four different categories:

- Business community (entrepreneurs; companies; economic groups) – Cat. Bus;
- Scientific researchers and research bodies – Cat. Sci;
- Cybersecurity service providers and cybersecurity experts – Cat. Cyb;
- Other stakeholders (governmental bodies, international organisations, think tanks, academia) – Cat. Others.

In terms of identifying the most relevant stakeholders from the four categories above, they were sought from **15 Member States** from among the following:

- Participants in conferences on cybercrime and cybersecurity;
- Paper, reports, position papers, publications on cyber theft of trade secrets;
- Chief Information Security Officers (CISOs), Chief Information Officers (CIOs) and Chief Technology Officers (CTOs) from prominent companies operating in Europe;
- Academic professors and scientific researchers with extensive skills in cybersecurity and in-depth knowledge of cybercrime;
- Cybersecurity experts and cybersecurity service providers;
- Direct contacts provided by stakeholders consulted;
- PwC Databases and networks.

A draft questionnaire, used during the interviews and based on the gap analysis conducted during the literature review phase, was further improved based on preliminary findings and opinions gathered from the first round of interviews. The questionnaire was intended to identify and collate information that was missing or not publicly available through desk research activity, as well as stakeholder perceptions regarding the current threat and actionable recommendations to be considered.

A total of **41 interviews** were conducted during the period from March 2018 to July 2018. As a back-up solution in case stakeholders were unwilling to participate in an interview a request to complete the online questionnaire was sent.

3.3. Online Questionnaire

The interviews and the online questionnaire are **complementary tools** which were utilised to perform and complete the data collection and inform the analysis. They are pivotal in enabling the validation and further articulation of information obtained through the literature review as well as identifying and completing gaps in information.

The survey comprised a web-based questionnaire, which was available online from 7th May to 25th May 2018. Stakeholders unable to participate in the interview were invited to participate in the survey by email, which was created with a specific template. Once the stakeholder submitted their response electronically it was stored in a global database. The results were regularly checked so that reminders could be sent to those who had not yet responded. A total of **37 responses** were collected and analysed.

3.4. Workshop "Industrial Espionage In A Digital World"

On 4th October 2018 the services of the EC held a workshop on industrial cyber espionage where the preliminary findings and draft recommendations of this study were presented to stakeholders, including representatives and experts from Member States, EU agencies, individual businesses and business organisations, think tanks, academia, and from the intellectual property, SMEs and cybersecurity worlds. The workshop served as an opportunity for participants to share their experiences, discuss actual cases, and comment on the contractor's preliminary findings and draft recommendations. (See summary report, attached as Annex E).

3.5. Aggregation of Results Obtained

Concerning data collection and the aggregation of the results obtained, a mixed approach was adopted. This mix implies above all complementarity between qualitative and quantitative evidence gathered through the interviews, the online questionnaire and the workshop. In order to report evidence and stakeholder opinion on the topic of cyber theft of trade secrets and validate what was found during the literature review, all information were aggregated, ensuring also the confidentiality of the information obtained.

4. LITERATURE REVIEW ON CYBER THEFT OF TRADE SECRETS

An extensive body of knowledge and information in the field of cybercrime is produced and disseminated globally. The scope of this study is focussed on the cyber theft of trade secrets, which is a sub-theme of cybercrime. However, the research team scrutinised and reported information from cybercrime literature in general, as it provided some valuable information on the specific area of research. The body of literature devoted to cyber theft of trade secrets specifically, which is considerably less than that available on cybercrime, was then subject to a more systematic review and analysis.

As a general outlook on the existing literature, **there is only limited qualitative and quantitative information available on cyber theft of trade secrets**. The 2013 EC Impact assessment for the Directive 2013/914 on the protection of undisclosed know-how and business information (trade secrets) against misappropriation states that "Collecting data on the total number of cases of trade secrets within the European Union is a quasi-impossible task". And even Member States' intelligence services recognise that they are "groping in the dark" with regard to cases of economic espionage".[9]

One key reason for the lack of data on cyber theft of trade secrets is that **many intrusions are not detected**. Companies' intrusion detection systems unreceptively supervise the traffic on their networks for irregular activity, but skilled cyber criminals can avoid detection by manipulating the traffic stream. Therefore, there is no clear-cut way to detect cyber theft of trade secrets and today, a large number of these are detected by chance.

Even if detected, incidents are often not reported. **Companies are reluctant to admit that they have been victims of trade secrets misappropriation**. They are not incentivised to report incidents out of fear of impact on stock prices and marketplace reputation.

Even when intrusions are reported to mandated authorities, information is often vague or incomplete. Indeed, information and data are **collected and reported in different ways across EU organisations and countries**, according to different methodologies and taxonomies. The volume of data required to construct an accurate assessment that withstands scrutiny is significant. Therefore, the evaluation of the scale and impact of cyber theft of trade secrets remains challenging.

There is nevertheless a significant and growing body of literature on the topic that provides some direction. As a result of our literature review, the most active organisations in terms of knowledge production, comprehensiveness of data and recognition within the public debate are **cybersecurity service providers/product providers**, representing 31% of the sample with a total of 54 publications (see Figure 1).

[9] European Commission. (2013). Impact Assessment on a proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against misappropriation. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013SC0471&from=EN

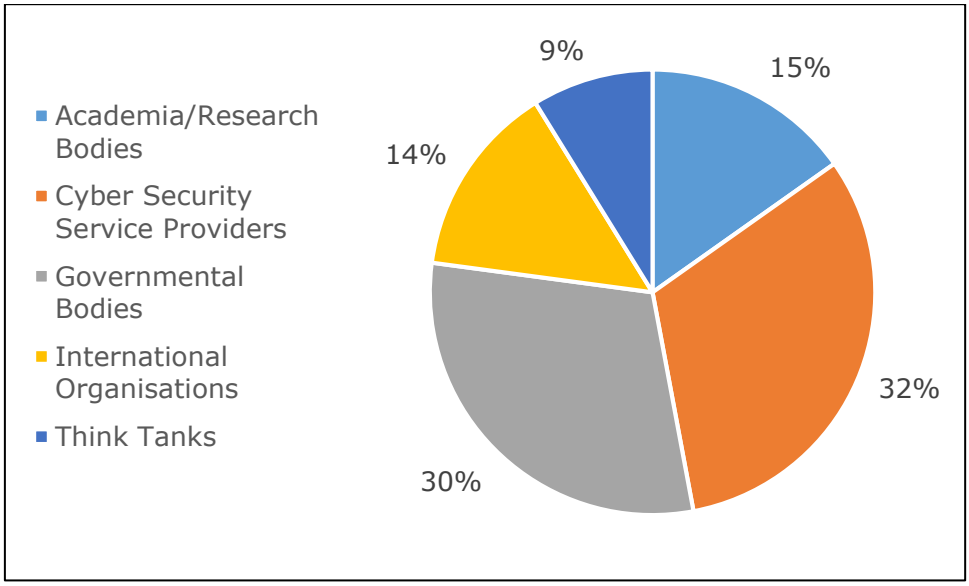


Figure 1 – Organisations addressing the topic

Cybersecurity providers have a prominent role in the dissemination of information in the field of cyber theft of trade secrets. Having access to a wide range of quantitative data on cyber intrusions detected through their cybersecurity software, they produce data which is extensively referenced in other studies. **The Verizon "Data breach investigation report" is one of the most relevant and recognised reports**. It provides quantitative assessment on cybercrimes and encompass a specific section on "cyber espionage". Similarly, **Symantec** published annually its **"Internet Security Threat Report"** that addresses, among other cybercrimes, cyber theft of trade secrets issues.

Concerning **national level publications in the EU** (reported as **Governmental Bodies** in the figure above), we can observe that within those countries considered in this study, **theft of trade secrets is also a recurring theme**. The most active countries in knowledge production being the UK, Germany, the Netherlands, Denmark, Belgium, Estonia, Poland, Italy and Spain. Several institutions/organisations linked with public bodies (such as national research centres) produce **annual reports on cybersecurity**. Member States often task within their National Cybersecurity Strategies a public body or a research centre to publish an annual report on cybersecurity. In some countries it is rather the national Computer Emergency Response Team (CERT) that publishes such reports.

While half of the national reports analysed address the topic of cyber theft of trade secrets in a specific section devoted to the purpose, all others mention the topic throughout the text in a non-systematic way when discussing different cybercrimes, actors, vulnerabilities and specific incidents occurring in the year of analysis. **The vast majority of these publications provide only limited quantitative information**. Some tailor their focus on certain aspects. Estonian (Information System Authority), Spanish (National Cryptology Centre) and Dutch (Ministry for Security and Justice) reports concentrate their analysis on the sectoral industry levels and impact. Others aim at providing assessments on the level of national threat of cyber theft of trade secrets (the Belgian Federal Science Security Office, the German Federal Office for the Protection of the Constitution, the Italian Association for IT Security, the Danish Centre for Cyber Security, the National Polish Computer Emergency Response Team, and the British National Cyber Security Centre). At national level **no institution or publicly affiliated research centre produce a report which is exclusively devoted to the topic of cyber theft of trade secrets**.

Academia and research bodies have produced some relevant studies and make up for 15% of all publications analysed. One of the most extensive empirical studies on the economic impact of "industrial espionage" is from the IZA Institute of Labor Economics "Industrial Espionage and Productivity." It gathers data from sources made available after the fall of the Berlin Wall to assess the Total Factor Productivity gap between East and West Germany as an outcome of industrial espionage perpetrated by the German

Democratic Republic. Although the study refers to espionage through non-cyber technologies, its assessment relies on an extensive collection of empirical evidence.

While there is a general interest on the specific issue of cyber espionage **only 9% of the literature comes from think tanks**. A substantial part of these publications addresses the topic being more interested in the national security dimension, while others focus on the impacts on competitiveness and innovation. One of the most relevant is a recent study from ECIPE "Stealing thunder, Cloud, IoT and 5G paradigm for protecting European commercial interests. Will cyber espionage be allowed to hold Europe Back in the global race for industrial competitiveness?" The Brooking Institute which is one of the world leading think tanks published the "Cyber-enabled Competitive Data Theft: A Framework for Modelling Long-Run Cybersecurity Consequences" that uses a peculiar methodology for analysing the impact of theft of trade secrets in consideration of the exiguous data available.

As a general finding, it is clear that **what is defined in our study as "cyber theft of trade secrets" in the literature is often conceived in a semantically different way** in terms of the understanding of the notion and what it encompasses according to the legal framework of reference that varies from country to country.

While our focus of research was mainly on European studies, reports and position papers, the research team came across a **wide range of publications originating in the United States** of America (US), typically produced by cybersecurity service providers, think tanks and academia. A general remark is that the US seems to be more active in knowledge sharing in the context of cyber theft of trade secrets compared to its European counterparts.

Finally, **one of the key challenges during the literature review was the identification of European companies that were victims** of cyber theft of trade secrets. In Europe, companies seem to be more reluctant in disclosing information on incidents of cyber theft of trade secrets than US-based companies. In fact, most reports, studies and online articles discuss European incidents only in generic terms and vaguely mention the targeted industry, while there are cases of companies from the US which provide details of such incidents. It was therefore particularly challenging to identify European companies that were victims of cyber theft of trade secrets as defined in the "scope and objective of the study".

The relevant data collected from the literature review will be referred to in the presentation of the key findings in combination with the data collected through stakeholder consultation. Nevertheless, there seems to be wide spread agreement that malicious cyber intrusions are growing in number. Such intrusions have different origins, intentionality and consequences, but it is clear that a significant part of such intrusions aim at collecting undisclosed information and in particular trade secrets. According to some reports, some intrusions are sponsored by States, with aim of collecting data to the benefit of companies of that state. China is recurrently quoted in this respect, and the US has been very vocal in condemning such practices.

KEY FINDINGS

- **There is a lack of data and information on cyber theft of trade secrets.**
- **National Authorities in nine out of fifteen countries publish annual reports on cybersecurity, and six of those reports detail incidents related to cyber theft of trade secrets (Denmark, Estonia, Germany, The Netherlands, Poland and Spain).**
- **Annual reports published by national centres for cybersecurity/ university research centres are available and reporting relevant information in Belgium, Italy and the UK.**

- **European companies almost systematically do not disclose any information concerning incidents of cyber theft of their trade secrets.**
- **Reported incidents are not typically described in terms that enable valuation calculations.**
- **In the US research on the topic is generally more extensive than in the EU.**

5. STAKEHOLDER CONSULTATION

The research team validated findings from the literature review with information collated during interviews with almost 50 relevant stakeholders who had demonstrated expertise or deep knowledge in the topic of cyber theft of trade secrets. Interviews were complemented by an online survey questionnaire, so as to give stakeholders an opportunity to express their opinions if they were not able to participate in an interview. The research team contacted four main categories of stakeholders:

- Business community (entrepreneurs; companies; economic groups) - Cat (Bus);
- Scientific researchers and research bodies - Cat (Sci);
- Cybersecurity service providers and cybersecurity experts – Cat (Cyb);
- Other stakeholders (governmental bodies, international organisations, think tanks, academia) - Cat (Others).

Stakeholders were selected according to their roles and responsibilities, their expertise, their active role in participating in conferences or workshops on the topics and their organisation's risk exposure to cyber theft of trade secrets. Desk research activities were pivotal in identifying the relevant stakeholders to be engaged.

For the purpose of the study, it was crucial to collect a high response rate from the business community, as these actors are the primary victims, or potential victims of trade secrets misappropriations. Therefore, organisations relying extensively on R&D investments for their business sustainability were considered as top interlocutors along with those who were directly affected by cyber espionage campaigns focussed on stealing trade secrets.

The table below indicates the number of stakeholders engaged in the study.

CATEGORIES	STAKEHOLDERS CONTACTED	AGGREGATED STAKEHOLDERS SUPPORT	PROPORTION OF POSITIVE REPLIES RECEIVED
Business community (entrepreneurs; companies; economic groups) - Cat (Bus)	388	28	7%
Scientific researchers and research bodies - Cat (Sci)	40	10	25%
Cybersecurity service providers and cybersecurity experts – Cat (Cyb)	114	9	8%
Other stakeholders (governmental bodies, international organisations, think tanks, academia) - Cat (Others)	179	31	17%
TOTAL	721	78	11%

Table 1 Data on Stakeholder Engagement

Of the 388 business representatives invited to participate in an interview or the online only 7% of these stakeholders responded positively. In contrast, a much higher response rate among scientific researchers and research bodies, and other stakeholders (e.g. governmental bodies, academia, etc.) was achieved, with 25% and 17% willing to participate in an interview respectively. These differing response rates can be explained for various reasons, depending on the specific category contacted.

Academics and representatives of governmental bodies seem to appreciate the opportunity to assist in increasing general awareness on the subject, and to contribute to the development of recommendations to counteract the phenomenon. Academics and scientific

researchers claim that researches on these topics are still very limited and would need more financial incentives from institutional bodies.

Cybersecurity service providers and cybersecurity experts had a very similar response rate to the business community (8% agreed to participate in an interview). There are several key reasons for such a low response rate. Firstly, although in most cases they were aware about cyber theft of trade secrets, they could not disclose the name of the company affected or many other details in accordance with the signed Non-Disclosure Agreements (NDAs). Secondly, most cybersecurity service providers and cybersecurity experts are actively engaged in drafting reports and publications and for this reason, it has not always been possible to easily obtain information on this topic.

Finally, as previously stated, the category with the lowest response rate is the business community. The team assume that the reason for such reticence on the side of businesses depends on its unwillingness to disclose critical company information or any recorded cyber theft of trade secrets, fearing huge reputational and economics damages. Even for publicly known cases and with the exception of just one company, the same companies either decline participation in the interview or preferred to talk about cases involving other companies.

It is relevant to underline that the overwhelming majority of stakeholders interviewed, when asked if they were aware of any case of cyber theft of trade secrets, were unwilling to provide any specific company name unless the case had been publicly disclosed. Many stakeholders also expressed their concern in providing information that could help identify the company.

Some commonalities across all stakeholder categories were identified in the analysis of responses. Specifically, there was overwhelming agreement on the current high level of the threat and its growth in the future, the inadequate degree of awareness within organisations and the lack of understanding and use of cybersecurity tools. These last two aspects were noted by all stakeholders with particular regard to SMEs. In fact, contrary to large companies, almost all SMEs do not have a specific figure within their organisation that deals with or has the proper skills related to cybersecurity. The lack of a dedicated budget also makes it difficult to acquire the most advanced cybersecurity tools and in the case of acquisition of cybersecurity tools, the lack of specific skills for their implementation or management often makes the investment futile. In this sense, large companies, which have more skills and more economic resources, should lead SMEs to undertake a virtuous path, if necessary, also through contractual limitations, in order to increase the cyber resilience of both parties.

Discrepancies across categories appear with regard to the measures for preventing and mitigating the risk of cyber theft of trade secrets. Not surprisingly, while academics and researchers also in this case recommended an increase in funding for cybersecurity research, cybersecurity service providers advocated for a boost in financial incentives for cybersecurity tools and products.

Finally, the team came across another relevant discrepancy with regard to the assessment on the usefulness of a reporting system. Indeed, stakeholders belonging to categories identified as "cybersecurity providers" and "other" were more in favour of a reporting system, being this at EU level or at national level, voluntary or mandatory, than the "scientific research" and "business" categories. More precisely, all "cybersecurity providers" were in favour of a reporting system and 84% of "others" provided positive feedback. Business and scientific research stakeholders expressed a positive reaction in (on average) 66% of responses.

Generally speaking, stakeholder opinion focussed on two main aspects regarding a possible reporting system. To be a valid tool, and in a way to avoid negative repercussion on business reputation, a reporting scheme should be on a mandatory and non-voluntary basis. This way collection of data would be efficient and fruitful and businesses would be reassured about their reputation, as each company would have to comply with reporting requirements. In addition, most respondents believe that, although important, having numerical data on such cyber theft would not bring major benefits but what would serve

the most is the introduction of more stringent regulations and harsher penalties for cyber criminals.

6. KEY FINDINGS OF THE STUDY

6.1.State of the Threat

6.1.1. Threat and Trends. Current Risks and Growing Concern

***Literature review**:* The past decade has seen rapid development in the field of information technology and a digital revolution that has provided unprecedented benefits to the European society and economy, facilitating trade and the provision of services, creating new opportunities for businesses and boosting productivity and economic gain. The creation of a virtual surface represents a new space of innovation and opportunity for all, including the business sector. Despite the multiplication of services and higher prospected incomes, this revolution also creates **new risks** for its users, in terms of both **economic and security threats**, amplified by the growing number of devices available and connected. Currently, these threats affect the industrial sector, calling for the intervention of states and the main regional and multi-lateral organisations, in order to guarantee a safer space where businesses can freely produce innovation and know-how. Cyber theft of business confidential information generates the most relevant cost for the industrial sector among all types of cybercrime.[10] It constitutes one of the **main threats to the stability and economic growth of companies and organisations in the EU**.

Considering the phenomenon at its roots, **industrial espionage is a method used throughout history** by developing economies to improve their standing. A famous example regards the British stealing of secret information about tea manufacturing production, which until 1848 was exclusive to China, and produced a substantial market for the UK, which continues to be part of its signature manufacturing.[11] A more recent example is that reported by the IZA Institute of Labor Economy which investigates the economic returns to industrial espionage by linking information from East Germany's foreign intelligence service to sector-specific gaps in total factor productivity (TFP) between West and East Germany. The study highlights that the average TFP gap between West and East Germany at the end of the Cold War would have been 6.3 percentage points larger had the East not engaged in industrial espionage. Currently, China is often accused of sponsoring cyber theft of trade secrets to the benefit of Chinese industry, which is to a large degree state-owned.[12] [13] [14]

Competitors' inclination has not changed today;[15] rather, it has increased as a result of the digital transformation. Rapid globalisation, increased mobility, advancements in technology and the anonymous nature of the Internet create growing challenges in protecting trade secrets. The risk of hacking is increasing exponentially as 26 billion personal, business and industrial devices and equipment are about to become seamlessly connected in Industry 4.0.[16] In this scenario, Europe appears to be one of the most targeted regions for unlawful appropriation of trade secrets. It has first class industrial and academic R&D such as for

[10] McAfee (2018). Economic Impact of Cybercrime – No Slowing Down.
[11] Rose Sarah, For all this tea. Hutchinson. 2009
[12] CSO. (2017). Germany warns of nation-state cyber espionage threat. Available at: https://www.csoonline.com/article/3211405/security/germany-warns-of-nation-state-cyber-espionage-threat.html
[13] Center for Strategic and International Studies (CSIS) and McAfee. (2018). Economic Impact of Cybercrime – No Slowing Down. Available at: https://www.mcafee.com/us/resources/reports/restricted/economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email&utm_term=0_7623d157be-bb9303ae70-
[14] Accenture. (2017). Cyber Threatscape Report. Available at: https://www.accenture.com/t20171010T121722Z__w__/us-en/_acnmedia/PDF-63/Accenture-Cyber-Threatscape-Report.pdf
[15] Søilen, K. S. (2016). Economic and industrial espionage at the start of the 21st century–Status quaestionis. Journal of Intelligence Studies in Business. Available at: https://ojs.hh.se/index.php/JISIB/article/viewFile/196/156
[16] ECIPE. (2018). Stealing thunder, Cloud, IoT and 5G paradigm for protecting European commercial interests. Will Cyber espionage be allowed to hold Europe Back in the global race for industrial competitiveness? http://ecipe.org/publications/stealing-thunder/?chapter=all

motor vehicles, biotech, infrastructure equipment and aerospace,[17] making it appealing to emerging countries.

A number of data and information sources help provide a glimpse into the threat landscape that the EU is facing.

Cyber theft of trade secrets concerns both public and private sectors on a regular basis,[18] with serious consequences, especially for the industrial sector. In 2015, Tilburg University highlighted that "20% of European companies suffered a breach".[19] Businesses in Italy (36%), France (24%), Germany (20%) and the Netherlands (17%) topped the list as the Europeans who fear cyber espionage the most.[20]

On this basis, "given the rapid rate of innovation across global industry and the rise of cyberattacks by competitors, foreign governments and hacktivist groups, this concern is expected to become even greater in the future".[21] The RSA FirstWatch team, with a focus on malware detection from incident submissions collected, states that the volume of cyber espionage malware employed increased almost **900%** in 2013 compared to all previous years combined.[22] Verizon, according to its own order of measure and data, shows an increase in the volume of cyber espionage: in 2016 cyber espionage comprised 25% of all incidents that resulted in the confirmed disclosure of data to an unauthorised party[23].

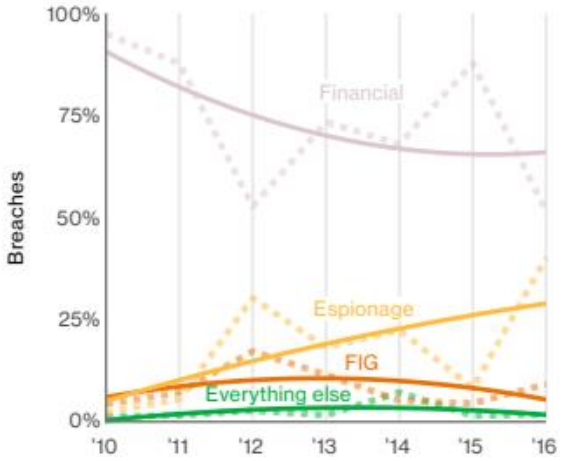


Figure 2 – Trends on the increase in percentage of cyber espionage data breach (Verizon)

***Stakeholder engagement**:* All stakeholders interviewed confirmed the same trends in the EU asserting that cyber theft of trade secrets represents a concrete and growing threat for all types and sizes of companies and organisations holding confidential information. In recent years, cyber espionage has become a concrete threat for millions of people, who

[17] Søilen, K. S. (2016). Economic and industrial espionage at the start of the 21st century–Status quaestionis. Journal of Intelligence Studies in Business. Available at: https://ojs.hh.se/index.php/JISIB/article/viewFile/196/156

[18] AIVD. (2016). Annual report 2016. Available at: https://english.aivd.nl/publications/annual-report/2017/04/04/annual-report-2016

[19] Tilburg University. (2016). Trade Secret Protection in the U.S. and EU. Available at: http://arno.uvt.nl/show.cgi?fid=141634

[20] Trend Micro. (2017), Challenges and Opportunities for 2017: Trend Micro Global. Available at: https://blog.trendmicro.com/challenges-opportunities-2017-trend-micro-global-research-peels-back-layers/

[21] Baker McKenzie. (2017). The rising importance of safeguarding trade secrets. Available at : https://www.bakermckenzie.com/-/media/files/insight/publications/2017/trade-secrets

[22] Alex Cox. (2012). The Cyber Espionage Blueprint: Understanding Commonalities In Targeted Malware Campaigns. RSA FirstWatch. Available at: http://www.emc.do/collateral/white-papers/rsa-cyber-expionage-blueprint-understanding-commonalities-targeted-malware-campaigns.pdf

[23] [23] Verizon. (2017). Data Breach Investigations Report. Available at: https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf

have fallen victim of such kind of cyber intrusion. Indeed, cybersecurity issues are affecting the EU on three principal dimensions: the geo-political dimension, the economic dimension and the personal dimension.

Businesses across the EU are constantly cyber-attacked and the cyber threat of trade secrets continues to grow. Stakeholders were of the view that one of the main issues is the lack of accurate and exhaustive data on the issue; hence, the real extent of the problem might be **much larger than what is currently perceived**.

Interviewed stakeholders were of the view that without deliberate and focussed action from national and supra-national organisations, the threat for European companies and organisations is likely to **grow in the future**.

Only around 10% of stakeholders were of the view that the level of threat will remain the same in the future; at the same time they felt strongly that the level of perception will grow as businesses become more aware of the threats and preventive actions are taken. In their view, the danger is not the increasing volume of incidents rather the development of more sophisticated cyber intrusion mechanisms and techniques.

All stakeholders identified a multi-faceted range of additional **relevant factors** that contribute to increasing the threat of cyber theft of trade secrets:

- Lack of awareness and competences within businesses;
- Wider online exposure of companies, which are also moving to cloud platforms;
- Growing speed with which hackers create new malware and develop their skills in using advanced technological tools;
- Slow pace at which policy makers address the problem;
- Increase in globalisation of markets;
- Global changes in geopolitical strategies;
- The development of new technologies, such as artificial intelligence.

6.1.2. The (In)ability to Detect Cyber Intrusions and Lack of Awareness

Literature review: The analysis led to some major findings. One of the most important findings is that there is limited ability among businesses to detect cyber intrusions in their systems. The **main obstacle** is that **attacks are becoming increasingly sophisticated**, and that there is a **general unawareness of the threat among businesses *per se*** along with inadequate knowledge to detect an intrusion.[24] Furthermore, two-thirds of the organisations affected do not recognise the occurrence of a cyber intrusion and consequently of the risks they are facing.[25] Intruders might retain undetected access to a company's IT system for years. Relatively few organisations understand that they are potential targets, meaning that many fail to protect themselves adequately.[26] A number of studies confirm this trend – criminals retain access to confidential information for a long time without being discovered and victims attribute a "decline in revenue to growing competition rather than theft."[27]

[24] FE - Centre for Cyber Security. (2017). The cyber threat against Denmark. https://fe-ddis.dk/cfcs/CFCSDocuments/The%20cyber%20threat%20against%20Denmark%202017.pdf

[25] Massimo Pellegrino. (2015). The threat of state-sponsored industrial espionage. EUISS. Available at: https://www.files.ethz.ch/isn/191348/Alert_26_Industrial_espionage.pdf

[26] AIVD and MIV. (2017). Cyberespionage: are you aware of the risks? Available at: https://english.aivd.nl/publications/publications/2017/10/26/publication-cyberespionage-are-you-aware-of-the-risks

[27] McAfee, CSIS (2018). Economic Impact of Cybercrime – No slowing down. Available at: https://www.mcafee.com/us/resources/reports/restricted/economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email&utm_term=0_7623d157be-bb9303ae70-

In fact, EUROPOL observed an upsurge attributed to **advanced persistent threat (APT)**. APTs operate silently remaining undetected over long periods with the intent to exfiltrate sensitive data.[28] They are becoming more prevalent each year on a global scale, relying heavily on social engineering techniques, such as spear-phishing, aimed at persuading unaware employees to circumvent companies' IT security measures.[29]

Some of the most serious and troublesome APTs affecting European interests are detailed in Table 2.

Threat	Year	EU Member State Targeted	Description
APT28	2017	At least seven European countries	APT28 targeted the hospitality sector with the intent of stealing passwords and credentials from business travellers, using publicly accessible Wi-Fi networks of hotels, to then infect the organisational networks when the traveller returned home.
Operation Bugdrop	2017	AUS	Sensitive information acquired from its targets include audio recording of conversations, screenshots, documents.
APT10	2017	FRA, SWE, FIN, UK	This threat actor targets managed information technology service providers to access client information for espionage purposes.
UPS	2015	UK	Phishing operation which targeted companies in different industry sectors such as technology, engineering, defence and aerospace.
CARETO	2014	POL, GER, FRA, ITA, IRE, ESP	Careto is a piece of espionage malware that targeted research institutions, energy, oil and gas companies and private equity firms.
AXIOM	2014	GER, UK, NED, ITA, BEL	The Chinese Group "Axiom" targeted organisations that are strategic for economic interests in different industry sectors such as telecommunications, technology and energy.
UNIT 61398	2013	FRA, FIN, UK, GER, NED	The Unit 61398 targeted 20 major industries including financial services, chemicals, energy and healthcare.

Table 2 - List of APT groups and intrusions targeting European organisations[30]

Stakeholder engagement: "Was my company ever struck by a cyber intrusion?" This is among the most common questions cybersecurity experts are asked when engaged by company executives. Of stakeholders interviewed 65% highlighted that still too many companies are not aware of the risks they are incurring. Top managements still tend to

[28] Bitdefender. (2017). Companies blame competition for corporate cyberespionage. Available at:https://download.bitdefender.com/resources/files/News/CaseStudies/study/156/Bitdefender-Whitepaper-CISO-crea1530-A4-en-EN-GenericUse.pdf

[29] ECIPE. (2018). Stealing thunder, Cloud, IoT and 5G paradigm for protecting European commercial interests. Will Cyber espionage be allowed to hold Europe Back in the global race for industrial competitiveness? Available at: http://ecipe.org/publications/stealing-thunder/?chapter=all

[30] Information retrieved from: Council on Foreign Relations. Cyber Operations Tracker. Available at: https://www.cfr.org/interactive/cyber-operations; ECIPE. (2018). Stealing thunder, Cloud, IoT and 5G paradigm for protecting European commercial interests. Will Cyber espionage be allowed to hold Europe Back in the global race for industrial competitiveness? , http://ecipe.org/publications/stealing-thunder/?chapter=all; Lindsay Smith, Ben Read. (2017). APT28 Targets Hospitality Sector, Presents Threat to Travelers. FireEye. https://www.fireeye.com/blog/threat-research/2017/08/apt28-targets-hospitality-sector.html

look at cybersecurity expenditure as a cost rather than a desirable investment, ignoring the relevance of the threat and potential consequences to their companies.

For companies the most difficult thing to establish is **what information was stolen**, not only whether the cyber intrusion ever took place. Stakeholders reported many cases where companies – after detecting a cyberattack – could not comprehend the complexity of the attack as they were not able to analyse what data had been stolen.

Stakeholders made the following statements concerning the timescales associated with incidents:

- The average period of time between penetration of a company's IT system and the detection of an intrusion is around **200 days**;
- Once a hacker gains access to a network they can operate for a period ranging from a **few days to more than 12 months**;
- It usually takes between **five to six years to assess the indirect impacts** of the theft.

Attribution – the process of tracking, identifying and laying blame on the perpetrator of a cyberattack or other hacking exploit - is critical for an effective cyber deterrence strategy as anonymity enables malicious cyber activity. On matters of intelligence, attribution, and warning, Department of Defence (DoD) and the intelligence community have invested significantly in all types of collection, analysis, and dissemination capabilities, all of which reduce the anonymity of state and non-state actor activity in cyberspace. Intelligence and attribution capabilities help to unmask an actor's cyber persona, identify the attack's point of origin, and determine tactics, techniques and procedures.[31]

With regard to the cyber theft of trade secrets, obtaining information about the "actor's cyber persona" or group – in the hypothesis of a prompt detection – potentially could help limiting the damage of a discretional industrial information breach.

While in many cases companies are not aware of a cyber intrusion, when they know about it they do not want to make it public, fearing huge economic losses, reputational losses and loss of business opportunities. One of the greatest challenges faced during the study was to collect accurate information on actual cases of cyber theft of trade secrets. Despite the difficulty in collecting such cases, episodes are recorded **throughout Europe** and only **less than the 15%** of stakeholders interviewed reported that they were **unaware of a case** of cyber theft of trade secrets.

6.1.3. Impact on Companies and Organisations

Literature review: Proper quantification of the economic impact of cyber theft of trade secrets is a serious challenge. This is for several reasons. Damage to organisations goes far beyond the time it takes to deal with a breach or outage resulting from the cyber theft of trade secrets. To understand the economic impact of a theft of trade secrets, both immediate and long-term consequences need to be taken into consideration.

Among the most challenging aspects of the measurement of the impact of cyber theft of trade secrets, is the ability of businesses and organisations to evaluate intangible assets, such as confidential information. This is because it is not sufficient to know how much a company spent on research to determine the value, as many other factors come into play. Adopting assessment tools for their trade secrets companies can estimate what the product would fetch on the market if offered for sale and evaluate its future revenue stream. On the other hand, it is not always the case that the perpetrator who acquires trade secrets through extracting information from a computer network benefits immediately. Many high-tech products require significant "know-how" and experience to produce. Stolen trade secrets alone do not provide that and there may be a long lag between the theft and the introduction of a competing product. For some advanced technologies, there may be a lag

[31] Department of Defence, THE DEPARTMENT OF DEFENSE CYBER STRATEGY 11–12 (2015).

of five to ten years between the theft of trade secrets and the appearance of a competing product on the market.

Despite the assessment challenges, there have been several attempts at estimating the cost of cyber theft of trade secrets. McAfee considers that annual losses worldwide from cybercrime range between **$500 billion and $600 billion** globally, with close to one fourth of these incidents being related to cyber espionage[32]. Estimates from the Brussels-based think tank ECIPE consider that commercial cyber espionage jeopardises up to **€ 60 billion in economic growth and up to 289,000 jobs in the EU.**[33]

According to the literature costs sustained by companies that suffered from cyber theft of trade secrets can be divided in sub-categories:

- **Opportunity costs:** Include lost business opportunities, lost sales or lower productivity, forfeiture of first-to-market advantage, loss of profitability, or even loss of entire lines of business to competitors. Breached companies may face competitors who are suddenly able to replicate their products or solutions at a cheaper price. In 2016, 23% of organisations experienced a loss of opportunity due to intrusions, and among them 42% registered an opportunity loss accounting for more than 20% of its value to the company;[34]
- **Negative impacts on innovation**: Companies invest in R&D to create a return. Therefore, trade secrets represent a significant portion of their assets. R&D generates a competitive advantage, and therefore return, if its results are used exclusively by the ones that invested in R&D. If the results are leaked to and used by competitors, then R&D does not bring substantial competitive advantage. Additionally, as the threat augments,[35] companies become less prone to invest in innovation, due to the risk of misappropriation of their R&D. The company holding the trade secrets risks decreasing its profit margin expectations and reduces the likelihood of future reinvestment in R&D;
- **Increased costs for security:** Include the annual global expense on cybersecurity software, as well as the cost of cleaning up affected systems and cybersecurity insurance. In this respect, SSP Blue expects that companies across the globe will spend about $170 billion on cybersecurity by 2020; an increase of 10% since 2015;[36]
- **Reputational damage:** Companies endure this impact as a consequence of a theft becoming publicly known. The damage includes, among others, lost value of customer relationships, value of lost contracts, and devaluation of trade name.[37] In this regard, 600 mid-sized businesses across six European countries (Germany, Spain, France, Hungary, the Netherlands and the UK) reported the occurrence of reputational damage in 48% of hacked businesses and financial loss in 33% of cases.[38] There are geographical variables on business perception of reputational

[32] CSIS. McAfee. (2018). Economic Impact of Cybercrime – No Slowing Down. Available at: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1IdhuHdutm_source=Pressutm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21utm_medium=emailutm_term=0_7623d157be-bb9303ae70-194093869

[33] ECIPE. (2018). Stealing thunder, Cloud, IoT and 5G paradigm for protecting European commercial interests. Will Cyber espionage be allowed to hold Europe Back in the global race for industrial competitiveness? Available at: http://ecipe.org/publications/stealing-thunder/?chapter=all

[34] Cisco (2017). "017 Annual Cybersecurity Report. Available at: https://www.cisco.com/c/dam/m/digital/1198689/Cisco_2017_ACR_PDF.pdf

[35] Business Europe (2017). The proposal for a Cybersecurity Act - a BusinessEurope position paper. Available at: https://www.businesseurope.eu/sites/buseur/files/media/position_papers/internal_market/2017-11-23_pp_cybersecurity_act.pdf

[36] Will Yakowicz (2015), "Companies Lose $400 Billion to Hackers Each Year," Inc., September 8, 2015. Access at: https://www.inc.com/will-yakowicz/cyberattacks-cost-companies-400-billion-each-year.html

[37] An exception to this trend can be identified in the decision taken by Thyssenkrupp, which decided to report the intrusion it suffered in 2016 in order to decrease reputational loss. For more details on this, please see annex C of this report "Case Studies Identified".

[38] PWC (March 2012), Beyond cyber threats: Europe's First Information Risk Maturity Index, A PWC

risks. UK businesses seem to be more sensible among some European countries (UK, France, Germany, Italy, Sweden and Denmark), to the point that British IT executives perceived reputational damage as the costliest risk in 80% of cases, almost three times higher than in Italy.[39]

Stakeholder engagement: Based on interviews, when detected, **immediate impacts** of a cyber theft of trade secrets account for only **around 10% of costs** the company will have to face; these are mostly directly related to the cybersecurity expenditure invested and on the IT system recovery. The remaining **90% of costs depends on long-term impacts** such as loss of know-how, competitive advantage and the loss of jobs.

As an example, in real numbers, an American company called EMC, was hacked by a Chinese perpetrator (allegedly state-sponsored). Hackers broke into its computers and swiped data that could be used to breach defences of some systems guarded with its technology. The cyber intrusion resulted in the **loss of 700 jobs**, including jobs from its **Austrian subsidiary**, and the loss in stock value **of more than $1 billion**.

Almost 70% of stakeholders consider economic and reputational losses as the most relevant impacts suffered as a result of cyber theft of trade secret.

As stakeholders underlined, economic impacts are proportionate to the value of the information and data stolen, which can be pivotal in maintaining a company's market position and market share. Losing such an advantage implies a direct impact on turnover and can even lead companies to bankruptcy. One stakeholder described the case of a defence industry company, which went bankrupt partially due to cyber theft of relevant technologies for the production of fighter airplanes. Interviews also informed about many cases involving SMEs that have literally ceased trading, because they had lost a significant market share, directly due to the subtraction of proprietary information.

It remains quite difficult to evaluate the cost associated with reputational losses. Once media present the news to the public, then there is an evident cost in reputation, which increases at the rising of **"digital reputation".**[40] Digital reputation has become a key requirement to businesses and the loss of it is associated with a bigger impact than its improvement. Digital reputation follows oscillations, similar to stock exchange charts, which may have sudden increasing and decreasing peaks. Following the diffusion of news about a cyber theft of trade secrets, the decreasing peaks would cause considerable damages, as they are much more durable over time than the increasing peaks. Nevertheless, stakeholders underlined that, as reported by the literature review, measuring the overall costs of a cyber theft of trade secrets is a challenging exercise. For a clearer picture of the impact of cyber theft of trade secrets, it is paramount to capture the right information. Summarising some of the key points suggested from the stakeholders these are the questions that should guide data collection and analysis:

- "Who" is the intruder;
- "Why" it happened;
- "When" it happened;
- "How" it happened;
- "What" was stolen exactly.

report in conjunction with Iron Mountain, March 2012

[39] Bitdefender. (2015). Companies blame competition for corporate cyberespionage. Available at: https://download.bitdefender.com/resources/files/News/CaseStudies/study/156/Bitdefender-Whitepaper-CISO-crea1530-A4-en-EN-GenericUse.pdf

[40] Digital reputation has become a key requirement to businesses and the loss of it has a bigger impact than its improvement. It follows oscillations, similar to stock exchange charts, which may have sudden increasing and decreasing peaks. Following the diffusion of news about a cyber theft of trade secrets, for a company the decreasing peaks would cause considerable damage as they are much more durable over time than the increasing peaks.

The more information available, the more precise the measurement of the impact would be. Nevertheless, the full availability of information is critically dependent on the single case taken into consideration. Stakeholders identified as the main obstacles for the quantification of the impacts:

- The **time delay** in recording the negative impacts;
- The difficulty in calculating **indirect costs**.

6.1.4. How Targeting Changes from One Company to Another: Sector, Size and Country

***Literature review**:* As pointed out by CISCO, cyber theft of trade secrets affects all sectors leaving none to spare,[41,42] but there are researches and assessments pointing to some industries and countries being more prone than others to "fall into the trap".

Despite the different methodologies for data collection and adopted taxonomies of impacted economic areas, the analysis of reports from cybersecurity providers,[43,44,45] leading research organisations[46,47] and reports from national and international bodies, [48,49,50,51,52] all suggest some economic and industrial sectors appearing to be most affected by cyber theft of trade secrets:

- Manufacturing sector;[53]
- Information and communication technologies;
- Financial and insurance activities;

[41] Cisco (2017). 2017 Annual Security Assessment. Available at: https://www.cisco.com/c/dam/m/digital/1198689/Cisco_2017_ACR_PDF.pdf
[42] Verizon (2016). 2016 Data Breach Investigation Report. Available at: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf
[43] Verizon. (2017). Data Breach Investigations Report. Available at: https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf
[44] Center for Strategic and International Studies (CSIS) / McAfee. (2014). Net Losses. Estimating the Global Cost of Cybercrime. Available at: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf
[45] FireEye/Marsh & McLennan Companies, Inc. (2017). Cyber Threat: a perfect storm about to hit Europe. Available at: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-world-eco-forum.pdf
[46] Massimo Pellegrino. (2015). The threat of state-sponsored industrial espionage. EUISS. Available at: https://www.files.ethz.ch/isn/191348/Alert_26_Industrial_espionage.pdf
[47] Baker McKenzie. (2017). The rising importance of safeguarding trade secrets. Available at : https://www.bakermckenzie.com/-/media/files/insight/publications/2017/trade-secrets
[48] AIVD. (2016). Annual report 2016. Available at: https://english.aivd.nl/publications/annual-report/2017/04/04/annual-report-2016
[49] AIVD and MIVD. (2017). Cyberespionage: are you aware of the risks? Available at: https://english.aivd.nl/publications/publications/2017/10/26/publication-cyberespionage-are-you-aware-of-the-risks
[50] Centro Nacional de Inteligencia. (2017). Cyber-Threats and Tendencies 2017 edition. Available at: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2249-ccn-cert-ia-16-17-cyberthreats-trends-2017-executive-summary-1/file.html
[51] UK Government. (2015). UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf
[52] European Internet Organised Crime Threat Assessment (IOCTA). Internet organised crime assessment. Available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment
[53] Among EU Member States, the manufacturing sector has been the most targeted at all in 2016, taking into consideration the following countries: Germany, the UK, Belgium, Spain, Denmark, Sweden, and Finland. Data available at: FireEye/March & McLennan Companies, Inc. (2017). Cyber Threat: a perfect storm about to hit Europe? Available at: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-world-eco-forum.pdf; and Verizon. (2017). Data Breach Investigations Report. Available at: https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf

- Health and medical technology.

The 2018 Verizon Data Breaches Investigation Report states that cyber espionage in the public sector constitutes up to **77%** of all cyber intrusions.[54] The reports includes in this sector 22,788 cyber espionage incidents in 2017, out of which 304 with confirmed disclosure of data.

An interesting evolution is the rise of academia and research centres as targets. EUROPOL states that sensitive data sources, such as from the healthcare sector, will increasingly be targeted.[55] In some areas where there has been decade-long research, testing and approval cycles, targeted attacks to exfiltrate such data sets are likely to increase.[56]

Some national level cybersecurity reports provide additional evidence to understand the problem.

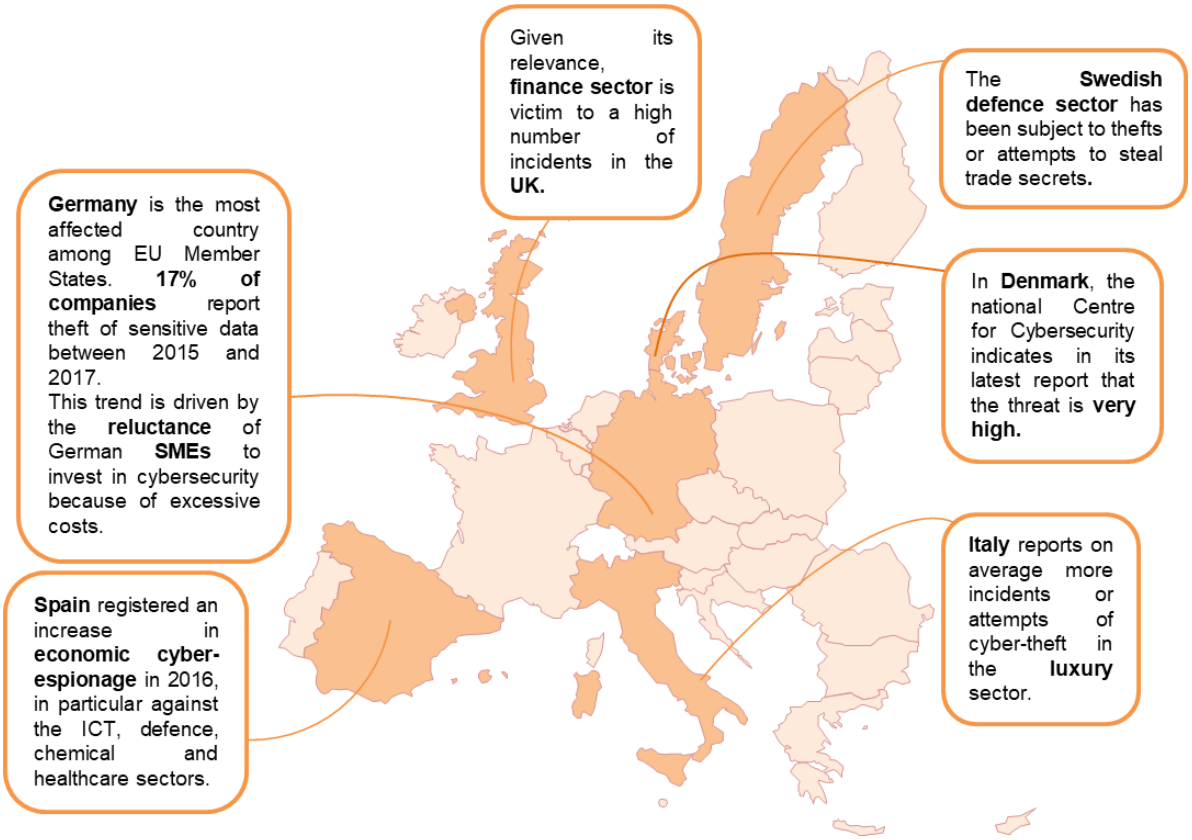


Figure 3 – The geographical distribution of incidents

In Europe, **Germany** appears to be the most affected country by the increase in the number of cyber thefts of trade secrets. Bitkom, an association including more than 2,500 IT companies, surveyed its members over a period of two years, revealing that 53% of them suffered from economic espionage. Moreover, 17% of companies surveyed reported that sensitive data was stolen between 2015 and 2017 and 11% reported theft of intellectual property and industrial confidential information.[57]

[54] Verizon. (2018). Data Breach Investigations Report. https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf Instead, the 2017 Verizon Data Breaches Investigation Report identified manufacturing as the most sector most affected by cyber-espionage, totalling up to **94%** of all cyber intrusions.

[55] EUISS. (2015). The threat of state-sponsored industrial espionage. Available at: https://www.files.ethz.ch/isn/191348/Alert_26_Industrial_espionage.pdf.

[56] Europol. (2016). IOCTA 2016 Internet Organised Crime Threat Assessment. Available at: https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf

[57] Bitkom (2017). Wirtschaftsschutz in der digitalen Welt. https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/07-Juli/Bitkom-Charts-Wirtschaftsschutz-in-der-digitalen-Welt-21-07-2017.pdf .[57] This report

In **the Netherlands**, cyber theft of trade secrets affects both the economic and political realm, carried out generally by state-sponsored actors. The Cyber Security Assessment of the Dutch Ministry of Security and Justice identifies industrial espionage conducted by companies as stable and not posing a threat,[58] while includes state-sponsored espionage among the threats described as "expedient". Besides, the report underlines that two-thirds of affected companies were not aware of these attacks up to the moment of notification by intelligence services. [59]

The **Danish** centre for cybersecurity's report informs in a dedicated section about the very high level of threat represented by cyber espionage, particularly against research-intensive and high-tech industries. Nevertheless, activities are described in generic terms and the attacker is generally described as a state-sponsored actor. Despite the report includes industrial espionage in its analysis, it does not provide any data.[60]

In **Finland**, "technology companies engaged in R&D and the business that serve them are the most vulnerable to cyber espionage".[61]

The **Belgian** University of KU Leuven surveyed 181 companies. Among those who suffered a data system interference, in both data collection periods[62], the victimisation rate of cyber espionage has increased from 3.6% in the first wave to 10.6% in the second wave (+7%).[63]

The **Estonian Information Security Authority's report** provides a list of sectors identified as main targets of cyber industrial espionage (energy, ICT, chemical, and biotech sectors) and another one with sectors more exposed to state-sponsored cyber espionage (strategic companies and service providers).[64]

The **Spanish** national centre for cryptology's report provides a specific section describing the increase in economic cyber espionage in the course of 2016, with an increased level of intrusions in IT, defence, chemical, energy, and health sectors. The report considers political cyber espionage as the main threat in the EU and Spain, and apparently, the major number occur during international negotiations. [65]

The **Italian yearly Clusit report** on Security of Information identifies cyber espionage (geopolitical and industrial inclusive of IP theft) as a relevant threat, with a **growth rate of 46% from the previous year**. It indicates how recent EU legislations on cybercrime has increased **the level of awareness among businesses** and the public administration.

Stakeholder engagement: Stakeholders confirmed the same findings from the literature review concerning the most impacted sectors (manufacturing sector, information and communication technologies; financial and insurance activities; health and medical technology) but mentioned repeatedly that also research organisations are targeted.

Stakeholder engagement: Interviewed stakeholders stressed the fact that in all sectors the threat becomes particularly damaging if the targeted company focuses extensively in R&D. In particular, large companies and those operating in specific sectors, such as finance, insurance, and critical infrastructure are those with the highest level of awareness,

focuses on the analysis of the cyber-espionage against German businesses and includes information on the nature of the attackers, the typology and quantitative entity of damage to the industrial sector, as well as the geographical origin of the attacks.

[58] The source refers to "stable" as "no phenomena recognised that poses a threat". Ministry of Security and Justice, National Coordination for Security and Counterterrorism – Cyber Security Assessment 2017

[59] National Cyber Security Centre. (2016). Cyber Security Assessment Netherlands csan 2017. Available at: https://english.nctv.nl/binaries/CSAN2017EN_Web_tcm32-278746.pdf

[60] Danish Centre for Cyber Security – The cyber threat against Denmark 2017

[61] Finnish Security Service Intelligence (2017). SUPO 2017. Available at: http://www.supo.fi/instancedata/prime_product_julkaisu/intermin/embeds/supowwwstructure/75373_Supo_2017_ENG_www.pdf?a393b24bf98ed588

[62] Data collection periods: First Wave (June-August 2016), Second Wave (November 2017- February 2018).

[63] Letizia Paoli, Jonas Visschers, Cedric Verstraete & Elke van Hellemont (2018), The Impact of Cybercrime on Belgian Businesses, available at: https://bcc-project.be/surveys/industry-survey-final-report-31082018.pdf

[64] Republic of Estonia, Information System Authority. Annual Cyber Security Assessment 2017.

[65] National Cryptology Centre - Cyber threat and tendencies, 2017 Edition

due to the fact they have been among the first victims of this unlawful activity. Companies in the retail and manufacturing sectors and SMEs in general demonstrate much lower awareness on the issues.

Stakeholders highlighted how hackers might modify their *modus operandi* depending on which sector they are targeting, or even the Member State in which a targeted company is located. For example, the financial sector is one of the most targeted ones, mainly through theft of credentials allowing cyber criminals to access important trade secrets, such as negotiation details for company acquisitions. Moreover, consulting firms are also not immune to the risk, especially if they operate in the high tech/ICT sector or in the execution of mergers and acquisitions.

The geographical distribution of incidents varies across Europe as well. For example, stakeholders highlighted that in **Italy**, **luxury industry** represents a sector particularly targeted, given the country's solid reputation in this field, while in the **UK** the most targeted sector would be **finance**. In **Denmark**, various **IT companies** suffer the theft of sensitive data, in particular in reference to an attack, which began in 2010 originating in China. In the **Netherlands**, companies in different industry sector such **Energy**, **Hi Tech** and **Chemical**, are suffering cyber espionage the most.

Shipping is another targeted sector. **Europe alone represents one third of the entire shipping industry**. Many systems digitally controlled that can be hacked in a ship, for example, the cooling systems or the air conditioning systems. The kind of cyberattacks conducted against the maritime sector are: 77% malware, 57% phishing campaign, 23% spear-phishing campaign. The kind of data stolen are personal data and operational data (e.g. route plans, next ports, supplies to be ordered, fuel orders, etc.). The kind of data stolen are often personal data but also operational and sensitive data (e.g. route plans, next ports, supplies to be ordered, fuel orders, etc.). Despite the shipping industry being important, most of the companies operating in this sector are SMEs, which could suffer the rapid growth in digitalization.

6.1.5. Cyber Theft in the SME Environment

Literature review: SMEs tend to underestimate the potential threats of cyber espionage and mistakenly believe risks only apply to nation states and large multinationals. This false sense of security can result in businesses taking an overly relaxed attitude to protecting their systems and data – making it easier for cyber-spies to launch their intrusions.[66]

The fact that SMEs operate on a smaller scale means that they should approach the threat of cyber espionage in a specific manner. SMEs hold peculiar advantages and disadvantages in combating cybercrime. The **low budget** and **lack of awareness** are undoubtedly the main disadvantages, but at the same time, as opposed to large companies, they can leverage on **greater flexibility** as they face less bureaucratic constraints and have the opportunity of taking **direct action** in order to correct problems.[67]

Today, **96.5%** of all SMEs in advanced economies store some form of business data digitally. A considerable amount of intellectual capital and know-how is already digitised and stored online. "SMEs are very attractive targets for cyber criminals. No matter the nature of a SME's economic area, every company is seen as a lucrative target".[68] Hackers are attracted not much by the gain that they can make but mostly but rather from the minimal effort needed to access SMEs' confidential data.[69]

[66] Kaspersky Lab. (2013). Who's spying on you? No business is safe from cyber-espionage.
[67] UNICRI. (2015). Guidelines for IT Security in SMEs. http://www.unicri.it/news/files/Research-Guidelines_for_IT_Security_of_SMEs-Flavia_Zappa_FINAL.pdf
[68] UNICRI. (2015). Guidelines for IT Security in SMEs. Available at: http://www.unicri.it/news/files/Research-Guidelines_for_IT_Security_of_SMEs-Flavia_Zappa_FINAL.pdf
[69] UNICRI. (2015). Guidelines for IT Security in SMEs. http://www.unicri.it/news/files/Research-Guidelines_for_IT_Security_of_SMEs-Flavia_Zappa_FINAL.pdf

Furthermore, cyber criminals often view SMEs as an entry point for intrusions against larger businesses. Many smaller businesses enjoy 'trusted partner' status with high profile enterprises – and criminals are increasingly keen to exploit those relationships. The so-called "**supply chain attack**" is one of the three most used techniques hackers put in place when penetrating an IT system.[70] "Attackers have found it increasingly difficult to break into big companies' networks. By hacking into smaller companies' networks, the attacker leverages on the small companies' knowledge and identities to break into bigger enterprises."[71]

Studies carried out in Germany, Italy and the UK have shown how these three countries and their SME economies are commonly targeted by cyber thefts of trade secrets.

German SMEs - which amount to 3.5 million businesses and produce more than half of the country's economy - have been reluctant to invest in cybersecurity to protect against thefts and other cyber intrusions, because of significant costs they cannot face. This has been one of the main drivers in the increase of cyber intrusions in the country.[72]

In **Italy**, according to sectorial studies, SMEs represent a favourite target for hackers: **71% of all data breaches**, aimed primarily at fraudulent acquisition of knowledge and intellectual property, are against companies with less than 100 employees. Italian SMEs are an important part of the national economic system, both for their large number - they represent over **90% of the Italian industrial fabric** - and for the wealth of skills that characterizes them[73].

In the **UK, one in four firms** operating in the UK's knowledge-based economy has suffered a breach of intellectual property in the timeframe between 2011 and 2016, according to the Federation of Small Businesses (FSB)[74]. FSB's study illustrates how important identity and ideas are to a firm's bottom line, with almost one in three (30%) of the small businesses surveyed that own some form of intellectual property rights stating they are dependent on it for **75% to 100% of their revenue**.

***Stakeholder engagement**:* As highlighted in the literature review, stakeholders report that SMEs are more exposed than large companies to the threat of cyber theft of trade secrets. There are various reasons for this:

- SMEs do not fully understand and consider the threat;
- SMEs do not have enough economic funds to invest in cybersecurity;
- SMEs do not have sufficient know-how, expertise and technologies to prevent cyber intrusion.

The **85% of stakeholders** interviewed noted that SMEs consider themselves too small or insignificant to be a target of cyber theft of trade secrets. Lack of awareness combined with limited resources to be invested make them very vulnerable to cyber thefts. Compared to other areas, SMEs in Southern Europe are seen by stakeholders as neither aware of the problem, nor as having the fundamental technological measures to protect themselves. Furthermore, employees in small companies often lack direct cybersecurity training, as for SMEs it is already difficult to have specialized IT human resources. The maturity level of cybersecurity for SMEs is **very low** and hackers are aware of it; theft of trade secrets in these cases becomes much easier.

[70] The Council of Economics Advisers (2018). The Cost of Malicious Cyber Activities to the US Economy. Available at: https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

[71] Kaspersky Lab. (2013). Who's spying on you? No business is safe from cyber-espionage. Available at: https://media.kaspersky.com/en/business-security/kaspersky-cyber-espionage-whitepaper.pdf

[72] The Wall Street Journal (2017). Hit by Chinese Hackers Seeking Industrial Secrets, German Manufacturers Play Defence. Available at: https://www.wsj.com/articles/hit-by-chinese-hackers-seeking-industrial-secrets-german-manufacturers-play-defense-1506164404

[73] http://www.leonardocompany.com/-/cyber-risks-intellectual-property

[74] http://www.jelfsmallbusiness.co.uk/business-network/blog/2015/08/2016/10/smes-struggling-to-protect-intellectual-property/

Indeed, stakeholders look at supply chain as one of the most common environments where cyber theft can occur and spread among different companies. Even when a large company adopts the most stringent cybersecurity policies and the most advanced technological tools, a weak link in the chain (usually, a SME) is probably sufficient to nullify any kind of effort and investment.

For example, in 2017, CCleaner suffered a massive **supply-chain malware attack**, where hackers compromised the company's servers for more than a month and replaced the original version of the software with the malicious one. This led to 2.3 million devices being infected and 20 High Tech companies targeted (e.g. Google, Microsoft, IBM, Cisco etc.).

The fact that SMEs are so vulnerable to the threat of cyber theft of trade secrets impairs the resilience of larger enterprises.

KEY FINDINGS

- **The threat is concrete. Without undertaking deliberate and focussed action, the threat of cyber theft of trade secrets is expected to become even greater in the future.**
- **Europe is a primary target of cyber theft of trade secrets, due to its expertise and knowledge in key industrial sectors. The most affected sectors are:**
  - **Manufacturing;**
  - **Information and communication technologies;**
  - **Financial and insurance activities;**
  - **Health and medical technologies.**
- **In 2016, 289 cyber theft of trade secrets followed by disclosure of data were registered in Europe (Verizon, 2017).**
- **The time-lag between intrusion and detection registered in Europe is three times longer than in the rest of the world: 469 days against an average of 146 (FireEye, 2017).**
- **Annual losses from cybercrime targeting trade secrets are estimated to be between $50 billion and $60 billion globally (McAfee, 2018), resulting in a loss of competitiveness, jobs and reduced R&D investments. 289,000 jobs could be at risk in Europe (ECIPE, 2017), rising to one million jobs by 2025.**
- **Direct costs are only around 10% of costs the companies will have to face. The remaining 90% of costs depends on indirect impacts and they are recorded only after five to six years.**
- **Cyber espionage methods and techniques employed by the perpetrators have become increasingly sophisticated and businesses are not aware of the threat.**
- **The types of perpetrator are changing: competitors and hacktivist groups are followed by state-sponsored actors.**
- **SMEs are more exposed than large companies to the threat of cyber theft of trade secrets.**
- **SME budgets for cybersecurity are generally inadequate to implement required mechanisms and tools. This, together with lack of awareness, represent undoubtedly the main disadvantages.**

6.2.Prevention, Mitigation and Reporting

6.2.1. Risk Management and Adoption of a Multi-disciplinary Approach to Develop Cyber Theft of Trade Secrets Frameworks

Literature review: A poor risk management strategy influences the overall security of a company and can potentially lead to higher vulnerability to cyber intrusions. Jahner and Krcmar more than ten years ago promoted **risk culture as an essential component of an integrated IT risk management.**[75]

In this sense, **cybersecurity frameworks** provide core controls and processes – such as **standards, guidelines, and best practices** – useful to companies for cyber risk management, and as a **cornerstone of a resilient enterprise.** [76] Cybersecurity frameworks help companies to introduce preventive actions in all possible aspects of their operations, from the adoption of specific policies and procedures to the employment of the most advanced technologies.

Although there is no common framework for cybersecurity in Europe, in the last few years some important initiatives have been undertaken at national level:

- The CIIP ("Critical Infrastructures Information Protection") Framework in France;[77]
- The "Cyber Assessment Framework"[78] in the UK;
- The "Esquema Nacional de Seguridad"[79] in Spain;
- The Italian National Cyber Security Framework[80] (Based on the NIST Framework[81]) in Italy.

However, the rate of adoption of these initiatives is still limited due to the fact that organisations are encountering major implementation problems when they try to use them. Organisations reported that they face significant challenges in trying to implement cybersecurity frameworks, according to a survey of 319 IT security decision makers[82]. Respondents identified a number of obstacles to cybersecurity framework implementation, including **lack of trained staff** (57%), **inadequate budget** (39%), **lack of prioritisation** (24%), and insufficient **management support**. At the same time, among organisations that adopted cybersecurity frameworks, **95% have seen benefits** from this.

To effectively implement a cybersecurity framework requires the involvement of company senior management and the engagement of all staff. Some reports point out an **increase in the level of risk awareness among CEO and management board** members in recent times.[83] This is partly attributable to the introduction of the **GDPR and NIS**

[75] S. Jahner, H. Krcmar (2005), Beyond Technical Aspects of Information Security: Risk Culture as a Success Factor for IT Risk, in: Association for Information Systems AIS Electronic Library, AMCIS 2005 Proceedings; Management

[76] Accenture. (2015) Making your Enterprise Cyber Resilient, available at: https://www.accenture.com/t20171108T100707Z__w__/us-en/_acnmedia/Accenture/Omobono/cyber-resilience/pdf/Accenture-Making-Your-Enterprise-Cyber-Resilient.pdf

[77] https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/

[78] https://www.ncsc.gov.uk/guidance/introduction-cyber-assessment-framework

[79] https://administracionelectronica.gob.es/ctt/ens#.W2mpktIzZPa

[80] Research Center of Cyber Intelligence and Information Security, Laboratorio Nazionale CINI di Cyber Security (2016), 2015 Italian Cyber Security Report, available at : http://www.cybersecurityframework.it/sites/default/files/CSR2015_web.pdf

[81] For further details, see Annex H. NIST. (2017). NIST Cybersecurity Framework. Available at : https://www.nist.gov/cyberframework

[82] https://www.hitachi-systems-security.com/blog/cybersecurity-frameworks-challenges/

[83] Mandiant / FireEye. M-TRENDS 2017 (2017), available at: https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

Directive,[84] but also to more frequent and sophisticated cyber incidents such as cyber theft of trade secrets.

The literature clearly identifies a number of fundamental approaches to cybersecurity addressed at companies and organisations to limit the risk or extent of damage from a cyber intrusion. **Five main areas** emerge from this analysis, as shown in the figure below:

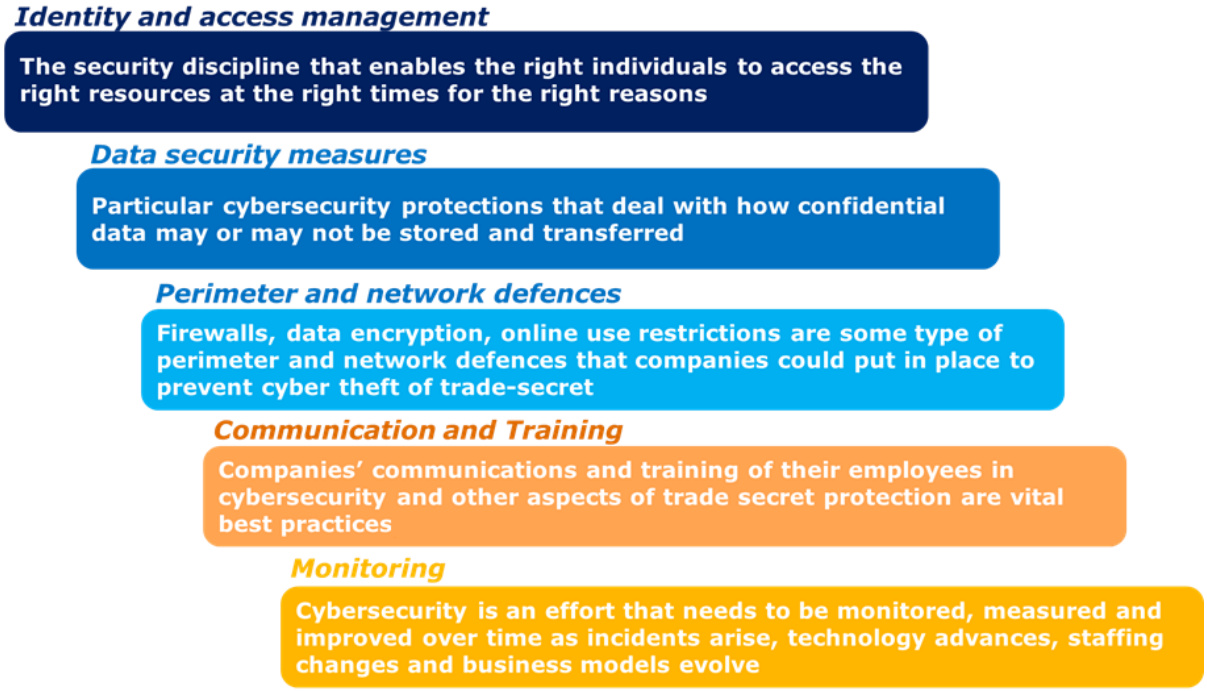


Figure 4 – Basic approach for cybersecurity

Recent reports published by ENISA and cybersecurity service providers[85] [86] [87] [88] include **specific mitigation actions countering cyber espionage and theft of trade secrets**.

Although intrusions are increasingly sophisticated, the RSA FirstWatch team believes that through understanding the basic cyber espionage attacker "blueprint" and commonalities noted between many advanced campaigns, organisations can create effective best practices for detection and response at both the host and network level.[89]

In detail, suggestions for security analysts include:

- Focussing on Configuration Management, which allows the defender to zero in on processes that do not fit the norm. These usually appear as friendly processes, but significant cues show that they are not legitimate;
- Knowing their network for quick detection of intrusion. This goes far past net flow, and ideally requires full session data and protocol detection to be effective;

[84] For more details on the NIS Directive, please refer to Annex F of this report.
[85] ENISA. (2017). Threat Landscape Report 2017 - Final Version 1. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017
[86] Kaspersky. (2013). Who's spying on you? No business is safe from cyber-espionage. Available at : https://media.kaspersky.com/en/business-security/kaspersky-cyber-espionage-whitepaper.pdf
[87] Symantec. (2017). ISTR – Internet Security Threat Report. Available at : https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf
[88] PwC. (2014). Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential threats. Available at: https://create.org/wp-content/uploads/2014/07/CREATe.org-PwC-Trade-Secret-Theft-FINAL-Feb-2014_01.pdf
[89] Alex Cox, (2012). The Cyber Espionage Blueprint: Understanding Commonalities In Targeted Malware Campaigns. RSA FirstWatch. http://www.emc.do/collateral/white-papers/rsa-cyber-expionage-blueprint-understanding-commonalities-targeted-malware-campaigns.pdf

- Looking at common processes running out of an atypical location;
- Investigating Random Filenames;
- Investigating Locations that provide "auto-run" capability after reboot;
- Paying close attention to the allowed paths in and out of your network;
- Analysing HTTP header information, which can reveal compromises, both by the presence of identifying information in the header fields, as well as inconsistencies in header information and construction;
- Reviewing Atypical Domains.

Companies do not yet have standard procedures to consistently or systematically identify or prioritise their trade secret portfolio, let alone consistent means to assess the economic impact of the loss of trade secrets.[90] PwC developed together with Create.org a **framework for the assessment of value of trade secrets**. The framework includes: (a) a direct method to estimate the lost future revenue and profitability associated with the theft of a trade secret, and (b) an indirect method evaluating the more intangible adverse impacts of such an event, as measured through various non-financial performance indicators. The framework identifies five main steps to protect companies from cyber theft of trade secrets:

Source: create.org

- Companies should document and locate the inventory of their trade secrets, aggregating them into main categories, (e.g. Product Information, Research & Development, Critical & Unique Business Processes, Sensitive Business Information, IT Systems & Applications);
- Clustering trade secrets also assists in managing the identification of vulnerabilities in the existing protocols that may create unnecessary risk and exposure for the company. The assessment of the maturity of the trade secret protection programme and the specific processes is an effective way to understand the vulnerabilities;
- As a further step, using value-based judgments on the relative importance of a trade secret, the identification of a Relative Value Ranking analysis allows the company to conduct a qualitative assessment. This leads to a selection of trade secrets that have the biggest impact on the operations and performance of the business. The value of trade secrets can be rank as 'low,' 'medium' or 'high', based on criteria such as the impact to the company's reputation, core business, culture, competitive advantage or future revenues;
- This process enables management to segment the total impact into manageable building blocks, allowing separating both direct and indirect impacts. This helps to establish a complete picture of the economic losses attributable to a trade secret theft;
- Through the analysis of trade secrets, company management is able to make informed decisions about how best to use its existing resources to strengthen its ability to mitigate potential threats. The main categories of effective trade secret protection include: Policies, Procedures & Records; Cross-functional Compliance Team; Scope & Quality of Risk Assessment; Management of Third Parties; Security

[90] PwC and Create.org (2014). Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential threats. Available at : https://create.org/wp-content/uploads/2014/07/CREATe.org-PwC-Trade-Secret-Theft-FINAL-Feb-2014_01.pdf

& Confidentiality Management; Training & Capacity Building; Monitoring & Measurement; Corrective Actions & Improvements.

A good strategy consists of a **multi-disciplinary approach**, using knowledge of their business alongside a likely cyberattack scenario to understand what actions may be required. Accepting valuation techniques to calculate the breach's true cost could provide business leaders with a more accurate depiction of a company's cyber risks throughout the response life cycle.[91]

***Stakeholder engagement*:** Stakeholders confirmed the view that there is no "silver bullet" in combating cyber theft of trade secrets. Being this the state-of-the-art, it is paramount to incorporate soft and hard assets. Intrusions within companies result in data being removed from the administrative level from either the virtual machine or the back-up in **99.9% of cases**. This alarming data provided by stakeholders should lead to a **change in cultural behaviour** within companies. Company decisions to introduce the use of long passwords makes them actually less safe, as long passwords are more deducible (e.g., employees tend to use their favourite football team or their children's name). Likewise, some stakeholders observed that rules are too lax when providing **administrator access** for employees, and the related removal. Others noted how knowledge of security protocols is not widespread across businesses and most of the time employees lack suitable tools to understand how cybersecurity (when in place) works within the company.

Protecting infrastructure through the adoption of effective measures is a primary objective, as it is the **strategic detection of possible intrusions**. Cyber intrusions are usually not detectable, as confirmed confidentially during the interviews with some national intelligence officials. This could be overcome by defining a specific role and identifying a **person responsible** for and dedicated to cybersecurity. Small size enterprises suffer a higher economic cost for investing in such a position; alternatively an existing employee compatible with the role could take in on, reducing the cost.

Stakeholders also recognised that the adoption of a cyber-strategy based on a risk assessment approach increments deterrence, detection and resilience and allows the company to readjust to rapid changes in the cyber world.

Supply chain risk management represents another crucial issue for companies, as all the constituent actors of the supply chain must protect trade secrets, given that **processes and procedures vary depending on the confidentiality and importance of the information involved**. Security must adapt itself to precise processes and procedures and a proper strategy must be able to cover all of them, cognisant of the supply chain.

As noted by more than one stakeholder, cybersecurity frameworks are a good tool to properly assess cyber risks and increase the maturity level of cybersecurity within a company or organisation; but are usually insufficient. The **adoption, implementation and support for a common cybersecurity framework,** as well as **providing guidelines and standards would be useful** for a number of reasons.

First, it should **include the provision of economic support**, which could be directed to companies or governments in order to increase spending on cybersecurity.

Frameworks and assessments at EU level should also address the need to **reinforce IT security training through the arrangement of accredited courses** as well as simulated cyberattack events designed to test IT system security and resilience. It was suggested that ENISA could be tasked with **designing a basic framework to strengthen IP protection for SMEs** that do not have the resources for complex security frameworks.

Both at the national and at EU level, intelligence agencies or forensic teams should be able to identify, through the framework, all the weaknesses of an IT system. A framework would be useless if it does not address the possibility to identify a ""zero day"" vulnerability. Most

[91] Deloitte (2016). The hidden costs of an IP breach: Cyber theft and the loss of intellectual property. Available at: https://www2.deloitte.com/insights/us/en/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html

cyberattacks happen because of these vulnerabilities; therefore, a cybersecurity framework would be useful to increase the cybersecurity maturity level but not to discover weaknesses. It is important to note that cyberspace is a dynamic environment that needs a "real time" response.

Nevertheless, stakeholders were keen to highlight that too many standards could create confusion and some concerns, particularly among SMEs. Indeed, the lack of IT personnel in the SME environment makes difficult the understanding of standards and frameworks. Moreover, the implementation of standards is often very expensive compared to the available budget of SMEs.

A risk assessment, taking into consideration all of the controls available, should lead the company to review its policies and adopt **new technologies**.

In line with findings from the literature review, stakeholders suggested the adoption, as basic cybersecurity measures, national and international standards (i.e. ISO27001, ISO27002 etc.), cybersecurity frameworks and **encryption methods** (i.e. encryption of disks where sensitive information is stored or for confidential information shared via e-mail). These measures generate direct positive impact on the fight against cyber theft of trade secrets. Additionally, another suggestion was the implementation of an EU research programme to develop a non-static algorithm. In fact, this kind of algorithm is more secure, compared to static ones, resulting in a higher level of security for those enterprises adopting it. Moreover, the algorithm could be implemented through a framework, which would provide direction on instruments and scalability.

The adoption of appropriate technological tools and mechanisms would assist companies in increasing the possibility **to identify a cyber intrusion** and multiply the possibilities to collect intrusions traces in the system (**log and monitor marking**). **Intrusion detection tools** remain the top priority and basic step in the prevention strategy to fight cyber theft of trade secrets for companies.

Advanced technological solutions allow **company infrastructure** to better resist an intrusion. Solutions suggested by interviewed stakeholders comprise: the adoption of Security & Privacy by design and Privacy by default, Regular penetration testing activities, Intrusion Detection Systems and Anomaly based Detections Systems, adoption of Security Operations Centre, Cybersecurity Knowledge/Processes/Training programme.

IT specialists tend to look more at innovative technologies rather than simply at cybersecurity tools, that can support the development of more sophisticated protection measures, such as **self-evaluating systems** of the protection level for companies. This should be made scalable – as cybersecurity needs of SMEs are different from that of global enterprises, as well as across sectors: not all sectors suffer from the same kind of threat and method of cyberattack.

6.2.2. Investments to Prevent Cyber Theft of Trade Secrets

***Literature review**:* Companies that carry out a sound risk assessment are better positioned to prioritise investments and protect their trade secrets more effectively. Such an assessment allows businesses to appropriately balance investments in cybersecurity with efforts to develop better threat visibility, and the ability to respond more rapidly and more effectively in the event of a cyber incident.[92]

In terms of numbers, Morgan Stanley estimated in 2016 that spending on cybersecurity products and services would more than double from **$56 billion in 2015** to **$128 billion in 2020**.[93]

[92] Deloitte, "Beneath the surface of a cyberattack - A deeper look at business impacts"
[93] Morgan Stanley. (2016). Cybersecurity: Time for a Paradigm Shift. Available at: http://www.morganstanley.com/ideas/cybersecurity-needs-new-paradigm

The literature review on this topic identified a **comprehensive theoretical approach** and offers a variety of **models** to determine the optimal level of **cybersecurity investment** for organisations. Gordon and Loeb developed one of the first models focussing on information security investments. In their view, a company achieves an optimal investment level by comparing expected benefits of the investment and the associated costs, with the investment increasing at the growth of the threat.[94] Moreover, organisations can reach a point at which information becomes so vulnerable that the highest level of security can no longer be justified from an economic point of view. However, the **model assumes the possibility to anticipate all necessary information on threats and consequences of intrusions,** which rarely occurs especially in the case of theft of trade secrets.

To properly invest in cybersecurity for the protection of trade secrets it is necessary that a company knows its value.

The approach incorporates inputs on threat actors, probability and severity of incidents, organisational protections and vulnerabilities, and future trends analysis that companies should consider. These inputs drive **the economic impact of a trade secret theft event** and are important elements that companies should factor into their assessment of how to protect their trade secrets. An assessment procedure on the impact of cyber theft of trade secrets leads the way towards the creation of aggregate data fostering future national level estimate.

The literature revealed one more important factor influencing the decision-making process for investing resources in cybersecurity – **occurrence of intrusions**. Unless a company itself or another company in the same sector or in the supply chain is attacked or suffers from a cyber-related incident, **spending on cybersecurity can be seen by a management board as unnecessary**.[95] The **incident can** relatively easily **change the minds** of the relevant management board members and result in additional budgets focussed on improving cyber resilience.

However, it should be noted that it is **not possible to achieve complete protection no matter how much money a company invests in cybersecurity**. There is always a chance of intrusion through a previously unknown vulnerability. Thus, experts recommend monitoring constantly the importance of data considered as confidential information and crucial for the company's development and core business activities. For that which cannot be protected companies should not write it down, at least not on anything that is connected to the internet."[96]

Governments generally provide for different supporting measures for companies, ranging from executing regulatory prerogatives to offering financial aid to foster strategic investments. In recent years, an overwhelming number of Member States have updated their National Cybersecurity Strategies. The objectives of these new strategies are to increase economic and social prosperity, and to provide protection against cyber threats. More specifically, **partnerships with industry**, **economic drivers**, and **incentives** are prioritised, including **public private partnerships (PPPs)**, identification of critical business actors and sectors to the economy, creating **cyber insurance**, and **creating technological independence** in cybersecurity.[97]

Stakeholder engagement: A number of **factors** motivate decisions relating to investment in cybersecurity for the protection of trade secrets; stakeholders confirmed the literature review findings on company investment needs and the pivotal role of government in supporting strategic company decisions for investments. In addition, stakeholders

[94] L. Gordon, M. Loeb, (2002). The Economics of Information Security Investment.
[95] N. van der Meulen, (2015), Investing in Cybersecurity, RAND Europe, at: https://english.wodc.nl/binaries/2551-full-text_tcm29-73946.pdf
[96] Søilen, K. S. (2016), Economic and industrial espionage at the start of the 21st century–Status questions. Journal of Intelligence Studies in Business, 6(3).
[97] CCDCOE (2015). Economic Aspects of National Cybersecurity Strategies. Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/Economics%20of%20cybersecurity.pdf

reported that in some cases, CISOs and CSOs are concerned about the lack of **consciousness at management level** of their own companies regarding **the need to invest more in robust security measures.**

Stakeholders supported measures such as the possibility of compensating companies, and SMEs in particular, by **providing funding, incentives or tax reliefs**. This entails using this issue as an opportunity to raise awareness and at the same time increase investments.

Some stakeholders recognised the positive consequences of a "**technology/IT welfare**", which allows companies access to basic technologies to protect critical and secret information. Companies are able to purchase cybersecurity services and technological tools increasing cybersecurity maturity and generating employment. An interesting proposition, as described by one stakeholder, would be the provision of incentives to companies and governments in setting up and implementing **Vulnerability Assessment Systems**. Moreover, **PPPs** were described as a way to provide incentives that would enable companies to improve their reputation and receive certifications. In this regard, the Netherlands created a public-private cooperation environment, such as a platform in which central government, regional, local and private partners - including critical infrastructures - can cooperate.

6.2.3. Awareness and Training

Literature review: the literature review highlights the important role that awareness plays among employees in tacking cybersecurity issues and cyber theft of trade secrets.

In fact, companies need to embrace an overall mentality change **raising awareness among their own employees** emphasising the importance of training at all levels. Security awareness training for employees is expected to become a **fundamental cyber defence strategy**.[98] This effort must include all employees: from training newly hired employees including education on cyber risk best practices, to ongoing security education for more seasoned employees. Training and awareness-raising activities can have **fundamental impacts on the volume and severity of cybercrime**.

Moreover, there is a **scarcity of professionals** trained in cybersecurity aspects and a need to create capacity in this area and develop a pipeline of talent. Frost and Sullivan esteemed the need for Europe to educate 350,000 cybersecurity professionals by 2022, to prevent a possible shortage.[99]

A good way of raising awareness among senior management is to run an attack simulation with them[100] to ensure a company's processes are suitably robust in the event of an attack. Interestingly a cyberattack on a company can have a positive impact on the general awareness of cybersecurity among employees. About 38% of attacked companies increased security awareness training among employees; and 37% said they increased their focus on risk analysis and mitigation.[101] The EC has also pointed out the need for companies to promote cybersecurity awareness at all levels, both in business practices and in the interface with customers. Industry should reflect on ways to make CEOs and boards more accountable for the provision of cybersecurity.[102]

---

[98] Marsh & McLennan. (2018). MMC Cyber Handbook 2018, available at: https://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/mmc-cyber-handbook-2018.pdf

[99] Frost & Sullivan. (2017). 2017 Global Information Security Workforce Study, available at: https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf

[100] Institute of Directors, Cyber Security: Ensuring business is ready for 21st century, 2017, at: https://www.iod.com/Portals/0/PDFs/Campaigns%20and%20Reports/Digital%20and%20Technology/Cyber-Security-21stcentury.pdf?ver=2017-03-24-141846-840

[101] Cisco, (2017), Annual Cybersecurity Report; at: https://www.cisco.com/c/dam/m/digital/1198689/Cisco_2017_ACR_PDF.pdf

[102] European Commission, Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Cybersecurity Strategy of the European Union: An open, Safe and Secure Cyberspace;

***Stakeholder engagement*:** It is important to properly prepare the European industry to counter upcoming cyber espionage campaigns. Raising awareness seems to be the **key measure** characterising an effective strategy to tackle cyber theft of trade secrets, as pointed out by stakeholders at both company and national level. When asked about the most effective measures and policies that a company may enact to face the challenge of cyber theft of trade secrets, the preferred option (25% of stakeholders), was the provision of **training and capacity building on the issue.** This is due to the fact that a large amount of cyber thefts of trade secrets stem from a lack of awareness of security measures among employees.

Stakeholders generally recognised the **need to increase awareness** at management level. This may have a pivotal role, such as enhancing the role of CIO and CISO and hiring valuable professional resources able to keep the cybersecurity system updated and effective. This reduces the vulnerabilities to unsophisticated external threats, such as phishing. At the same time, management should be made aware of the importance of building a solid internal security education. This proves particularly true when it comes to **SMEs. Small businesses** do not have IT Departments; they rely on external advisors only. A **good strategy** could be at first to **raise awareness on what trade secrets are** and to make SMEs aware of the importance of the information they own. Then it would be useful to work on an **easy and simple wording to disseminate basic rules** on cybersecurity measures to protect information and supply chain IP and trade secrets. An interviewee stated that technological tools are not sufficient on their own to protect a company, which must be dynamic, and able to adapt itself to the rapid changes in the cyber world. Given the high quantity of threats, (i.e. a computer virus production rate is roughly one every six seconds), **company employees need continuous training** about correct behaviours to be adopted in managing information and working on data that could be subject to cyber theft. In the long-term, this approach produces an economic advantage, considering the training as an investment in information security.

In addition to continuous training for employees, there are several ways to foster awareness. One is **providing content and material** related to capacity building and employee training, increasing the knowledge on the risks and encouraging investments in cybersecurity. Stakeholders also underlined the need to raise awareness among policy makers at all level of governance. The EU could coordinate with large companies so that their communication and lobbying capabilities may raise governments and national authorities' awareness on the topic.

Stakeholders also stressed the importance of making companies **aware of the national Computer Emergency Response Team (CERT) role** to ensure incident reporting, as well as disseminating information on law enforcement and judicial tools. Awareness improvement initiatives should not only target companies as government and international organisations themselves have limited knowledge and policy action is often lagging behind. Therefore, courses/events, a **platform** containing training and capacity building material should be in place not only for employees but also for policy makers, the judiciary system and society as a whole.

6.2.4. The EU Policy Background and its Coordination Action

***Literature review*:** The legislative accomplishments of the EU on protection of trade secrets come down to the 2016 EU Directive for the "Protection against the unlawful acquisition of undisclosed know-how and business information (trade secrets)".[103] The Directive harmonises the definition of trade secrets in accordance with existing internationally binding standards (more notably the 1994 TRIPS

[103] European Commission. (2016). Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

Agreement).[104]Additionally, the Directive includes civil law remedies to victims of trade secret misappropriation can seek protection. These are:

- Court orders prohibiting the use and further disclosure of misappropriated trade secrets;
- The removal from the market of goods that have been manufactured on the basis of a trade secret that has been illegally acquired;
- The right to compensation for the damages caused by the unlawful use or disclosure of the misappropriated trade secret.

However, cyber theft of trade secrets raises additional challenges to ordinary cases of trade secrets disputes. In all likelihood many companies do not realise they are being spied upon and even when they detect an intrusion, attribution remains extremely challenging. Without identification of the perpetrator it is impossible to bring legal proceedings against them. In addition, many companies refrain from admitting publicly that they were victims of cyber theft. Therefore, the Directive must be complemented by other initiatives.

A unified approach for preventing and reporting on cyber thefts of trade secrets, and the need to create greater coordination among the actors involved, are among the main challenges. Some initiatives are paving the way for more engagement and successful actions by demonstrating how **cooperation on cybersecurity is important**. Four EU level organisations, (ENISA, EDA EUROPOL-EC3, CERT-EU) have recently signed a Memorandum of Understanding, which "aims at leveraging synergies between the four organisations, promoting cooperation on cybersecurity and cyber defence and is a testament to the trusted partnership that exists between these EU agencies."[105]

Outlook of the EU political stance on Cybersecurity

To tackle cybersecurity challenges the EU adopted the 2013 Cybersecurity Strategy of the European Union (EU Cybersecurity Strategy), the Network and Information Security (NIS) Directive, and Directive 2013/40/EU on attacks against information systems. This set of initiatives and instruments form the core policy response of the EU to the current cybersecurity challenges.[106]

The same year, the Commission's Communication 2016/410 "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry" presented measures aiming at strengthening Europe's cyber resilience system and to foster a competitive and innovative cybersecurity industry in Europe, with particular reference to the need to protect trade secrets from cyber intrusions.[107]

With regard to the **institutional set-up for cybersecurity**, three main agencies (ENISA, EDA and EUROPOL-EC3) and the CERT-EU are the core of the EU action.

The **2016-2020 ENISA Strategy** underlines that, by 2020, ENISA will act as focal point for EU Institutions, CERTs and national authorities collating, analysing and making available information on global cyber issues with a view to developing insights on issues of high added-value for the EU".[108] In the meantime **the European Parliament and**

[104] World Trade Organisation. (1994). Agreement on Trade Related Aspects of Intellectual Property Rights. Available at: https://www.wto.org/english/docs_e/legal_e/27-trips.pdf

[105] https://www.europol.europa.eu/newsroom/news/four-eu-cybersecurity-organisations-enhance-cooperation

[106] European Commission (2016). Brussels, 5.7.2016. Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry. Available at:

[107] European Commission (2016). Communication 2016/410 "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry". Available at: https://ec.europa.eu/digital-single-market/en/news/communication-strenghtening-europes-cyber-resilience-system-and-fostering-competitive-and

[108] ENISA (2016). ENISA Strategy 2016-2020. Available at: https://www.enisa.europa.eu/publications/corporate/enisa-strategy

the Council are examining a legislative proposal from the EC reinforcing the role of ENISA.[109][110]

In the same context, the Council has agreed its position on a **Common Cybersecurity Certification**, which creates a mechanism for setting up schemes for specific ICT processes, products and services.

The **European Defence Agency (EDA)** supports Member States in the development of their defence capabilities and cooperates in the area of cybersecurity and cyber defence.[111]

EUROPOL EC3 supports Member States law enforcement operations in response to cybercrime in the EU, coordinates prevention and awareness measures; carries out strategic analysis and develops standardised training.[112]

Finally, the EU decided in 2012 to set up a permanent **Computer Emergency Response Team (CERT-EU)** for the EU institutions, agencies and bodies. Other than functioning as a national CERT, it cooperates closely with CERTs in the Member States and beyond as well as with specialised IT security companies.

Several reports and studies highlight that protecting the private sector from economic espionage, sabotage and other threats is a **joint responsibility** between the government and industry. Building trusted relationships is a major consideration in encouraging organisations to report incidents and share information. Governments enhance industry cyber resilience by sharing threat and actual breach intelligence in real time with business as well as with other governmental organisations across the EU.

A well performing cooperation between national governments, law enforcement agencies, companies and sector specific information sharing mechanisms may lead to **major improvements on threat analysis and prevention initiatives, reducing the average time of response** to a cyber intrusion and thereby bolstering cyber resilience across Europe. A competitive European cybersecurity industry reduces the damage caused by cyber espionage. Set up by 17 organisations active in ICT, the European Cyber Security Protection Alliance (CYSPA) is a promising initiative aimed at increasing the capacity of industry to protect itself from cyber threats. Parallel to this, the European Organisation for Security (EOS), which is the leading European business organisation representing the private security sector, is well-placed to inform policy makers and facilitate dialogue between institutions and the security industry.[113]

Data collection brought together under the authority of a European Cybersecurity Coordination Platform is deemed to provide more widespread information and the establishment of more interoperability through a common taxonomy and a joint sharing mechanism.[114] Both business community and government bodies look at the EU, and

[109] ENISA (2017). European Commission proposal on a Regulation of the European Parliament and of the Council on the future of ENISA. Available at: https://www.enisa.europa.eu/news/enisa-news/european-commission-proposal-on-a-regulation-on-the-future-of-enisa

[110] http://www.consilium.europa.eu/en/meetings/tte/2018/06/08/

[111] https://www.eda.europa.eu/Aboutus/Missionandfunctions

[112] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

[113] Massimo Pellegrino, EUISS - The threat of state-sponsored industrial espionage. Available at: https://www.files.ethz.ch/isn/191348/Alert_26_Industrial_espionage.pdf

[114] European Parliamentary Research Service, European Parliament Building an Effective European Cyber Shield. Available at: http://ec.europa.eu/epsc/publications/strategic-notes/building-effective-european-cyber-shield_en

especially ENISA, positively due to their coordination role. [115,116,117,118,119] In this respect, the European Political Strategy Centre provides an extensive overview concerning the EU effort in "Building an Effective Cyber Shield", indicating how ENISA is expected to become in the next few years a "fully-fledged European Cybersecurity Coordination Platform, equipped with adequate resources and executive competences."[120]

The literature points at the advantages of governmental cross-border cooperation. At diplomatic level, some efforts were taken in negotiating bilateral cybersecurity agreements. One of the most notorious events was the US – China bilateral agreement (see Annex H) for further details).[121] This agreement provided a model for other similar treaties, thus paving the way for bilateral agreements between China and Australia and China and Canada[122]. Scott J. Shackelford suggests considering novel strategies to enhance cybersecurity such as using international trade law and particularly bilateral investment treaties (BITs) as a vehicle to mitigate cyberattacks and better protect trade secrets.[123]

Other forms of collaboration have been taking place among European CERTs. For instance, Denmark, Finland and Sweden, together with Iceland and Norway, collaborate through the Nordic National CERT Collaboration.[124] This includes technical cooperation and cybersecurity exercises to assess and strengthen cyber preparedness, examine incident response processes and enhance information sharing in the region.

[115] BSA (2015). BSA feedback on European Commission 'inception impact assessment' on the 'Proposal for a Regulation revising the ENISA Regulation (No 526/2013) and laying down a European ICT security certification and labelling framework'. Available at: http://www.bsa.org/~/media/Files/Policy/Data/08042017ResponseToCommissionRoadmapICTSecurityCertificationandLabelling.pdf

[116] Microsoft (2017). Microsoft Response to the European Commission's Proposal for a Regulation on ENISA and ICT Cybersecurity Certification Framework. Available at: https://ec.europa.eu/info/law/better-regulation/feedback/7992/attachment/090166e5b6f93d2b_en

[117] European Parliament and the Council. (2013). Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing regulation (EU) 526/2013, and on Information and Communication Technology and Cyber Security Certification ("Cybersecurity Act"). Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/670021/cyber_security_certification_.pdf

[118] London Stock Exchange Group. (2017). London Stock Exchange Group's response to the European Commission's proposal for a regulation on ENISA and on ICT cybersecurity certification. Available at: https://www.lseg.com/sites/default/files/content/documents/Regulatory/2017/Dcember/LSEG%20response%20to%20the%20European%20Commissions%20proposal%20for%20a%20regulation%20on%20ENISA%20and%20on%20ICT%20cybersecurity%20certification.pdf

[119] ANSSI (2017). The Ambition of European Union Member States on the 'Cybersecurity Cyber-package'. Available at: https://www.ssi.gouv.fr/en/actualite/the-ambition-of-european-union-member-states-on-the-cybersecurity-cyberpackage/

[120] European Political Strategy Centre (EPSC). (2017). Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level. Available at: http://ec.europa.eu/epsc/publications/strategic-notes/building-effective-european-cyber-shield_en

[121] ENISA. (2017). Threat Landscape Report 2017 - Final Version 1. Available at : https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

[122] See: Prime Minister of Australia, AUSTRALIA AND CHINA AGREE TO COOPERATE ON CYBER SECURITY. See also: Canada National Security and Intelligence, Joint Communiqué - 2nd Canada-China High-Level National Security and Rule of Law Dialogue. National Security and Intelligence. See also: Canada National Security and Intelligence, Joint Communiqué - 2nd Canada-China High-Level National Security and Rule of Law Dialogue. National Security and Intelligence.

[123] Scott J. Shackelford, Eric L. Richards, Anjanette H. Raymond, Amanda N. Craig. (2015). Using BITs to Protect Bytes: Promoting Cyber Peace by Safeguarding Trade Secrets Through Bilateral Investment Treaties. American Business Law Journal.

[124] https://www.msb.se/en/Tools/News/Nordic-cyber-security-exercise-was-conducted-in-Linkoping/

The US Strategy for Protection of Trade Secrets, a story in short:[125]

- In February 2013, the White House released its "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets." The strategy has five main pillars: 1. international engagement, including diplomatic messaging and use of trade policy tools 2. company-to-company sharing of best practices to reduce the risk of trade secret theft 3. investigation and prosecution of trade secret theft and increased information sharing between law enforcement, the intelligence community, and companies, 4. a review of U.S. legislation, 5. increasing public awareness of the risks of trade secret theft.
- The **Commission on the Theft of American Intellectual Property** estimated back in 2013 that the costs of trade secret thefts equate to 1% - 3% of US GDP per year;
- **National Institute for Standards and Technology** (NIST) established in 2013 a **policy framework** consisting in standards, guidelines, and best practices to manage cybersecurity-related risk, including cyber theft of trade secrets;
- In 2015, the FBI developed a **checklist for reporting on economic espionage and cyber theft of trade secrets**, which provides means to establish the economic value of the secret stolen and details necessary measures to ensure the trade secret was duly protected. Although not meant as a comprehensive guide, it provides some specific questions that are a good starting point for businesses to consider when evaluating security controls;
- The **Obama Administration**:
  - Signed in 2015 the **Bilateral Economic Cyber-espionage Agreement** with the Chinese counterpart;
  - Issued the "**Defence Trade Secrets Act**" in 2016, which creates a private civil action against misappropriation of trade secrets;
- The Commission on the Theft of American Intellectual Property issued in 2018 an **update of the 2013 report**, which underlines how cyber theft of trade secrets might do the greatest damage to the US economy, among all form of economic espionage;
- In 2018, the **Trump Administration** issued:
  - A **"Memorandum on the Actions by the United States Related to the Section 301 Investigation"** stating that the Chinese Government is infiltrating US networks and stealing intellectual property, trade secrets, and confidential business information from US companies;
  - The May 2018 "**New strategy for cybersecurity and cyberattacks deterrence**" contains a report incorporating the **deterrence agenda** and an additional document, explaining the **Administration's international engagement strategy**.

***Stakeholder engagement*:** As cybercrime a global issue, stakeholders emphasised the need for **coordinated actions** in the fight against misappropriation of trade secrets through cyber means should be carried out at the highest level of governance.

As underlined by stakeholders, cyber theft of trade secrets is becoming more and more a matter of diplomacy. In this context, the European External Action Service (EEAS) presented in 2017 the "cyber diplomacy toolbox", a framework implemented in order to

[125] For more details, please refer to Annex H of this report.

push for a joint EU diplomatic response to malicious cyber activities, aimed at providing mitigation of cybersecurity threats and expected to encourage cooperation and facilitate mitigation against medium and long-term threats.

At national level, a constructive example of a coordinated policy at national level is the **UK National Cyber Security Centre** (NCSC). NCSC is the result of a consolidation of different UK government departments that now cooperate, working with many service/internet providers, issuing **guidance on overall security control and policies**. Through the NCSC the UK Government has been able to set **mandatory requirements** on cybersecurity for companies collaborating with it, and this could prove to be helpful with respect to cyber theft of trade secrets also.

Stakeholders emphasised how cooperation among key actors through the increased involvement of **business associations** would be beneficial in the prevention and mitigation of cyber incidents. This kind of collaboration could lower the likelihood of **reputational loss for businesses** and allow the sector to **learn from experience** and at the same time **receive an immediate notification of a breach** occurring in other companies. Building trusted relationships through cooperation is a major consideration in **encouraging organisations to report incidents and share information**.

6.2.5. Law Enforcement

***Literature Review*:** Cybercrime law enforcement needs to rapidly evolve to enhance prevention and mitigation measures. To this end, the EU is reinforcing its cybercrime legal framework (e.g., Directive on attacks against information systems, 2013; Framework Decision on combating fraud and counterfeiting, 2001).126

In fact, among the countries in scope, **legal protection and law enforcement of cyber theft of trade secrets is moving forward as Member States are transposing their specific laws to the EU Directive 2016/943**. **Sweden and Belgium** appear to be among the most legally advanced countries in the EU with ad hoc legislation on trade secrets.[127]

Countries such as **Austria**, **Germany**, **Poland** and **Spain** strongly rely on unfair competition law, while **Italy** and **Portugal** have specific provisions on the protection of trade secrets included in their respective Codes of Industrial Property. **France** has specific provisions on the protection of manufacturing trade secrets also included in its Code of Industrial Property. Tort law is also widely used to protect trade secrets, particularly in **the Netherlands**. In common law countries such as the **UK** and **Ireland**, lacking any specific legislation, trade secrets are effectively protected by the common law of confidence and by contract law.

It is also worth noting that in the majority of jurisdictions, **cases involving trade secret infringement are not heard by specialist judges**. Dedicated intellectual property specialised courts which also have jurisdiction (although not exclusive) in trade secrets cases have been established only in Italy and the UK.[128]

---

[126] Migration and Home Affairs, EU Commission, Cybercrime, available at: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en

[127] New Swedish Act on the Protection of Trade Secrets (2018), Revision of the Swedish Act on the Protection of Trade Secrets (1990). Available at: https://www.regeringen.se/490aa7/contentassets/ed33ca1388a447b594c394bff703b026/en-ny-lag-om-foretagshemligheter. English summary available at: https://www.lexology.com/library/detail.aspx?g=6d6a7ef5-a085-4fcc-b9f0-f3bd5edc1979
Adoption of the Belgian Act on the Protection of Trade Secrets (25 July 2018), https://www.linklaters.com/en/insights/publications/2018/july/adoption-of-the-belgian-act-on-the-protection-of-trade-secrets

[128] European Commission. (2013). Study on Trade Secrets and Confidential Business Information in the Internal Market. Available at: http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf

***Stakeholder engagement*:** In the course of interviews, stakeholders pointed out how law enforcement is fundamental to reduce the number of incidents across EU Member States. From a trade perspective, there are different aspects to be taken into account in reference to legal protection and law enforcement issues. Unfair competition can be conducted by domestic or international economic operators and sovereign states. In the former case, jurisdiction would most probably differ between the two states and international law would have to step in. International law **does not set any general rule** but provides the principles of **state sovereignty** and **non-intervention.**

One of the most critical question refers to whether economic espionage is violating the sovereignty of the state. Taking legal action in a domestic court could not be possible if the accused belongs to another State. Indeed, the accused State could rely on the possibility of **State immunity**. State immunity is a principle of international law that is often relied on by states claiming that a given court or tribunal does not have jurisdiction over it, or to prevent enforcement of an award or judgment against any of its assets.

In the context of international law, **Article 39 of TRIPS[129] (managed by the WTO)** states: "In the course of ensuring effective protection against unfair competition, Members shall protect undisclosed information in accordance with paragraph 2 and data submitted to governments or governmental agencies in accordance with paragraph 3. Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices…"

Therefore, considering Article 39, States who are member to the WTO are obliged to protect undisclosed information. In this context, when a state provides help or protection to the companies or organisations carrying out economic espionage, is it not infringing such obligation? There is potential to rely on Article 39. But to do so it **is important to have evidence**, which is very difficult to collect.

Therefore, given the problem of law enforcement in the international context, stakeholders pointed out how policy makers could tackle government supported cyber espionage by:

- **Unilateral action** – imposing economic sanctions (justification could be security threat);
- **Bilateral action** – including respective provisions in regional trade agreements similar to those in the new US-MEX-Canada agreement;
- **Multilateral action** – adopting code of conduct for governments to abstain from cyber theft or funding such theft.

6.2.6. Incident Reporting Schemes

The scarcity of available information on cyber theft of trade secrets raises the issue of whether there are sufficient mechanisms, and incentives, for business to report incidents.

***Literature review*:** The **NIS Directive**[130] requires Member States to set up National Computer Security Incident Response Teams (CSIRTs or CERTs) responsible for receiving, reviewing and responding to cybersecurity incident reports and activity. The Directive incident reporting protocol requires that organisations notify "without undue delay" CERTs and other relevant bodies about any significant security incidents encountered.[131] The EU Regulatory Framework for Electronic Communications also establishes compulsory **incident notifications**. However, such obligations are foreseen exclusively for operators

[129] https://www.wto.org/english/docs_e/legal_e/27-trips_04d_e.htm
[130] See Annex F - European Commission. (2016). Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union
[131] ENISA, Incident Reporting, https://www.enisa.europa.eu/topics/incident-reporting

of essential services and providers of electronic communications[132], **leaving aside all other companies** and organisations operating across the EU.

National CERTs act as **security point of contact (PoC) for the country.[133]** In most cases this role is fulfilled by the governmental CERT, which serves government and governmental agencies.

Not all the **CERTs** established across Europe are member of the CERTs network[134] and they do not report cyber incidents information in a standard manner at EU level through the Computer Emergency Response Team (CERT-EU).[135] **Significant differences** in the ways Member States transposed the Directive into their national legal frameworks caused the misalignment.[136] As underlined by the ENISA[137] report[138], national CERTs in the EU are in need of harmonisation of requirements, definition, terminology, and training opportunities.

A set of **best practices** have been formulated into a series of documents. Although these are not strictly related to cyber theft of trade secrets, they indicate the need to **maintain law enforcement aspects of cybercrime** in order to increase the quality of cooperation between National CERTs and Law Enforcement Agencies (LEAs).[139] Best practices that have been developed by CERT initiatives and forums regard the need to **establish a clear cooperation framework between National CERTs and LEAs**, making sure these are aligned with national regulations on investigations. Where frequent cooperation occurs, the national/governmental CERTs have been formalising the process by defining procedures to ensure that cooperation with law enforcement agencies follows a **formal, legal process**.

One of the key issues with CERTs is their proliferation and differences in reporting systems that confuse companies. Also, companies are generally not conscious of the **CERT's existence and of its powers**.[140] An awareness raising campaign may be beneficial. For example, in 2016 CERT Poland handled 1,926 incidents, 32% more than in 2015. This is a result of an **increasing awareness regarding the presence of CERT teams and their role in responding to incidents and threats**, as well as the direct cooperation of CERT Poland, together with an increasing number of entities and organisations.[141] Awareness raising of National CERTs is accompanied by the increase in trust and cooperation between Computer Response teams and businesses, in particular at sector level.[142] Also B2B platforms for information exchange are being considered.

***Stakeholder engagement*:** Stakeholders were asked to provide their views on the purposefulness of a specific reporting system for cyber theft of trade secrets.

The majority of interviewees considered positively the adoption of such a reporting system allowing for regular **information sharing on incidents.** On the contrary, some stakeholders perceive as difficult to implement such a system due to the company's **inability to detect the attack**, and the unwillingness to share information for **reputational reasons**. It is rarely the case where companies can demonstrate and be certain that the target of the attack was only to steal intellectual property.

---

[132] Regulation (EC) No 544/2009 of the European Parliament and of the Council of 18 June 2009 amending Regulation (EC) No 717/2007 on roaming on public mobile telephone networks within the Community and Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2009.167.01.0012.01.ENG

[133] ENISA. (2009). Baseline capabilities for national / governmental CERTs

[134] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map

[135] http://cert.europa.eu/

[136] https://www.enisa.europa.eu/topics/incident-reporting

[137] See Annex G for further details on the European Network and Information Security Agency (ENISA)

[138] ENISA. CERT Cooperation and its further facilitation by relevant stakeholders.

[139] ENISA (2012), Baseline Capabilities of n/g CERTs - Updated Recommendations 2012 available at https://www.enisa.europa.eu/publications/updated-recommendations-2012

[140] Baseline Capabilities of National/Governmental CERTs

[141] CERT Polska (2016), "The security landscape of the Polish Internet", available at: https://www.cert.pl/wp-content/uploads/2017/04/cert2016_ENG.pdf

[142] https://www.enisa.europa.eu/topics/csirts-in-europe/capacity-building

This is particularly true for SMEs. Indeed, stakeholders highlighted that **benefits** of a reporting system **differ** between the reporter and the *reportee*. In fact, many stakeholders understood the usefulness of having a critical mass of data in order to craft policies and have a better understanding of the problem.

However, from the **business** point of view, having to report information was perceived as a hurdle. For companies **reporting obligations means having to employ resources with related costs**. Therefore, companies need to clearly see a **tangible benefit**. By reporting criminal activities to public authorities, people expect a follow up otherwise there is no clear cooperation from citizens and companies. Companies report if they can have some degree of trust that their effort contributes to law enforcement.

Some of the stakeholders who agreed with a reporting system suggested making it **mandatory**, rather than having it on voluntary basis. As reporting is already mandatory for some cyber incidents, stakeholders discussed the advantages of extending the requirement **to trade secrets and IPRs** and should apply to all companies and organisations.

Some others believe in a **voluntary reporting system**. If it were to be kept voluntary, a **virtuous structure** would have to be put in place and incentives would need to be developed. These could be related to **timely information sharing.** Hence, public authorities would receive the report at the time of the attack and would communicate the ongoing threat to the affected businesses. Alternatively, incentives could be provided by the **dissemination of methods to prevent and respond to attacks**. Therefore, authorities would receive and share not only notification on the attack, but the tools and methods used by hackers and the ones adopted in response.

One central theme emerging from the stakeholder engagement is the **need to establish what information should be reported**. The reporting system could require information, for example, on the data stolen, the nature of attack experienced, the impact and the volume (if measurable) of consequences the company has suffered.

The possibility of leaning on **business associations** to create a platform for the exchange of information and whether the reporting should be **sector based** was another option discussed. Business associations **inspire enough trust** in companies, assisting in the realisation of a community among already engaged members with targeted communication. Such associations could function as a bridge between EU institutions and transfer information on attacks immediately, allowing for cross-border control as well as for a faster intervention of international police cooperation, when required or applicable. According to the view of one stakeholder, sectorial reporting could be implemented within national CERTs, in order to maintain sectors' sensitivity and requirements relevant, or implemented directly at law enforcement level.

Stakeholders identified two already existing reporting systems, which they suggested could serve the need to define a cyber theft of trade secrets reporting mechanism. An example of an existing reporting system is the **Automotive Information Sharing Analysis Centres (ISAC)**, which analyses intelligence about emerging cybersecurity risks to the vehicle, in order to collectively enhance vehicle cybersecurity capabilities across the global automotive industry.

Alternatively, an anonymously reporting platform on cyberattacks is already active for **maritime companies**.

Shipping and maritime companies often operate with vessels of other countries, which might not have a structured cybersecurity strategy in place. Anonymity has practical positive effects. In fact, this platform allows companies to anonymously report on incidents from any location, without incurring reputational and economic loss related to publicising information on the attack, and by employing a user-friendly system. Moreover, companies will benefit from the use of the platform as, through the collection of data, statistics can be developed to then help insurance companies assess the risk and develop insurance coverage for such events. The stakeholder suggested it could evolve into a proper pan-European, or even global, scheme.

The overall conclusion is that there seems to be little appetite from industry for the setting up of a brand new and horizontal reporting mechanism at EU level. The mere prospect of having a more solid factual basis for policy making at EU and national levels is not considered a sufficient incentive for individual companies to report incidents or attempts of trade secret theft by cyber means in a systematic way. A more feasible approach could be the promotion of sector based and industry led reporting systems that could function as rapid alert systems between peers and which would progressively increase awareness and expertise and improve preparedness and resilience.

7. RECOMMENDATIONS TO ADDRESS THE CHALLENGE

Based on findings gathered through the literature review and stakeholder consultation, the team developed a set of recommendations aimed at addressing the challenges posed by cyber theft of trade secrets. Recommendations are focussed on **four main areas,** designed to be implemented by the EU, taking into consideration the existing strategies and legal instruments to tackle cyber theft of trade secrets. The four areas identified are: "Awareness and Training", "Facilitate Businesses in Addressing the Challenge", "Enhance institutional and Coordination Capabilities" and "Law Enforcement".

The first area of focus – Awareness and Training – addresses the core problem of general **unawareness of the threat of cyber theft of trade secrets** among European businesses, especially SMEs, and recommends the organisation of meetings, events, media publications, and dissemination of case studies, to strengthen management-level awareness and ensure continuous training for all level staff. In order to increase awareness of the threat among policy makers and high-level officials, case studies, best practice measures and existent guidelines would have a useful role – in particular in relation to the identification of internal departments, responsible employees and the role of relevant actors, such as CERTs and ENISA. The EU could promote a culture of information sharing, including the setting up of sector-based reporting mechanisms.

Increasing awareness of the risks associated with cyber theft of trade secrets leads to greater demand for new **preventive measures within industrial sector**. A set of incentives at EU level can assist businesses, particularly SMEs, in addressing the challenge and support their technology development and knowledge transfer among all sectors and categories of business. Moreover, the development of new tools and technologies should be advanced by increasing both public and private funding to research and innovation.

The EU should act as a coordinator to bring about political momentum on the issue and could do so by providing **a concerted solution to a shared problem. The EU should foster** international cooperation among sectoral key players regarding the adoption and implementation of effective countermeasures. The EU and Member States could reinforce the resources and competences of ENISA with a view to supporting increased cooperation and coordination among national authorities.

Finally, aiming at ensuring certainty and predictability of **law enforcement**, more stringent laws and penalties will be fundamental at EU level. The creation of a specific investigation law enforcement body for the prosecution of cyber theft of trade secrets can foster European monitoring and intervention operations.

Focus area	Recommendation Description
Awareness and Training	**Strengthen management-level awareness of the risk of cyber theft of trade secrets.** In many companies, especially SMEs, management is neither aware of the possibility of being a target nor of the risks of cyber theft of trade secrets. As an outcome, they do not adopt appropriate countermeasures. This issue affects management of the supply chain which comprises different types and sizes of companies (large companies can be attacked using SMEs as vehicles to reach them). Awareness of the threat at each level of the supply chain must be ensured to protect critical business information. • **Organise targeted events.** Organisation of industry events and conferences, setting up events in collaboration with industrial associations and organisations at EU level (e.g. Business Europe and DigitalEurope) can assist in raising awareness on the subject; • **Disseminate content via multi-media sources**. Such content should concern threats or activities carried out by institutions and should be published in specialist magazines, business reviews and newspapers, as well as on television. It is important that easy, clear and specific messages on the issue are disseminated. Awareness can be raised by means of "practices" and should be done in the local language; • **Disseminate case studies and best practices among senior executives**. Awareness actions (using reports or leaflets) should target high-level executives in senior management. Case studies are fundamental for achieving widespread comprehension of the threat of cyber theft of trade secrets. The spread of best practices could be managed by "EU knowledge centres". However only the most relevant best practices should be disseminated as a multiplication of them may generate confusion; • **Provide a public repository of best practices and guidelines**. A possible model tool could be the UK National Cyber Security Centre, which offers guidelines to SMEs entitled 10 steps to Cybersecurity. Such guidelines ought to be focussed on cyber theft of trade secrets. Best practice measures include classification of internal departments within a company, appointment of an employee person responsible for cybersecurity who has received trainings on cyber theft of trade secrets prevention and mitigation, running exercises and simulations, running regular vulnerability assessments, encryption of trade secrets, role of national CERTs and ENISA, and log and monitor marking; • **Promote a culture of information sharing.** Businesses and organisations should be incentivised to discuss the threat and consider the setting up of peer alert systems such as platforms allowing for anonymised incident reporting in order to build collective knowledge and increase **resilience**.
	Increase awareness of policy makers and high-level officials of the risk of cyber theft of trade secrets. In order to promote and support Member State action against cyber theft of trade secrets, and build a stronger prevention, education and culture at local and business level: • **Strengthen communication campaigns to policy makers.** There is a need to coordinate actions at a higher and central level, to ensure a coherent and well-targeted set of messages on cyber theft prevention and mitigation measures. ENISA could promote in its awareness raising campaign (European Cyber Security Month) the issue of cyber theft of trade secrets as a key point of interest; • **Coordinate with large companies to increase awareness raising efforts**. Multinationals have strong communication and lobbying capabilities. The EU should support them in pushing governments and national authorities to be more aware of the threat; • **Organise high-level meetings and roundtable events**. Ministers and high-level officials should be invited to events where cases of cyber theft of trade secrets and regulations are discussed with their peers from other Member States and with EU officials.
	Boost training of professionals and relevant civil servants. There is a general scarcity of cybersecurity-trained professionals, and in particular of those specialised in cyber theft of trade secrets. Therefore, there is a need to create capacity in this area and develop a pipeline of talents. Likewise, also members of the judiciary system and law enforcers should increase their expertise. Building on the Digital Competence Framework, the EC should elaborate a set of basic competences, training materials, and a certification system for cyber theft of trade secrets: • **Support the creation of multi-disciplinary teams responsible for cyber theft of trade secrets.** The EU should push for the creation of operational teams with diverse and complementary expertise coming from a variety of professional backgrounds; legal experts, informatics engineers, cybersecurity experts, investigative officers. This should be encouraged in tandem with the development of specific units tackling the issue across EU institutions, such as EC3, CERT-EU, EDA and particularly ENISA;

Focus area	Recommendation Description
	• **Establish regular training and certification.** Member States, in coordination and with the support of the EU, should develop courses and certifications for relevant civil servants based on a common set of guidelines. Universities could also consider developing courses on the topic of cyber theft of trade secrets. It is fundamental that these trainings provide easy, clear and simple messages that can be understandable by all stakeholders.

Focus area	Recommendation Description
Facilitate Business in Addressing the Challenge	**Encourage and support SMEs to invest in prevention and countermeasures**. SMEs oftentimes do not have the capabilities to adopt state of the art tools and methodologies to increase their security level and should therefore receive support. • **Consider the opportunity of funding a study on the impact of cyber theft of trade secrets for SMEs only.** The EU should take into consideration the possibility of providing funding to a study, which would analyse the specific position and environment of SMEs, with regard to cyber theft of trade secrets, in order to better evaluate what are the main requirements and mechanisms useful to this size of business. The study could foresee the realisation of a survey aimed at evaluating the standing of SMEs in the different sectors; • **Provide incentives to SMEs.** EU institutions should push national governments to provide incentives, subsidies or tax reliefs to SMEs investing in the adoption of countermeasures for cyber theft of trade secrets. Another suggested mechanism would be a "technology/IT welfare", with related toolkits to allow SMEs access to basic technologies protecting their critical information and helping them to define their level of data confidentiality. This mechanism would allow companies to increase their cybersecurity maturity and generate employment, while supporting the development of tools to monitor cyber incidents. Alternatively, promote national incentive policies enabling companies to improve their **reputation** when receiving **security certifications.** A final mechanism could be to award extra points at public tenders should the company demonstrate an increase in cybersecurity standards following a past attack. The most suited partners that could reach SMEs and disseminate toolkits would be industry associations and SMEs associations; **Disseminate guidelines for SMEs**. While several guidelines concerning cybersecurity in general are disseminated more specific ones relating to cyber theft of trade secrets should be disseminated. Guidelines should indicate what the minimum requirements are when it comes to security measures to prevent cyber theft of trade secrets. They could indicate what are the best practices in technology and knowledge transfer (i.e. exchange of classified emails, servers to protect trade secrets) and incentivise large businesses in supporting SMEs with their technological knowledge.
	Stimulate the development of new tools and technologies. Preventing and/or fighting theft of trade secrets entails a continuous race between offence and defence. New tools such as artificial intelligence and machine learning can give companies advanced ways to counter offenders. • **Increase public funding in research and innovation.** It is suggested that within the Horizon 2020 programme an EU "Cyber theft of Trade Secrets" topic is launched in the focus area "Boosting the effectiveness of the Security Union". Similarly, new Research and Innovation Actions in the next framework programme Horizon Europe can boost the development of new tools and technologies. To this end, the EU may also redirect a portion of the existing "SME Instrument". Specific funding for the development of new solutions to counter cyber theft of trade secrets could be included in the new Digital Europe programme. Funding could also be steered to new technologies such as distributed ledgers, which have clear applications in countering cyber theft of trade secrets; • **Boost private funding in research and innovation.** EU institutions and entities should encourage national governments to recognise tax credit for R&D expenses in the acquisition of new knowledge, feasibility studies or prototyping, aimed at preventing and/or countering cyber theft of trade secrets. At Member State level, such incentives could be provided directly; • **Promote collaborative innovation at sector level with cooperation between established businesses and start-ups.** The EU could form a consortium focussed on attracting innovation contributors to define and develop practical tools for the prevention of cyber theft of trade secrets. The

	program could be based on the assessment of the real needs shared at company level by the contributors to the monitoring and improvement/adjustment activities, to deliver sustainable, efficient and innovative tools to enhance companies' protection from cyber theft of trade secrets.

Focus area	Recommendation Description
Enhance Institutional and Coordination Capabilities	**Foster the use of common cybersecurity assessment frameworks and toolkits.** A crucial role for EU institutions should be to coordinate the adoption, implementation and support of common, frameworks toolkits, and guidelines related to cyber theft of trade secret. • **Adoption, implementation and support for a common vulnerability assessment framework.** EU institutions should coordinate with EU Member States to develop and support companies in the adoption of a common vulnerability assessment framework for identifying weaknesses in their IT systems and secure their trade secrets. To this end, PPPs could be a driver. Also, the EU and the Member States should clarify details on Vulnerability Equity Process, source and encryption; • **Develop a toolkit supporting businesses in identifying, classifying and protecting their confidential information.** Such a toolkit could consist in a catalogue of specific and detailed security controls to protect businesses' critical information, as developed in the US with NIST 800-53. The toolkit could be composed of a module with different level of complexity and should be tailored for different sectors. The most suited partners that could reach SMEs and disseminate the toolkit would be industry associations and SMEs associations; • **Consider the adoption of a framework for the assessment of value of trade secrets.** EU institutions and other EU entities could coordinate with Member States and cybersecurity experts the definition of a framework to estimate with a risk-based approach the lost future revenue and profitability and evaluating the more intangible adverse impacts.
	Strengthen institutional capabilities. The EU could strengthen and empower existing institutions responsible for cybercrime such as ENISA, the CSIRT network and the national CERTs to increase their focal point on cyber theft of trade secrets. • **Strengthen the role of ENISA**. The EU and the Member States should equip the Agency with adequate resources and competences, to support coordination and cooperation between national authorities in fighting against cyber theft of trade secrets; • **Fostering the role of the CERTs network**. CERTs network should strengthen its centralising role and share across all affiliated national CERTs facts and trends on cyber theft of trade secrets incidents raising awareness on the topic by disseminating guidelines and content.
	• **Assess the purposefulness of adopting a system of reporting and notification of incidents specific to cyber theft of trade secrets.** An effective reporting system for cyber theft of trade secrets would help collect information on cyber theft activities in an anonymised form. On this basis an investigation of certain cyber theft activates, in particular those involving actors in third countries, could be initiated and be the basis for discussions in international fora. This action should be considered together with, or as a subsequent step to, the adoption of sectorial peer reporting system by sectorial business associations; • **Collect further information from the business sector**. While advantages for researchers and policy makers in having a reporting system are more evident, the private sector may have no incentives in reporting. A wider stakeholder engagement targeted to the business community would allow to better grasp their position and the underlying features of a possible reporting system in terms of beneficiary, authority of the report, modalities and incentives for reporting; • **Define a pilot reporting system for a specific industrial sector.** Consider the opportunity to launch a pilot reporting system for cyber theft of trade secrets incidents. The pilot would enable to gather real feedback from its users thus supporting the EU assessment of its relevance. The pilot would build a case and raise awareness on the matter possibly acting as a first step for a future roadmap. The reporting systems could use one of the existing tools adopted in B2B reporting systems.

Focus area	Recommendation Description
	Strengthen cooperation between key players as well as with other national or international organisations and governmental entities. Since cyber theft of trade secrets is a global issue, the adoption of effective countermeasures requires a coordinated action by regional and international organisations. Coordinated actions increase deterrence and resilience and push inter-institutional collaboration: • **Foster cooperation on prevention of cyber theft of trade secrets with national and international organisations.** The EU should support cooperation and exchange of information with and between sectoral organisations, such as law enforcement (e.g. FBI and Interpol), military (e.g. NATO), and economic (e.g. WTO, OECD) ones, to strengthen cross-border cooperation on the issue; • **Engage in bilateral negotiations and agreements.** The EU should engage in diplomatic efforts aimed at sealing bilateral agreements on countering cyber theft of trade secrets, such as that between US and China. Additionally, international trade law and bilateral investment treaties (BITs) could be used as a vehicle to mitigate cyberattacks and better protect trade secrets. EU bilateral agreements deal with trade secrets, but refinement might be necessary consider the cyber aspect. Provisions might also be included in regional trade agreements similar to those in the new USA-Mexico-Canada agreement. The EU could push for multi-lateral action such as ratification of code of conduct for governments to abstain from cyber theft or funding such theft; • **Strengthen cooperation and dialogue between key players.** The next Horizon Europe framework could stimulate the implementation of coordination and support actions involving research communities, industry public authorities and infrastructure operators, along the lines of the FP7 project European Cyber Security Protection Alliance (CYSPA). Another option is to support organisations such as the European Organisation for Security (EOS), in focussing on cyber theft of trade secrets. An example is the UK National Cyber Security Centre (NCSC), which consolidated a number of government departments that now cooperate with many service/internet providers, issuing guidance on overall security control and policies; • **Push for a renewal in the international debate on FIN 48 IFRS.** Consider a tax relief provision for companies complying with certain safety standards. In this regard, the European Union should coordinate the elaboration of a common position for Member States, fostering a greater international consensus calling for the adoption of the measures.

Focus area	Recommendation Description
Strengthen Law Enforcement	• **Introduce more stringent cybersecurity laws.** More severe, certain and rapid punishment for offenders acts as deterrents limiting the spread of the threat.
	Boost investigation capabilities at national and EU level to counter cyber theft of trade secrets: • **Create a National Cybersecurity Investigative Department responsible for prosecuting cyber theft of trade secrets.** This could operate as an independent law enforcement organisation, such as the Italian unit dedicated at fighting Mafia related crimes (DIA). It should be able to investigate an intrusion and ascertain whether an unlawful incident actually took place and should comprise specialists from different backgrounds, e.g. IPR experts, informatics experts, business experts. This entity could operate as a network providing intelligence and information and should work in close collaboration with Europol/EC3, national CERTS, and business associations.

8. CONCLUSIONS

The study shows that cyber theft of trade secrets is one of the main threats for companies and organisations operating in the EU, both in terms of prevalence and in terms of impact, and that such threat will remain and grow in the future unless a deliberate and focussed action is implemented by national and supra-national organisations.

By analysing quantitative data available, it clearly emerges how **the threat is real.** According to ECIPE (February 2018) there has been significant negative impact at EU level as a result of cyber theft of trade secrets: about **€60 billion** loss of economic growth, resulting in loss of competitiveness, jobs and reduced R&D investments. More specifically, **289,000 jobs** could be at risk in 2018, with that number rising to **one million jobs** by 2025.[143]

Some sectors are more targeted than others. Verizon shows that in 2016, 108 cyber espionage incidents occurred in the **manufacturing sector**, which is the most affected sector in the EU; 93% of these incidents involved external perpetrators, while **91% involved the theft or attempted theft of trade secrets**.[144]

Data gathered in the study also demonstrate how cyber theft of trade secrets **affects SMEs more than larger companies**:[145] due to their low budgets, the lack of awareness of being a target and the lack of skilled IT professionals.

However, there is a scarcity of data on the matter and companies are unaware about the modalities and impacts of the threat. This is true for the research industry but also policy makers at all levels of governance. It is safe to assume that the real extent of the problem might be **much larger than currently estimated**, both in terms of number of incidents and in terms of impact.

One of the key reasons for the scarcity of data on cyber theft of trade secrets is that many intrusions are **not detected**. **The lack of awareness** of the phenomenon, along with multiplication and sophistication of techniques adopted by hackers and the upsurge of Advanced Persistent Threats, makes the challenge even more daunting. Many companies do not believe they are a target for this type of cyber intrusion and the time lag between intrusion and detection in Europe is three times longer than in the rest of the world: 469 days against an average of 146. Moreover, the speed with which a new cyber espionage specific malware is developed by cyber criminals contrasts with the slowness of policy makers in facing the problem. The RSA FirstWatch team states that the number of submitted cyber espionage malware increased almost **900%** in 2013 compared to all previous years combined.[146]

Even when detected, cyber theft of trade secrets is often **not reported**. Companies are reluctant to admit that they have been victims of trade secrets misappropriation and there is no general obligation of reporting or notifying incidents of cyber theft of trade secrets.

In fact, companies fear huge **economic and reputational losses** from the possible diffusion of news related to the misappropriation.

---

[143] ECIPE. (2018). Stealing thunder, Cloud, IoT and 5G paradigm for protecting European commercial interests. Will Cyber espionage be allowed to hold Europe Back in the global race for industrial competitiveness? Available at: http://ecipe.org/publications/stealing-thunder/?chapter=all

[144] Verizon. (2017). Data Breach Investigations Report. Available at: https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf

[145] PwC. (2014). Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential threats. Available at : https://create.org/wp-content/uploads/2014/07/CREATe.org-PwC-Trade-Secret-Theft-FINAL-Feb-2014_01.pdf;

Kaspersky Lab. (2013). Who's spying on you? No business is safe from cyber-espionage. Available at: https://media.kaspersky.com/en/business-security/kaspersky-cyber-espionage-whitepaper.pdf

Supply. National SMEs engagement Programme UK. (2014). The SME Cyber Market: How your business can benefit. Available at: https://www.contracts.mod.uk/wp-content/uploads/2017/09/The-SME-Cyber-Market-How-your-business-can-benefit.pdf

[146] Alex Cox. (2012). The Cyber Espionage Blueprint: Understanding Commonalities In Targeted Malware Campaigns. RSA FirstWatch. Available at: http://www.emc.do/collateral/white-papers/rsa-cyber-expionage-blueprint-understanding-commonalities-targeted-malware-campaigns.pdf

The immediate impact for a company in this case is the loss of its trade secret itself, combined with the cost of cleaning up or totally replacing affected systems. However, this is just the **tip of the iceberg**. In fact, stakeholders emphasized that **90% of costs** are only effectively measured and assessed **five to six years following the cyber intrusion.** This applies to **the loss of competitive advantages** that should have been generated by R&D, combined with additional cybersecurity expenses, such as cybersecurity insurance premiums.

Whenever the cyber intrusion and the stealing or loss of data becomes public, affected companies suffer reputational damage as their valuation decreases due to lost value of customer relationships and devaluation of trade name. In carrying out the analysis of cyber theft of trade secrets, the regulatory framework and institutional background were also analysed. The current policy landscape seems more targeted at countering **cyber threats in general**, and there are no instruments looking at **cyber theft of trade secret specifically**. **Obligations** – such as the implementation of specific cybersecurity controls for protection of trade secrets – are **very limited or non-existent**, especially for some industry sectors and for SMEs. As an example, the NIS Directive,[147] along with the Regulatory Framework for Electronic Communications, establishes obligations concerning **incident notifications**, but they are exclusively addressed to operators of essential services and providers of electronic communications,[148] **leaving aside all other companies** and organisations operating across the EU.

To this end, the study formulates **four main areas of recommendations,** to be considered by the EU, taking into account both strategies and legal instruments tackling cyber theft of trade secrets. The four areas of action identified are the following:

- "Awareness and Training";
- "Facilitate Businesses in Addressing the Challenge";
- "Enhance Institutional and Coordination Capabilities";
- "Strengthen Law Enforcement".

The first area of focus – Awareness and Training - addresses the core problem of general **unawareness of the threat of cyber theft of trade secrets** among European businesses, especially SMEs, and recommends the organisation of meetings, events, media publications, and case studies dissemination, to strengthen management-level awareness and ensure continuous training for all level staff. In order to increase awareness of the threat among policy makers and high-level officials case studies, best practice measures and guidelines would be useful – in particular in relation to the identification of internal departments, responsible employees and the role of relevant actors, such as CERTs and ENISA. European businesses should also be incentivised to adopt a culture of information sharing, including anonymised mechanisms for incident reporting.

Increasing awareness of the risks associated with cyber theft of trade secrets leads to greater demand for new preventive measures for within industrial sectors. A set of incentives at EU level can help businesses, particularly SMEs, in addressing the challenge and support their technology development and knowledge transfer across all sectors and categories of business, the public sector and universities. In order to support an effective implementation of these measures, the EU can adopt new tools and technologies.

[147] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

[148] Regulation (EC) No 544/2009 of the European Parliament and of the Council of 18 June 2009 amending Regulation (EC) No 717/2007 on roaming on public mobile telephone networks within the Community and Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2009.167.01.0012.01.ENG

The EU should act as a coordinator to bring about political momentum on the issue, by providing **a concerted solution to a shared problem. The EU should foster** international cooperation among sectoral key players, for the adoption and implementation of effective countermeasures. Furthermore, The Commission and Member States through the ENISA Management Board could equip the Agency with adequate resources and competences in order to increase coordination and cooperation between national authorities. Additionally, deterrence and resilience should be strengthened by mean of cross-border cooperation in the event of a major cyber incident, as well as by providing an appropriate response to the level of the threat itself, which is generally global in scope.

Finally, aiming at ensuring certainty and predictability of **law enforcement**, more stringent laws and penalties will be fundamental at EU level. The creation of a specific investigation law enforcement body for the prosecution of cyber theft of trade secrets can foster European monitoring and intervention operations.

ANNEX A: METHODOLOGY FOR THE PREPARATION OF THE REPORT

The methodology adopted for the preparation of the Draft Final Report is based on our technical proposal, on the additional insights gathered during the Third Meeting, and from all comments received by the EC related to the Interim Report. It describes the activities and approach taken in relation to each of the specific deliverable components of Task 3:

- A description of the activities carried out and the methodology followed for the preparation of the Draft Final Report;
- A literature review, comprising a revision of the Interim Report based on additional data collected;
- A Stakeholder Consultation review, integrating the additional interviews carried out after the submission of the Interim Report;
- A description of the methodology for the preparation of the Dissemination Report, a smaller version of the Draft Final Report suitable for wide dissemination and awareness raising actions with key statements from the literature review and the Stakeholder Consultation.

The methodology is structured in four main blocks:

- Revision of the Literature Review and Stakeholder Consultation: this comprised:
    - Restructuring of sections to give a clear overview of the overall results obtained, improve fluency, avoidance of repetition, improve coherence and readability;
    - Integration of suggestions and comments provided by the EC;
    - Inclusion of documentation not yet identified, such as reports published after the submission of the Interim Report and documents highlighted by stakeholders during additional consultation;
- Integration of the Stakeholder Consultation;
- Refinement and integration of recommendations to address the challenge;
- Preparation of the Event and the Dissemination Report.

Revision of the Literature Review and the Stakeholder Consultation

The sections dedicated to the Literature Review and the Stakeholder Consultation have been subject to considerable revision and refinement throughout the execution of activities during Task 3.

The main objective of this activity was to completely restructure the chapters "4. Revised version of the literature review" and "*5. Stakeholder consultation – Key Findings*" inserted in the Interim Report, in order to elaborate a single chapter of "Key Findings" that reflects the main results obtained both from the Literature Review and the Stakeholder Consultation.

A further objective of this was to improve the narrative, readability and cohesiveness, as well as removing any instances of repetition, reintroducing also the "meta-analysis" language adopted for the Initial Report.

The original sections set out in the Interim Report have been restructured to answer each suggestion and comment provided by the EC, aggregated in the Draft Final Report as follows:

4. **Literature Review**: The chapter provides a comprehensive analysis of all the documentation, reports, papers, publications retrieved during the Desk Research activities, giving detailed statistics and information on the Member States and organisations addressing the topic.

5. **Stakeholder Consultation**: The chapter provides statistics and details on the Stakeholder Consultation, providing a high-level analysis of the results obtained from the interviews and from the online survey and the perceptions of the research team for the positive or negative participation of stakeholders in this initiative.
6. **Key Findings of the Study**: Comprises all the most important information and data retrieved from the former sections "*4. Revised version of the literature review*" and "*5. Stakeholder consultation – Key Findings*" of the Interim Report. This chapter is built by aggregating the main results retrieved from the Literature Review, from the Interviews and the Online Survey and it is structured in two sub-sections, namely:
   - **6.1 State of the Threat:** This sub-section provides the main results related to the current threat in Europe, stakeholder perception of the threat, possible future trends, the lack of awareness on the topic, concrete cases occurred and the negative impacts on large, small and medium enterprises;
   - **6.2 Preventing, Migrating, Reporting measures:** This sub-section provides an overview on the current policy measures adopted at EU level, the strategies and technological tools adopted by companies to counteract the cyber theft of trade secrets.
7. **Recommendations to Address the Challenge**: comprises four recommendations developed around four main areas identified by the team, these being: "*Awareness and Training*", "*Facilitate Businesses in Addressing the Challenge*", "*Enhance the institutional and Coordination Capabilities*" and "*Law Enforcement*".

To improve the Literature Review additional documentation has been added, identified from a variety of sources:

- Documents recommended by various stakeholders during additional consultation;
- Documents published after the submission of the Interim Report;

The additional literature has been particularly useful, in terms of informing the recommendations on measures to counteract cyber theft of trade secrets and to update the latest estimates of the negative impacts suffered by European companies.

Integration of the Stakeholder Consultation

The Stakeholder Consultation was designed with the intention of improving and building upon the (limited) data available online, with additional information and data collected through the interviews and survey. The questions were also designed so as to ensure alignment and integration with the Literature Review. Interviews/survey were conducted with stakeholders across four categories according to tender specifications. The list of key stakeholders was initially developed during the preparation of the technical proposal and was continuously updated and refined during the execution of Task 2.

Identified stakeholders were been grouped into four categories:

- Business community (entrepreneurs; companies; economic groups) - Cat Bus;
- Scientific researchers and research bodies - Cat Sci;
- Cybersecurity service providers and cybersecurity experts – Cat Cyb;
- Other stakeholders (governmental bodies, international organisations, think tanks, academia) - Cat Others.

Questions were designed for each category of stakeholders: questions for stakeholders from business and scientific fields were focussed on gathering information relating to their specific company or organisation, while questions posed to stakeholders from categories "Cyb" and "Others" investigated expert opinions in more detail.

When possible for Business and Scientific categories, CIOs, CISOs, CTOs were contacted. This preference was determined by the need to identify levels of security within companies and gain a technical overview.[149]

Taking into account the additional interviews conducted after the submission of the Interim Report, data from a **total of 78 stakeholder interviews/surveys** was gathered.

The primary data collection tool during Task 2 was a programme of stakeholder **interviews**. The request to participate in the **survey** was solely understood as a back-up solution in case stakeholders were unwilling to participate in an interview.

Therefore, the engagement process was structured in three rounds:

- **Round 1°:** Contact email to the entire list of contacts (**719**) inviting each stakeholder to participate in an **interview**. The email included information about the study and its objectives, as well as the overall policy goal to define appropriate measures to mitigate the cyber thefts of trade secrets. All emails were accompanied by two attached documents; a NDA and a Support Letter signed by the EC;
- **Round 2°:** A second round of engagement was undertaken involving a follow-up email to all stakeholders that did not reply in the first round. This time the email included options to undertake an **interview** and/or participate in the online **survey** by clicking on an attached link;
- **Round 3°:** A third round of engagement was undertaken involving **direct phone calls to 85 of the most valuable stakeholders** in order to arrange interview appointments.

The three rounds of engagement resulted in the following statistics.

Categories	Stakeholders contacted	TOR target	Aggregated Stakeholders Support
Business community (entrepreneurs; companies; economic groups) – Bus	386	30	28
Scientific researchers and research bodies – Scy	40	5	10
Cybersecurity service providers and cybersecurity experts – Cyb	114	5	9
Governmental bodies; international organisations; think tanks and academia – Others	179	10	31
Total	**719**	**50**	**78**

The 73 responses from the survey represents the aggregate data from the **survey** and from the **interviews**. The table below demonstrate the breakdown and the response rate for each of the categories as well as the data collection methodology coverage.

Categories	Aggregated Stakeholders Support	Stakeholders interviewed	Surveyed Stakeholders
Business community (entrepreneurs; companies; economic groups) – Bus	28	17	11
Scientific researchers and research bodies – Scy	10	7	3

[149] Respectively: CIOs (Chief Information Officers), CISOs (Chief Information Security Officers), CTOs (Chief Information Technology Officers).

Categories	Aggregated Stakeholders Support	Stakeholders interviewed	Surveyed Stakeholders
Cybersecurity service providers and cybersecurity experts – Cyb	9	5	4
Governmental bodies; international organisations; think tanks and academia – Others	31	12	19
Total	**78**	**41**	**37**

As a key finding Business community seemed much more reluctant to participate to our interviews since only **7% of the stakeholders** from this category accepted. In contrast, **20% of scientific researchers** participated to our interviews.

Refinement and integration of recommendations to address the challenge

The chapter "7. Recommendations to address the challenge" provide an overview of the main findings in this regard and aims at defining possible solutions that **policy makers at EU-level could implement in the future**.

Contrary to what was included in the Interim Report, which provided recommendations on three levels (company, national and European), this version of the Draft Final Report offers four different areas of recommendations, built up on the information gathered from both the literature review and the stakeholder consultation, and designed to be addressed to European policy makers. The four areas of recommendations identified are:

- "Awareness and Training";
- "Facilitate Businesses in Addressing the Challenge";
- "Enhance Institutional and Coordination Capabilities";
- "Strengthen Law Enforcement".

According also to the suggestions and recommendations provided by the EC during the Third Meeting, recommendations were developed according to the following criteria:

- Recommendations regarding cybersecurity in general were replaced, giving more concrete and specific recommendations considering what the threat is and what the risk is;
- Recommendations have been made specific, actionable and in line with latest directives and regulations;
- Recommendations devoted to companies were discarded, concentrating on the ones at European level. National level recommendations, furthermore, served as complementary to the European ones.

Each of the four areas of recommendations presents various action point with the relative descriptions. After the "Event" taking place in Brussels on 4th October 2018 with the participation of the relevant stakeholders identified, a final review of the recommendations will be presented in the Final Report.

Preparation of the Event and the Dissemination Report

To prepare properly the "**Event**", a detailed agenda, list of speakers and a Dissemination Report have been prepared for the EC. During Task 3, the activities carried out for the preparation of the Event were:

- Draft the list of the speakers from the business category and establish contact inquiring on availability/willingness to speak. These speakers were selected according to the following selection criteria:

  - Stakeholders that have been interviewed, deemed appropriate and who showed the interest in participating;
  - Stakeholders chosen on the basis of the different opinions registered and on the basis of the debate that they can create by participating;
  - Stakeholders from businesses which operate at the European level and have a strong innovative component;
  - Stakeholders from businesses based in Belgium, where the "Event" will take place, in order to encourage their participation at the "Event";
- Draft emails to invite stakeholders/experts to speak to the event;
- Draft "Save the Date" once the tentative speakers have been contacted. The "Save the Date" include a provisory agenda and a brief description of the study;
- Draft email to invite stakeholders as attendees to the event.

Once the availability is confirmed, each speaker and each confirmed attendee will receive a copy of the **Dissemination Report**.

The Dissemination Report is a ten page document prepared for sharing the value of the project with the relevant stakeholders engaged, giving preliminary insights of the Final Report and also contributing to increase interest in the "Event".

The Dissemination Report communicates to the stakeholder community about the project methodology, findings from literature review and the stakeholder consultation, recommendations to be considered and challenges encountered along the way.

ANNEX B: CASE STUDY PROTOCOL

The case study protocol outlined the work requirements and described the main procedures, including:

- Objectives, timetable and the resources allocated;
- Data collection methods and procedures;
- A case study template with guidance on length, outline, format and presentation style.

Data Gathering Template

Description of the trade secret held

Description of trade secret held

Quantification of trade secret with respect to total asset

Cybersecurity measures in place

Measures that your organisation proactively adopts to prevent theft

Cost of those measures (in terms of personnel or in financial terms)

Change in the measures and related costs before and after the attack

Specifics of the incident

Number of episodes

Methodology of the attack (e.g.: spear-phishing; watering hole attack; zero-day exploits; man in the middle attack, etc.)

Perpetrators

Detection (timing and methodology)

Reporting of the incident (e.g.: Law enforcement agency, Intelligence Services, Computer Emergency Response Teams, Press & Media, Business associations, others). Reasons for not reporting

Lawsuit and court case

Impact of the incident

Typology and description of the loss: economic Loss, Reputational Loss / Loss of clients, Loss of business opportunities, increase in cybersecurity expenditures, etc.

Quantification (in terms of resources and time both of the attack results and damage control)

Lessons learnt from the attack

Preventing measures that could have prevented the attack (e.g. cybersecurity tools, standards and assessment frameworks, risk assessment, training)

Damage control

New strategies implemented

ANNEX C: CASE STUDIES IDENTIFIED

Case n°1: Cyber espionage in ThyssenKrupp.

On 8th December 2016, the German industrial conglomerate ThyssenKrupp - world leader in the steel market - revealed that its technical trade secrets were stolen in a cyber intrusion on its systems. ThyssenKrupp is present in 79 countries and the growth and economic stability of the business is based on multi-million investment in R&D and their protection. The company invests around 30-50 million € a year on central initiative on cybersecurity out of an IT budget of one billion euros.

The secrets were stolen from the steel production and manufacturing plant design by attackers engaged in "organised, highly professional hacker activities." Several sources stated that the intrusion would have been carried out by a criminal group based in Southeast Asia. As regards the sites that have suffered the attack, the German business magazine Wirtschafts Woche reported that the attacks hit sites in Europe, India, Argentina and the US run by the Industrial Solutions division, which builds large production plants. The Hagen Hohenlimburg specialty steel mill in western Germany was also targeted, the report added. Besides, the company declined to identify specific locations which were infected or speculate on likely suspects. It said it could not estimate the scale of the IP losses.

It is noted that the company uncovered the intrusion in April, although the criminal activity apparently happened in February and involved hackers stealing project data from the company's plant engineering division and other areas of its business yet to be determined. Contrary to the time-lag usually reported in the literature, Thyssenkrupp managed to uncover the intrusion in 45 days. This occurred thank to a cybersecurity team in place since 2012 and the monitoring activities undertaken by CERT technicians who found some abnormalities on their systems. When investigating on the cyber intrusion, they realized that hackers were going from one system to the other system until they found the information they were looking for. Their goal was likely to identify the servers containing files and R&D data.

The research team had the possibility to partially discuss some details of the intrusion with the Head of Infrastructure and Security at Thyssenkrupp. He reported that, at the time of the intrusion, the company decided to make it public as it deemed safer for its reputation to be in control of the narrative in order to present the company as reliable and able to sustain the responsibilities deriving from the theft. This decision allowed Thyssenkrupp to maintain a direct link with authorities during investigations and in the end the company was able to prevent any loss of IP.

Despite the group publicly released that "no reliable estimation as to the damage" was possible to be shared, also considering the intangible assets involved, the following table shows the impact on the stock title after one year from the cyber incident:

Source: Financial Times "ThyssenKrupp reveals data stolen in cyberattack", December 8, 2016, available at: https://www.ft.com/content/7b556fb8-bd43-11e6-8b45-b8b81dd5d080

In the same period, a criminal complaint was filed with police in the state of North Rhine-Westphalia and an investigation, it said. State and federal cybersecurity and data protection authorities were kept informed at each stage, as well as Thyssen's board.

At the time, ThyssenKrupp also said the intrusion should not be blamed on security deficiencies at the group, or to human error. It cited expert opinion that claimed "it is currently virtually impossible to provide viable protection against organised, highly professional hacking attacks."

In the course of the final event of the Study, ThyssenKrupp was invited to take part as one of the main speakers. Their Head of Group Infrastructure & Security welcomed the EC activities to counter the threat of cyber theft of trade secrets and highlighted the importance of training people with strong skills in cybersecurity, raising awareness on the issue and the importance to enhance international cooperation.

Sources identified:

- https://www.ft.com/content/7b556fb8-bd43-11e6-8b45-b8b81dd5d080
- https://www.reuters.com/article/us-thyssenkrupp-cyber/thyssenkrupp-secrets-stolen-in-massive-cyber-attack-idUSKBN13X0VW
- http://www.datacenterdynamics.com/content-tracks/security-risk/thyssenkrupp-suffers-cyber-espionage-attack/97465.fullarticle
- http://www.dw.com/en/thyssenkrupp-victim-of-cyber-attack/a-36695341
- https://www.pcworld.com/article/3148604/security/cyberspies-stole-secrets-from-industrial-giant-thyssenkrupp.html

Case N°2: Operation Cloud Hopper- UK managed IT service providers.

Since late 2016, PwC UK and BAE Systems have been assisting victims of a new cyber espionage campaign conducted by a China-based threat actor. The espionage campaign, referred to as Operation Cloud Hopper, has targeted managed IT service providers (MSPs), allowing APT10 unprecedented potential access to the IP and sensitive data of those MSPs and their clients globally. This indirect approach of reaching many through only a few targets demonstrates a new level of maturity in cyber espionage. The campaign employed several malware including several iterations of remote access Trojans (RATs) including old but notorious families like PlugX, Poison Ivy, ChChes, and Graftor.

In particular the Operation Cloud Hopper campaign leveraged on well-researched spear-phishing messages aimed to compromise MSPs. Furthermore, the hackers used this tactic to obtain legitimate credentials to access the client networks of MPSs and exfiltrate sensitive data.

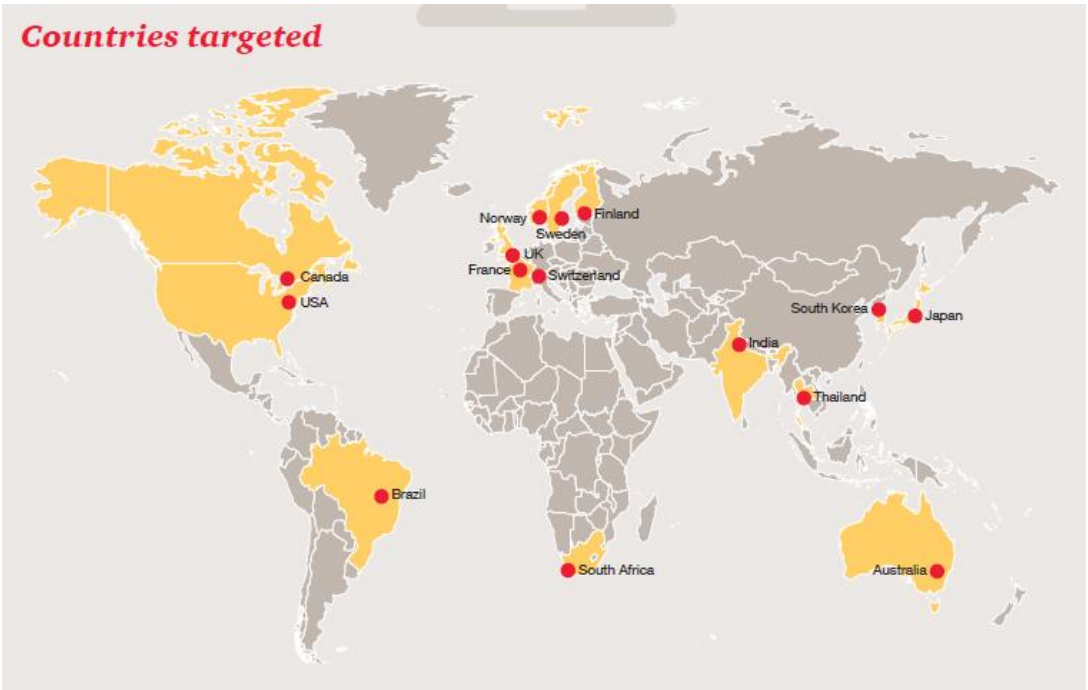
Analysing the malicious activities of the Chinese hackers it was possible to notice that the cyber intrusions followed MSPs' working hours: the cyber espionage activities started at 8:00 am until 12:00 pm, when the hackers took a "coffee break", to then resume from 13 pm to 17 pm.

Countries affected by the APT10 group include: Brazil, USA, Canada, UK, France, Switzerland, Sweden, Finland, South Africa, and India.

Chinese APTs have attacked several sectors, showing interest for any kind of innovation, including: energy and mining, engineering construction, metals, industrial manufacturing, telecommunications and professional services.

To develop the report, PwC UK cooperated closely with law enforcement and intelligence agencies. The difficulty in convincing companies to talk about this issue was among the main difficulties in conducting the study.

Below, a map created by the PwC network, about the countries affected by the cyber espionage attack.



Preliminary sources identified:

- https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-cloud-hopper-what-you-neeto-know
- https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf
- http://securityaffairs.co/wordpress/57781/apt/operation-cloud-hopper-apt10.html

ANNEX D: SURVEY QUESTIONNAIRE

In order to assist the EC - DG GROW in gathering evidence on the impact and volume of cyber theft of trade secrets, the team made an online questionnaire which is currently still available for stakeholders to take and results will be further adjourned in the final report.

The questionnaire, used as an alternative to the interview when stakeholders were not available for it, will help the Team and the EC to build additional specific evidence to the results of the literature review and the stakeholders' interviews.

Given the sensibility of the topic, the questionnaire was designed in a way that allowed stakeholders to skip questions they deemed too sensitive to reply to. Questions are either multiple choice, where stakeholders are asked to provide a ranking of different options, or close ended questions with just yes/no reply.

The questions of the survey were designed in tandem with the interview questions and allowed most of the time for comments (although there were no comment made). In fact the team aimed at ensuring to a certain extent a correspondence between questions as to ensure that dataset from the survey and from the interviews can be comparable. Certain questions are targeted to different sets of stakeholders:

- Business community (Cat I);
- Research bodies (Cat II);
- Cybersecurity experts and companies (Cat III);
- Other stakeholders (governmental bodies, international organisations, think tanks and academia) Cat (IV).

Questions on personal details, although not mandatory, were included in the first part of the survey in order to be able to differentiate by category. All respondents provided this detail.

We received feedbacks from a total of 36 stakeholders. More stakeholders entered the survey but the number of replies was so low that are not taken into account in the analysis of data. A total of 13 stakeholders belonging to CAT I and CAT II completed the survey while a total of 23 did so from CAT III and IV[150].

Below, the team provides an analysis of the results of the survey questionnaire.

Cyber theft of trade secrets as a real threat to the EU

In line with the results of the interviews, the survey displays how stakeholders consider cyber theft of trade secrets as a real and growing threat to business operating in the EU. Replies to Q1.1 were equally distributed between "agree" and "strongly agree", as were almost the ones to Q1.2, with "strongly agree" attesting to more than 60% and "agree" a bit lower than 40%. A sensitively similar patter can be found in the result of the question asking if stakeholders thought that any kind of company/organisation operating in the EU, which holds trade secrets, is a potential target of cyberattacks (Q1.3).

Replies regarding awareness of the threat (Q1.4) and cybersecurity tools (Q1.5) within companies and organisations highlight a general agreement with the statements offered. Only a percentage of respondents around 5% thought that level of awareness and cybersecurity tools within companies where high enough, while an average of 20% remain neutral.

SMEs, as already seen in interviews and in literature reviews, result exposed to the threat related to cyber theft of trade secrets at least as much as large enterprises: almost 60%

[150] Note: the Survey Questionnaire for CAT I and CAT II asked as well if the business/organisation was ever victim of a cyber theft and to provide details of the event. Moreover all CATs were asked if they were knowledgeable of an incident. Replies to these sets of questions were only partial as not all details were provided. These surveys are nevertheless considered completed by the team.

of stakeholders agreed with the statement provided, 40% strongly agreed and just a small 2% disagreed.

Impacts on companies and organisations

Stakeholders were asked to identify and rank the most relevant impacts suffered by a company or organisation victim of a cyber theft (Q1.6 and following chart). Options provided for this question are:

- Economic Loss;
- Reputational Loss;
- Loss of Business;
- Increase in cybersecurity spending;
- Other

Among these, the one selected by the highest number of respondents as first choice is Economic loss (almost 47% of the time) follows by reputational loss (25%) and loss of business opportunity (almost 16%). Increase in cybersecurity spending and "other" were never selected as most relevant impact.

With regard to categories I and II, namely businesses and research bodies, specific questions were submitted due to their direct exposure to trade secrets stealing. Given the total of stakeholders included in the survey, 93,33% affirmed that their organization holds information or knowledge kept away from their competitors (Q.2.1). 66,67% of stakeholders asserted that their organization adopted measures to prevent cyber thefts of trade secrets, and the remaining 33,33% recognised that probably the measures already enacted probably are not enough (Q.2.2.).

With regard to cyber thefts experienced during the last 5 years, 33, 33% of them admitted that their organization suffered from one or multiple cyber intrusions, while 40% negated it, 20% do not know and 1 was not able to answer to this question (Q2.3). 40% of them affirmed that suffered between 2 and 9 cyberattacks, 1 recognised over 20 attacks, 20% affirmed to have never suffered an attack, and 40% do not know (Q2.3.1).

Only 20% of the stakeholders were able to provide the following details about the attacks experienced: year and cause of the incident, and type of data stolen, and 40% of them specified the impact suffered; while 20% preferred not to disclose additional information.

Coming to the details revealed above mentioned, in the first case, the incident occurred in 2008, caused by data leakage, and designs were stolen, suffering for the subsequent copy of the product.

In the second case, the intrusion occurred each year during the last 5 ones, caused by all the typologies listed in the survey (spear-phishing, watering hole attack, zero-day, etc.), and the attacks consisted in daily attacks, probably state-sponsored or similar. Therefore, the organization monitor and manage the situation and consider themselves lucky enough so far, as no type of data stolen has been observed.

In the third case, the intrusion occurred in 2017, caused by social engineering, but no data has been stolen and therefore, the stakeholder does not considered any impact suffered.

The majority reported (Q2.4) the intrusion to a law enforcement agency or to CERTs (both 30%), while 20% preferred to report it to intelligence services, and a lower number to business associations (10%).

In answering to a precise question about the awareness of attacks (Q3.1), the majority (52.94%) considered his/her own company not aware about being attacked by a cyber theft of trade secret, against a 47,06%, who affirmed its awareness.

Out of the stakeholders who attested being aware of a case, only 2 were able to provide: year and cause of the incident, type of data stolen, the impact suffered, and possible additional information. In one case, the stakeholder was also able to identify the name of

the company that suffered the attack. Hypothetically, a last one did not provide any answer, as it was not mandatory.

Going deeper, the first stakeholder referred of a case dated 2017, whose cause was the infiltration to e-mail correspondence, through which personal information of the company and its clients. The impact of the intrusion provoked an abuse of the data stolen to get money from the company and from its clients, ending in a loss of confidence towards the company. The second stakeholder referred to several cases, occurred between 2015 and 2018, involving LinkedIn, Facebook, and some banks, but he had no idea about cause, and considered that the data stolen probably were account information, resulted in a loss of reputation, as well. Finally, the stakeholder referred that the attacker monitored the e-mail communication and at the right moment sent an e-mail with changed bank details to a client.

Other two cases have been reported with reference to 2017. The survey provided more details only for one of them: the intrusion occurred through social engineering and business data have been stolen.

Prevention, mitigating measures, reporting and recommendations to address the issue of cyber theft of trade secrets

All respondents (all CATs) provided a reply to the best measures that companies and organisation could implement in order to avoid cyber theft of trade secrets (Q4.1). In line with results of the interviews, the preferred option was "Target employee awareness raising and training" equally with "adopt the most advanced cybersecurity tools" (both attesting at 25%). These were followed by (in order of preference): the need to prioritise a cybersecurity strategy, the use of a common cybersecurity standard, and the suggestion to avoid adopting cloud platforms.

Stakeholders belonging to categories III and IV were asked to recommend the best ways to prevent cyber theft of trade secrets at national and European levels. These are multiple choice questions where respondents ranked the following options for national and European levels respectively.

National level (Q3.4):

- Raise awareness on the risk and recommendations;
- Encourage companies to invest in cybersecurity;
- Ensure law enforcement follows serious incidents;
- Introduce more stringent cybercrime laws
- Strengthen cooperation and dialogue between key actors;
- Introduce more stringent cybersecurity laws imposing adoption of minimum requirements to companies and organisations.

European level (Q3.5):

- Introduce or promote more stringent cybersecurity laws punishing criminals;
- Foster the use of common cybersecurity standards, assessment and frameworks;
- Join an international agreement (e.g. Obama-Xi Agreement);
- Introduce more stringent cybersecurity laws and penalties for companied;
- Strengthen cooperation between the EU and other national or international organisations (e.g. NATO, FBI, WTO).

Responses provided do not distance themselves from the results of the interviews. As showcased in Q3.4 and Q3.5 (and relative focus on first positions), stakeholders placed first the need to raise awareness and the need to strengthen the coordinating role of the EU respectively.

At national level, following the first position, the options that received the second and third highest number of preference were "introduction of more stringent cybersecurity laws" against criminal and "strengthen cooperation and dialogue between key actors".

At European level stakeholders placed in second and third position "foster the use of common cybersecurity standards, assessment and frameworks" and "introduce more stringent cybersecurity laws and penalties for companied".

In this section of the survey, stakeholders were asked as well to underline their preference, or not, for a reporting system. Almost 90% of them agreed and considered it beneficial to collect data on a regular basis (Q4.2), while almost the 80% pointed out as constructive a voluntary reporting system (Q4.3) and, as highlighted at Q4.4, a European law enforcement agency was the preferred organisation to receive the report (22%).

Based on results of multiple-choice question 4.5, businesses and organisations would be encouraged to report by trusting the effectiveness of law enforcement at national level, followed by the possibility to receive timely information and the opportunity to receive sufficient confidentiality guarantees.

Objective of the survey

PwC is supporting the EC in collecting and analysing data to report on the estimated volume and impact of the cyber theft of trade secrets, referred as all sorts of valuable information that businesses keep confidential because of its importance for their competitiveness. This includes, for example, business plans, research results, undisclosed manufacturing processes, technology and know-how, clients or providers' lists, the price that will be offered in a bid, the design and features of a new product or model.

The survey represents one of the first attempts to ascertain the real scale and impact of theft of trade secrets through cyber. With cyber intrusion, we refer to external and unlawful appropriation of information by accessing a company ICT network. Therefore, the appropriation and copying of information, by an employee that is achieved without unauthorised intrusion into a computer or a network is out of scope.

Your answers to the survey are of foremost importance to the measurement of the threat and in providing valuable insights and informed policy making for countering such unlawful activities, by analysing the point of view of organisations that could be aware and support business in managing such events.

Confidentiality & Data Protection

We understand the businesses' reluctance in disclosing sensitive data. In this regard, PWC is fully committed to make certain the confidentiality by ensuring that no-third party will ever be aware of your organisation information and that the best technical measure of data protection[151] are put in place. Furthermore, the results of the survey will be reported in aggregate form and no individual respondent will be identified, unless specifically agreed otherwise.

The survey will take around 15 minutes to complete and answers will be automatically saved allowing to return to the survey at a later stage.

[151] Details technical measures to ensure compliance and confidentiality of data.

Personal Data			
	Question	**Answer proposal**	
	I am responding to the questionnaire as:	☐ Business ☐ Research body ☐ Cyber security services/ products provider ☐ Academia ☐ Government body ☐ Think tank	**All CAT**
	What is your first name? (optional)	☐	**All CAT**
	What is your last name? (optional)	☐	**All CAT**
	What is your email address? (optional)	☐	**All CAT**
	What is your role/profession?	☐	**All CAT**
	What is the name of your organisation?	☐	**All CAT**

Survey Questionnaire			
Q1	Do you agree with the statement that cyber theft of trade secrets is a real threat to businesses operating in the EU?	☐ Strongly agree ☐ Agree ☐ Neutral ☐ Disagree ☐ Strongly disagree	**All CAT**
Q2	Do you agree with the statement that cyber theft of threat secrets could be a growing threat in the future?	☐ Strongly agree ☐ Agree ☐ Neutral ☐ Disagree ☐ Strongly disagree	**All CAT**
Q3	Do you agree with the statement that any kind of company/organisation operating in the EU, which holds trade secrets, is a potential target of cyber-attacks?	☐ Strongly agree ☐ Agree ☐ Neutral ☐ Disagree ☐ Strongly disagree	**All CAT**
Q4	Do you agree with the statement that companies/organisations are not aware of cyber risks related to the protection of trade secrets?	☐ Strongly agree ☐ Agree ☐ Neutral ☐ Disagree ☐ Strongly disagree	**All CAT**
Q5	Do you agree with the statement that companies/organisations operating in the EU do not adopt advanced technological tools or implement cyber security policies for the protection of trade secrets?	☐ Strongly agree ☐ Agree ☐ Neutral ☐ Disagree ☐ Strongly disagree	**All CAT**

Survey Questionnaire			
Q6	What do you think are the most relevant impacts for victims of cyber theft of trade secrets? Please rank the following options (1 should indicate the most relevant):	☐ Economic Loss ☐ Reputational Loss / Loss of clients ☐ Loss of business opportunities ☐ Increase in cyber security expenditures ☐ Other If other, please specify: [ ]	**All CAT**
Q7	Does your organisation hold information and knowledge that you need to keep away from your competitors?	☐ Yes ☐ No ☐ I don't know ☐ N/a	**CAT (I)** **CAT (II)**
Q8	Does your organisation proactively adopts measures to prevent theft, or theft attempts, of trade secrets through cyber?"	☐ Yes ☐ No	**CAT (I)** **CAT (II)**
Q9	Over the past five years, has your organisation suffer from one or multiple cyber-attacks, or attempts of, with the aim of stealing trade secrets?	☐ Yes ☐ No ☐ I don't know ☐ N/a	**CAT (I)** **CAT (II)**
Q10	If the answer to the previous question is yes, how many times?	☐ 1 ☐ 2 - 9 ☐ 10 – 20 ☐ 20+ ☐ I don't know	**CAT (I)** **CAT (II)**
Q11	If the answer to the previous question is yes please provide the following information: In case of large number of cyber-attacks with theft of trade secrets, please report the most relevant incidents.	a. Name of the company/organisation (optional) [ ] b. Year of the incident [ ] c. Causes of the incident (e.g.: spear-phishing; watering hole attack; zero-day exploits; man in the middle attack, etc.) [ ] d. Type of data stolen [ ] e. Please specify the impact suffered [ ] f. Additional remarks [ ] ☐ I prefer not to disclose any information in this respect	**CAT (I)** **CAT (II)**
Q12	If your company/organisation was hit by a cyber theft of trade secrets, did you report the incident? If so, to whom? Multiple choice allowed	☐ Law enforcement agency ☐ Intelligence Services ☐ Computer Emergency Response Teams ☐ Press & Media ☐ Business associations ☐ Others If other, please specify: [ ]	**CAT (I)** **CAT (II)**

Survey Questionnaire			
Q13	Are you aware of a case or more cases of a company/research organisation that suffered attempts or cyber-attacks with the aim of stealing trade secrets?	☐ Yes ☐ No If yes, please specify details: [ ]	**ALL CAT**
Q14	Do you agree with the fact that SMEs are exposed to risks related to the theft of trade secrets through cyber?	☐ Strongly agree ☐ Agree ☐ Neutral ☐ Disagree ☐ Strongly disagree	**All CAT**
Q15	Does your company adopt effective cyber security strategies and measures to mitigate cyber risks related to supply chain?	☐ Yes ☐ No If yes, please specify details: [ ]	**CAT (I)** **CAT (II)**
Q16	What do you think are the economic sectors[152] or research areas that are most impacted by theft of trade secrets? Multiple choice allowed	☐ ICT sector ☐ Industrial Defence sector ☐ Manufacturing, consumer goods and retail sector ☐ Finance sector ☐ Health and pharmaceutical sector ☐ Chemical sector ☐ Other If other, please specify: [ ]	**CAT (III)** **CAT (IV)**
Q17	What do you think are the most effective measures and policies that a company or research bodies may enact to face the challenge of theft of trade secrets? Please rank the following options (1 should indicate the most effective):	☐ Adopt the most advanced cyber security tools (e.g. Firewalls, Data Loss Prevention tools, SIEM systems, etc.) ☐ Use of common cyber security standards or assessment frameworks[153] ☐ Prioritize a cybersecurity strategy based on a risk assessment approach ☐ Target employee awareness raising and training ☐ Avoid the adoption of cloud platforms or other platforms that exchange data with the external perimeter ☐ Other If other, please specify: [ ]	**All CAT**
Q18	At the national level, what do you think would be the best recommendation for institutional	☐ Raise awareness on the risks and recommendations on measures for companies.	**CAT (III)**

[152] Baker McKenzie, (2017), The rising importance of safeguarding trade secrets.

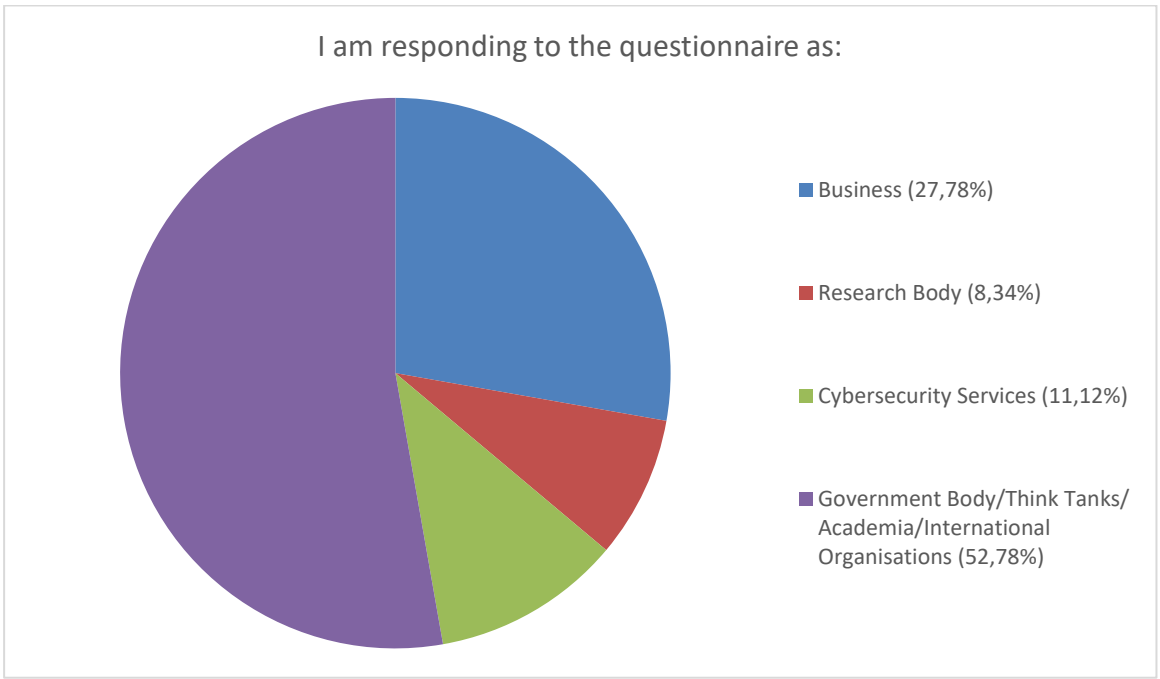
[153] Cybersecurity standards define both functional and assurance requirements within a product, system, process, or technology environment. (E.g. ISO/IEC 27001, COBIT 5, NIST SP 800-53 Rev. 4, PAS 555, etc.). A Cybersecurity Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. Frameworks are often customized to solve specific information security problems or to be implemented in a specific industry sector. Cyber Security Frameworks (e.g. NIST CSF, Italian Cyber Security Framework, CIS Critical Security Controls, CIIP Framework, etc.).

Survey Questionnaire			
	or governmental bodies for tackling the issue of cyber theft of trade secrets? Please rank the following options (1 should indicate the most relevant):	☐ Strengthen cooperation and dialogue between key actors. ☐ Ensure law enforcement following serious incidents. ☐ Introduce more stringent cyber security laws and penalties for not compliant companies/organisations and to punish cyber criminals harder. ☐ Create a national multiagency investigative body against cyber-crime. ☐ Encourage companies to invest in cyber security giving the possibility of tax relief or incentives. If other, please specify: ☐	**CAT (IV)**
Q19	At the European level, what do you think would be the best recommendation for tackling the issue of cyber theft of trade secrets? Please rank the following options (1 should indicate the best recommendation):	☐ Enhancing the EU coordination role (e.g. through ENISA).[154] ☐ Foster the use of common cyber security standards, assessment frameworks and technological tools.[155] ☐ Strengthen cooperation between EU and other national or international organisation (e.g. NATO, WTO, FBI, etc.). ☐ Join an international agreement with countries from which the majority of cyber-attacks are carried out (e.g. Obama-Xi agreement). ☐ Introduce more stringent cyber security laws and penalties for not compliant companies/organisations and to punish cyber criminals harder. If other, please specify: ☐	**CAT (III)** **CAT (IV)**
Q20	Would you consider beneficial to collect on a regular basis data on the volume and impact of cyber theft of trade secrets at EU level so that proper policy responses can be considered?	☐ Yes ☐ No	**All CAT**
Q21	Do you believe that it would be beneficial to have a system of volunteering reporting on incidents of cyber theft of trade secrets?	☐ Yes ☐ No	**All CAT**

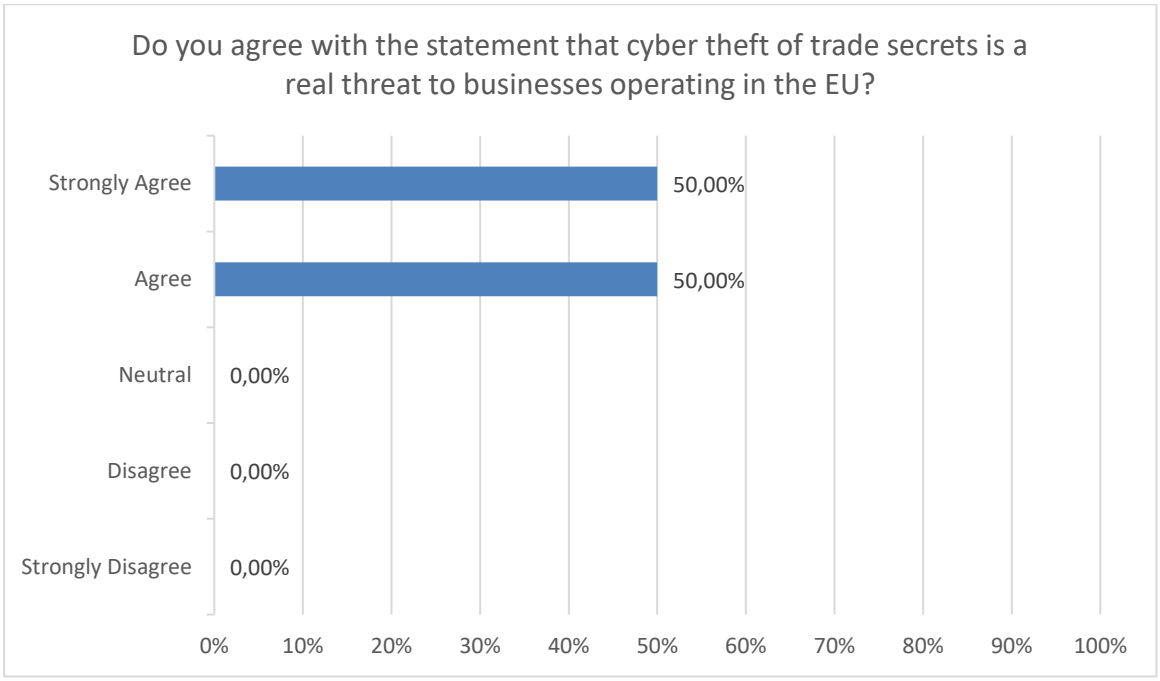
[154] Coordination between National regulators in EU agencies; Coordination between threat-focussed national security organisation; Coordination between Law enforcement agencies; Coordination between Computer Emergency Response Teams (CERTs).

[155] Cybersecurity standards define both functional and assurance requirements within a product, system, process, or technology environment. (E.g. ISO/IEC 27001, COBIT 5, NIST SP 800-53 Rev. 4, PAS 555, etc.). A Cybersecurity Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. Frameworks are often customized to solve specific information security problems or to be implemented in a specific industry sector. Cyber Security Frameworks (e.g. NIST CSF, Italian Cyber Security Framework, CIS Critical Security Controls, CIIP Framework, etc.). Technological Tools (e.g. Firewalls, Data Loss Prevention tools, SIEM systems, etc.).

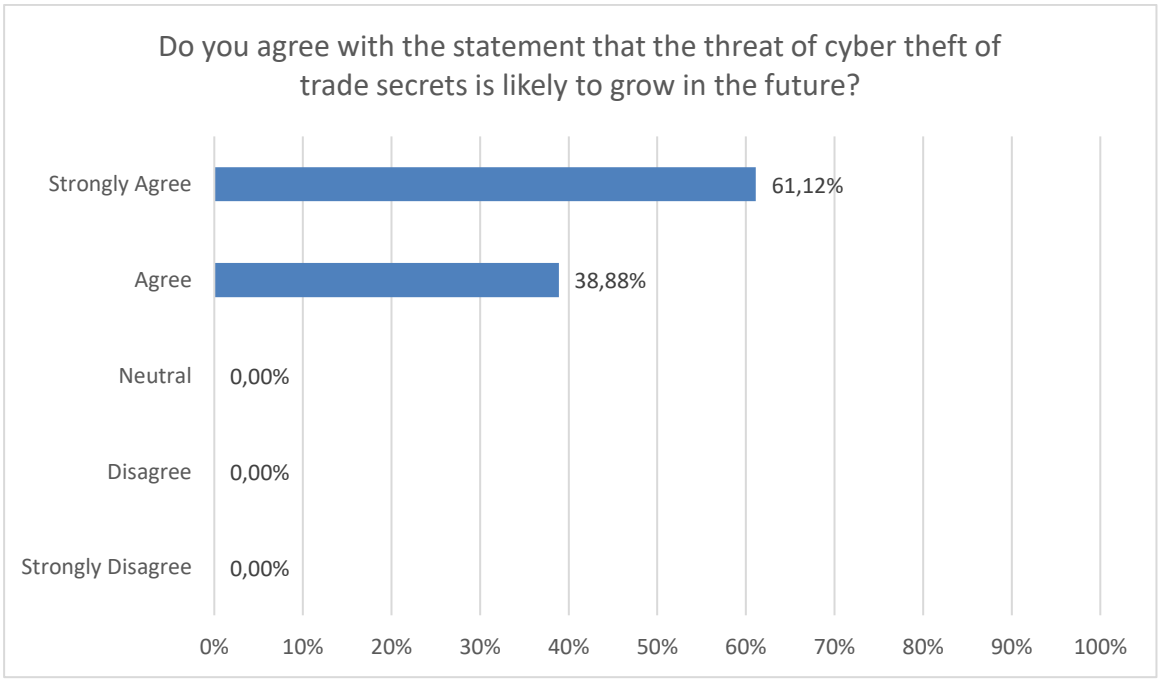
Survey Questionnaire			
Q22	To which organisation do you think the report should be submitted?	☐ National Law enforcement agency ☐ European Law enforcement agency (e.g. EUROPOL) ☐ Intelligence Services ☐ National Computer Emergency Response Team ☐ Computer Emergency Response Team for the EU Institutions, bodies and agencies (CERT-EU) ☐ European institutions (e.g. ENISA) or platforms If other, please specify: [ ]	**All CAT**
Q23	What do you think would encourage businesses to report the cyber theft of trade secrets to the authorities? Please rank the following options (1 should indicate the most relevant):	☐ Trust in the effectiveness of law enforcement at national level ☐ Receive sufficient confidentiality guarantees ☐ An easy notification procedure, using a user-friendly reporting template ☐ Possibility to receive timely information on cyber security trends, threat vectors, latest cyber-attacks, discovery of new vulnerabilities, best practices for cyber security. If other, please specify: [ ]	**All CAT**



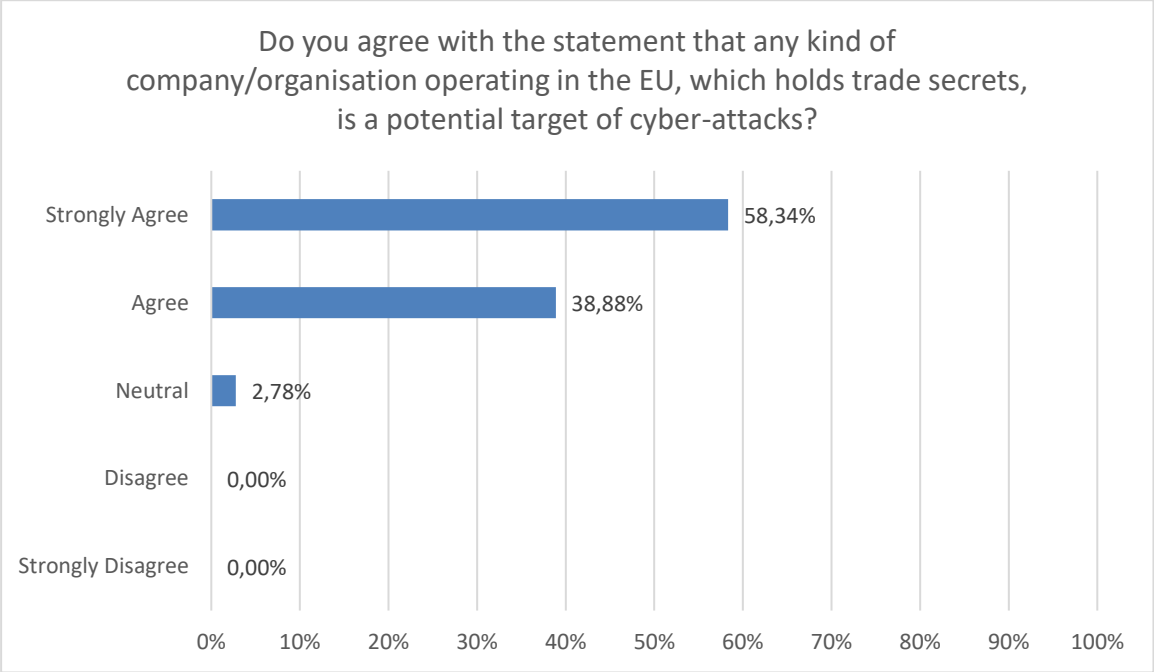
Q1.1


Do you agree with the statement that cyber theft of trade secrets is a real threat to businesses operating in the EU?
Strongly Agree
Agree
Neutral
Disagree
Strongly Disagree
50,00%
50,00%
0,00%
0,00%
0,00%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

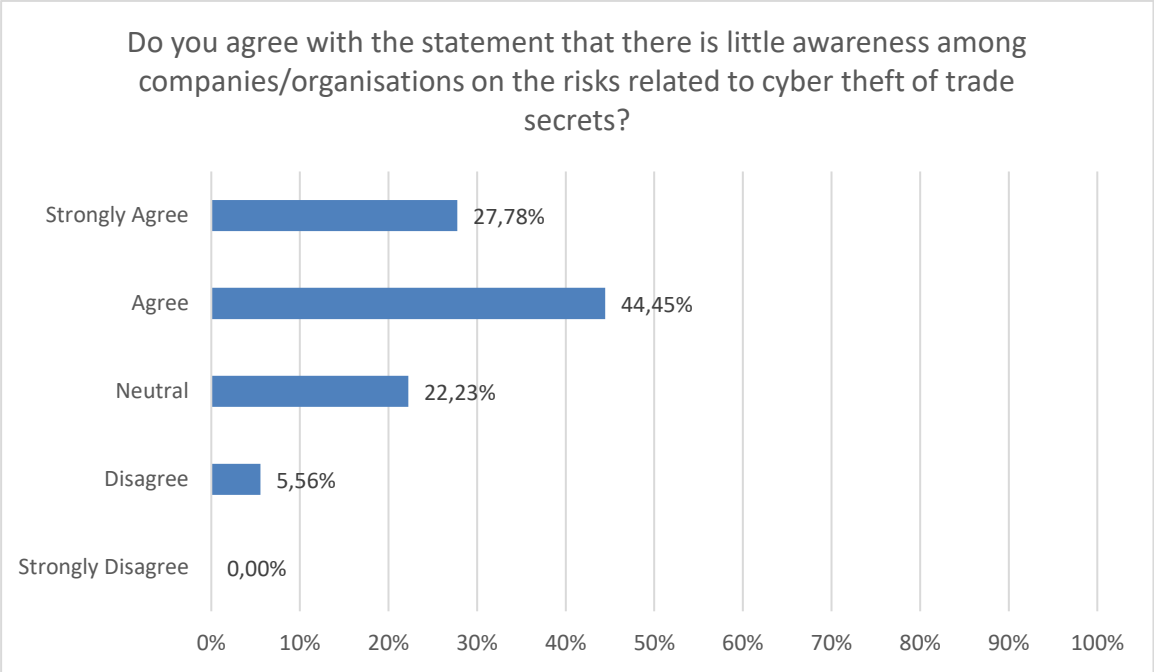
Q1.2


Do you agree with the statement that the threat of cyber theft of trade secrets is likely to grow in the future?
Strongly Agree
Agree
Neutral
Disagree
Strongly Disagree
61,12%
38,88%
0,00%
0,00%
0,00%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

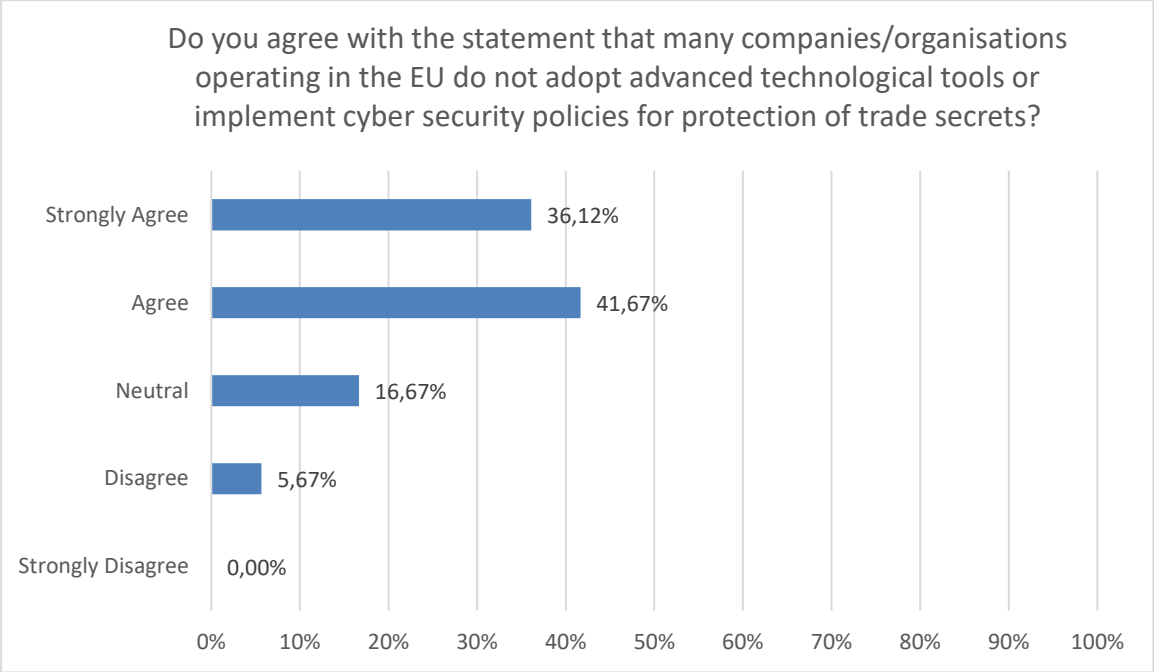
Q1.3


Do you agree with the statement that any kind of company/organisation operating in the EU, which holds trade secrets, is a potential target of cyber-attacks?
Strongly Agree
58,34%
Agree
38,88%
Neutral
2,78%
Disagree
0,00%
Strongly Disagree
0,00%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

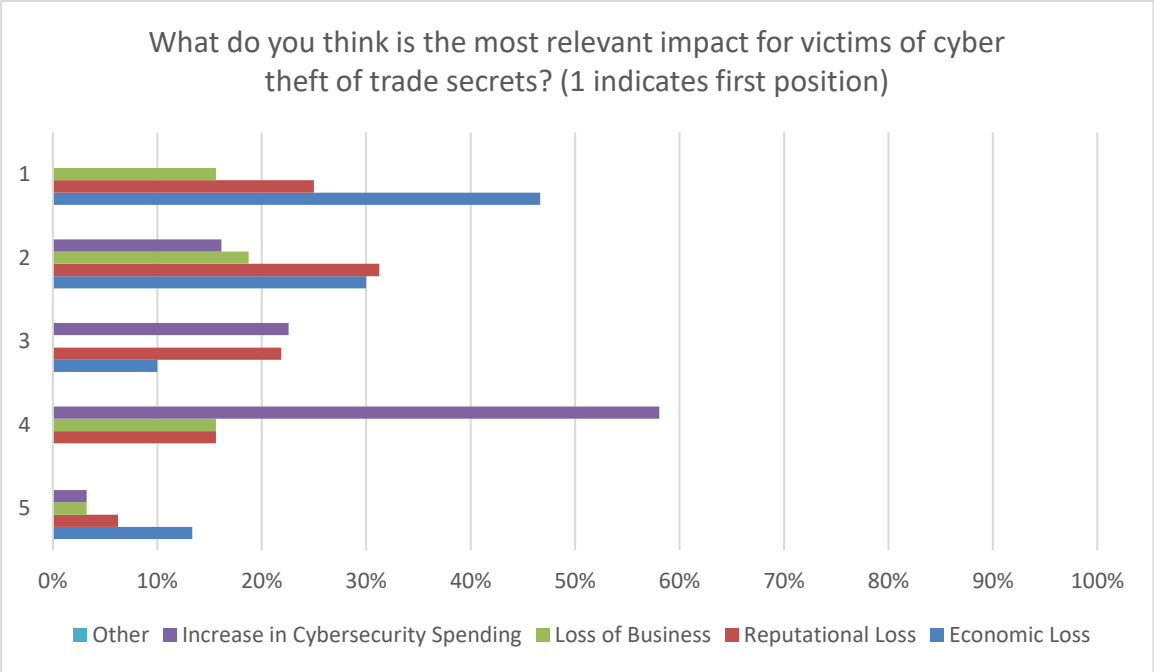
Q1.4


Do you agree with the statement that there is little awareness among companies/organisations on the risks related to cyber theft of trade secrets?
Strongly Agree
27,78%
Agree
44,45%
Neutral
22,23%
Disagree
5,56%
Strongly Disagree
0,00%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

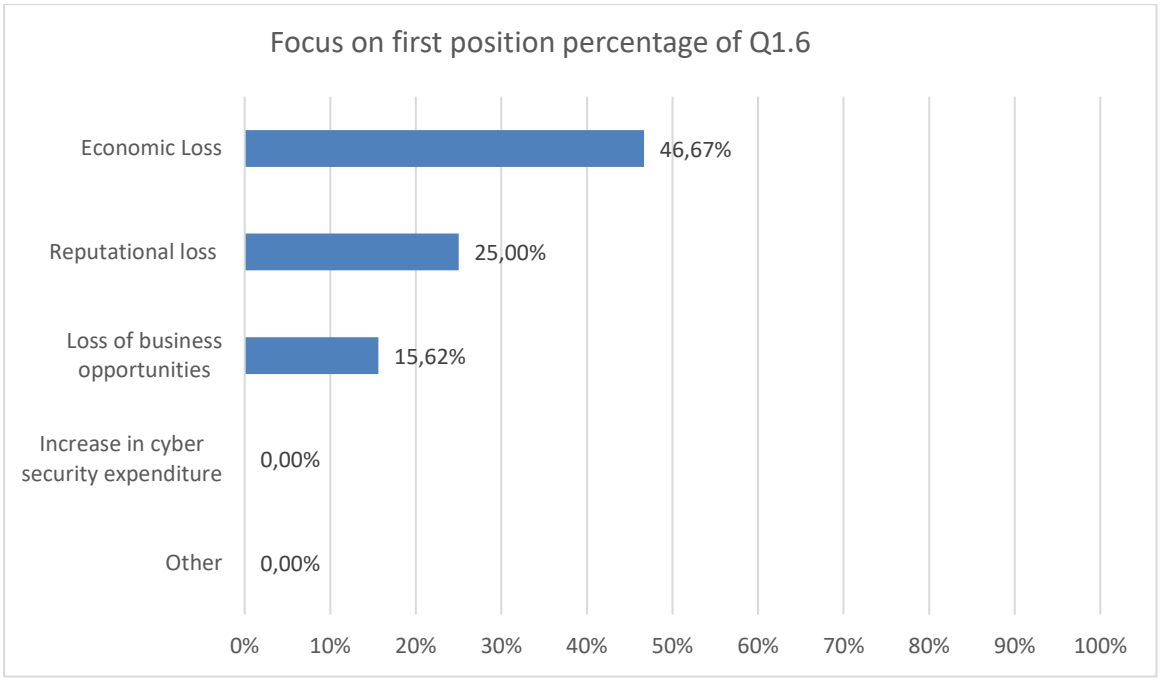
Q1.5



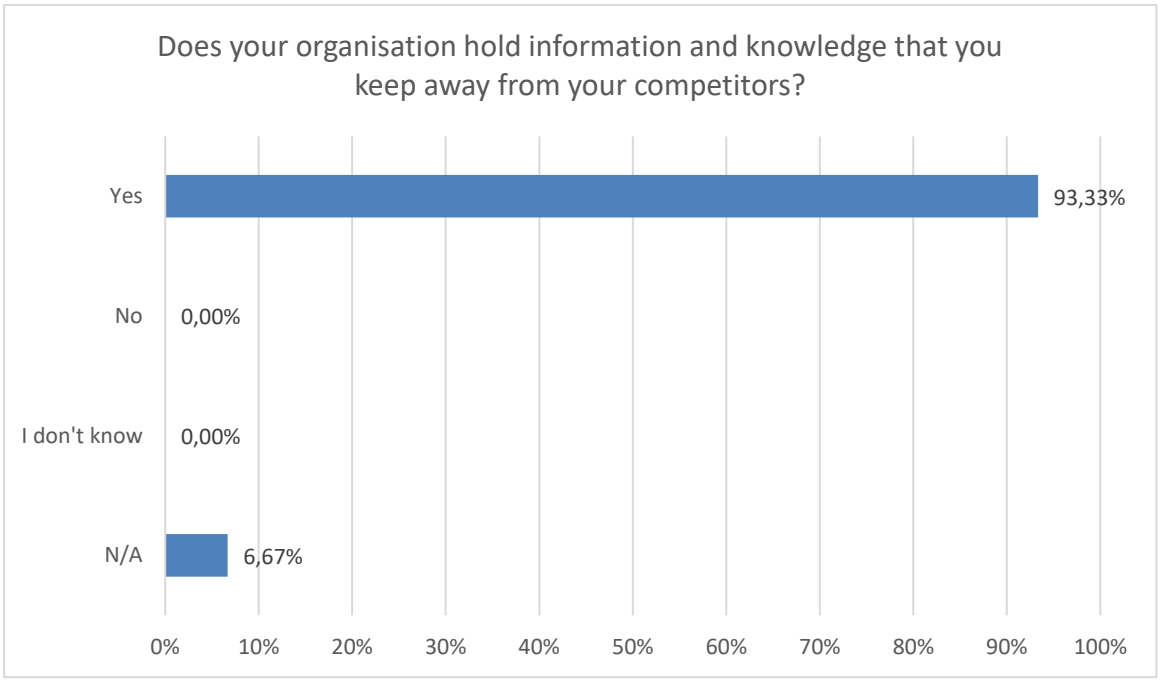
Q1.6



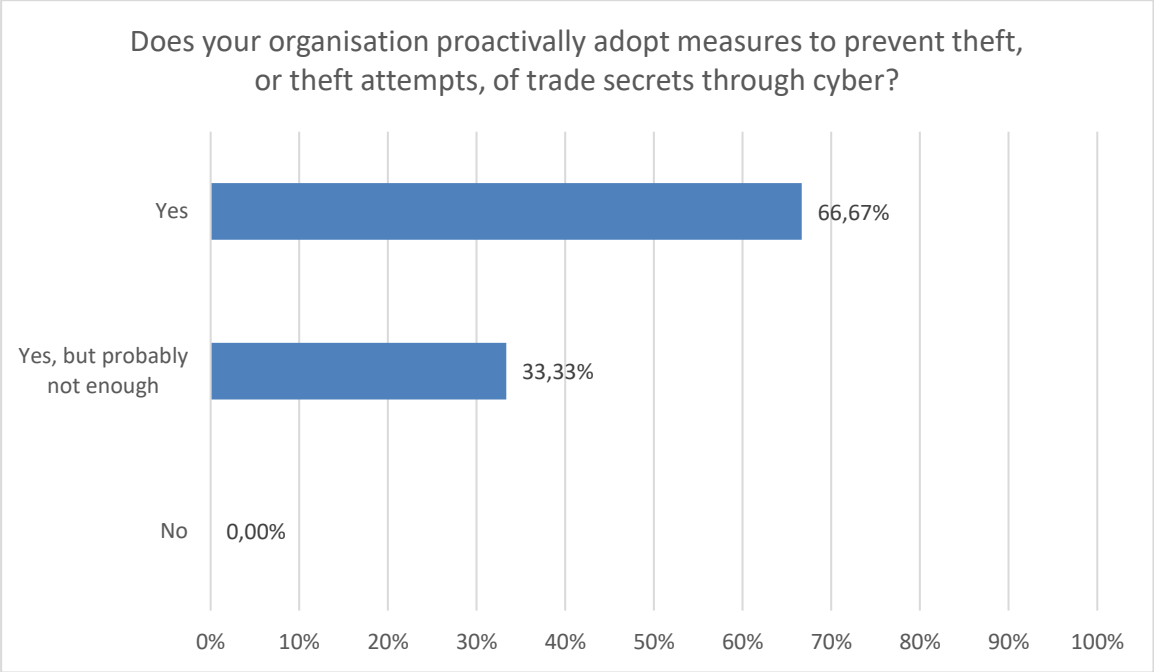
Focus on first position results:


Focus on first position percentage of Q1.6
Economic Loss
46,67%
Reputational loss
25,00%
Loss of business opportunities
15,62%
Increase in cyber security expenditure
0,00%
Other
0,00%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

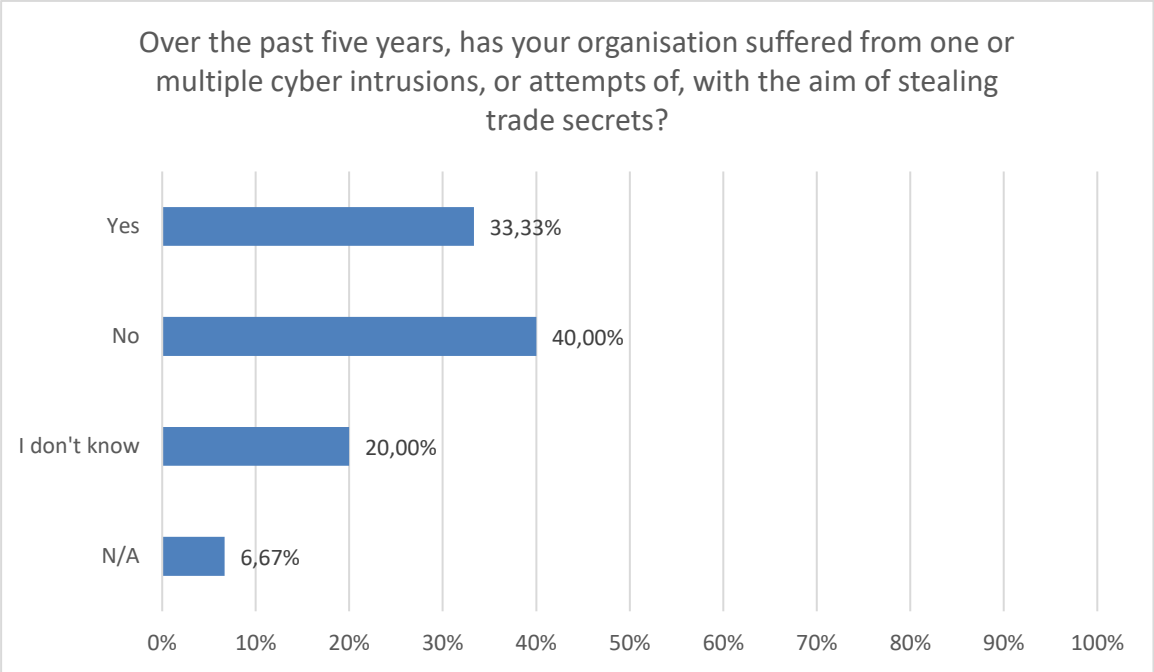
Q2.1


Does your organisation hold information and knowledge that you keep away from your competitors?
Yes
93,33%
No
0,00%
I don't know
0,00%
N/A
6,67%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

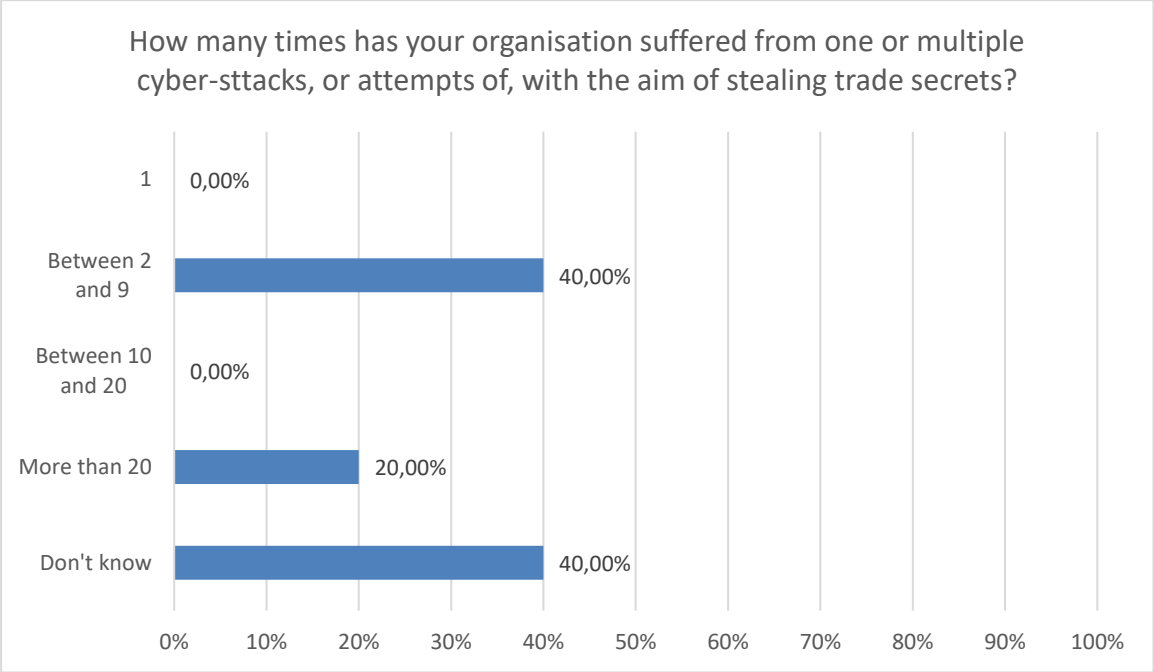
Q2.2


Does your organisation proactivally adopt measures to prevent theft, or theft attempts, of trade secrets through cyber?
Yes
66,67%
Yes, but probably not enough
33,33%
No
0,00%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

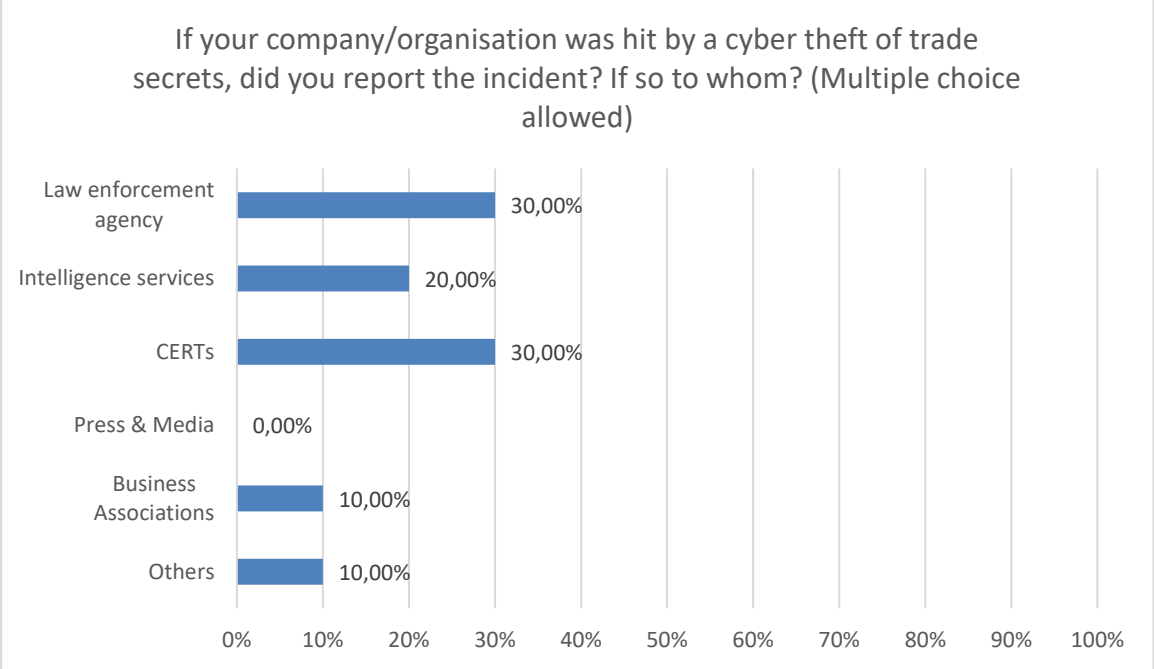
Q2.3


Over the past five years, has your organisation suffered from one or multiple cyber intrusions, or attempts of, with the aim of stealing trade secrets?
Yes
33,33%
No
40,00%
I don't know
20,00%
N/A
6,67%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

Q2.3.1


How many times has your organisation suffered from one or multiple cyber-sttacks, or attempts of, with the aim of stealing trade secrets?
1
0,00%
Between 2 and 9
40,00%
Between 10 and 20
0,00%
More than 20
20,00%
Don't know
40,00%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

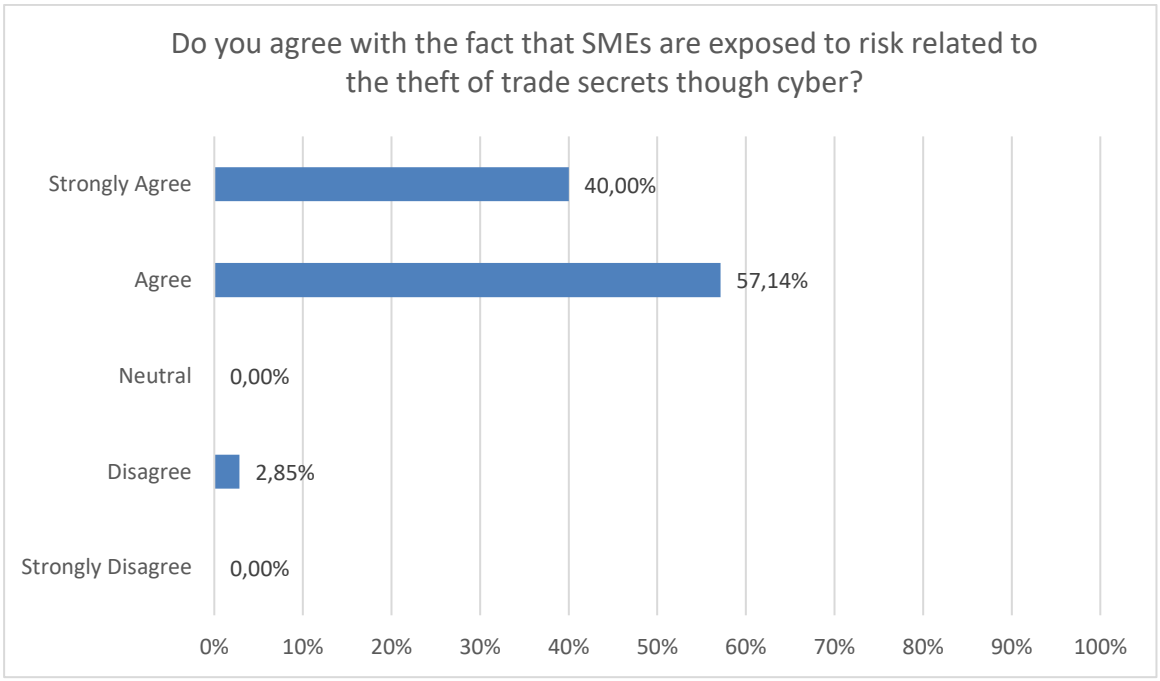
Q2.4


If your company/organisation was hit by a cyber theft of trade secrets, did you report the incident? If so to whom? (Multiple choice allowed)
Law enforcement agency
30,00%
Intelligence services
20,00%
CERTs
30,00%
Press & Media
0,00%
Business Associations
10,00%
Others
10,00%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

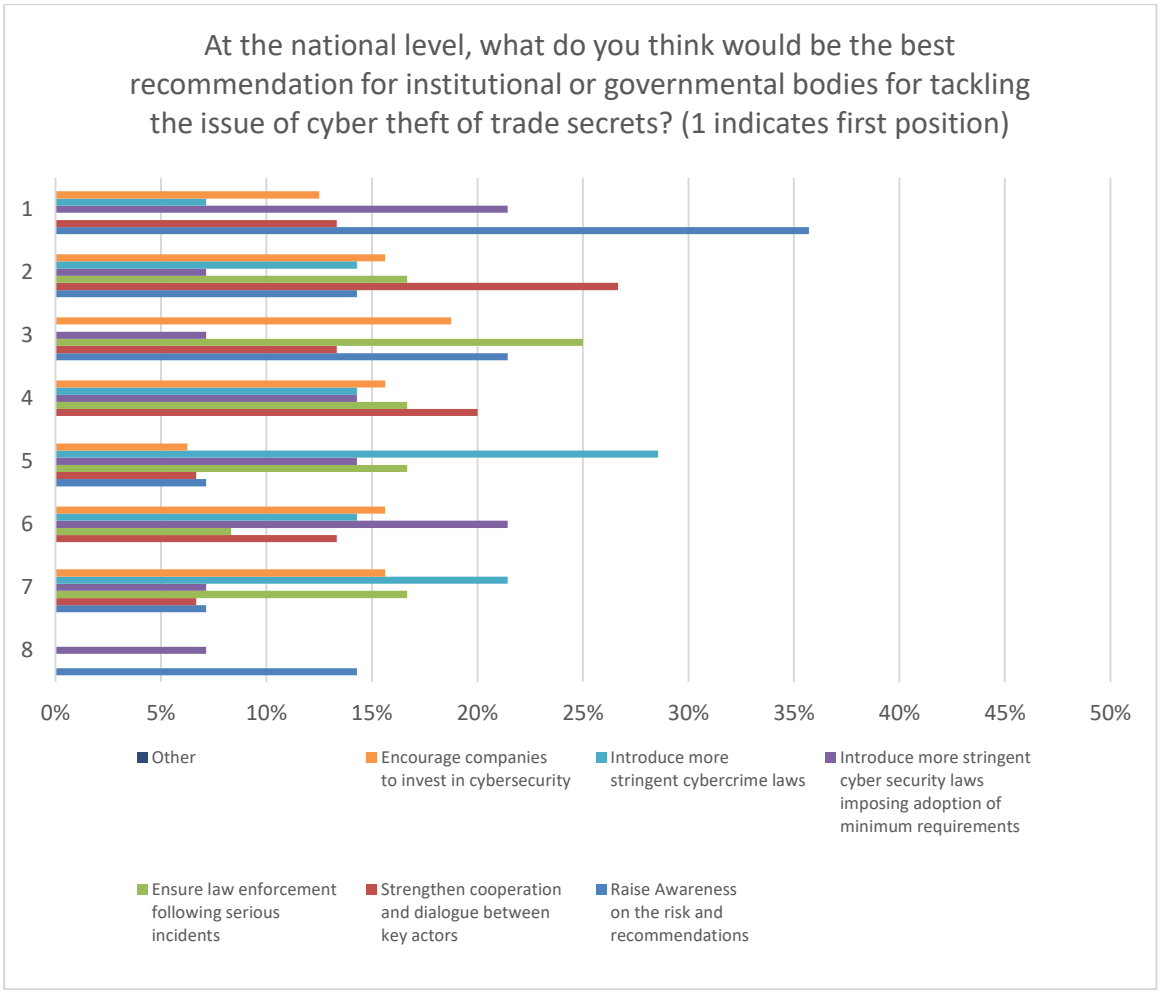
Q3.1


Are you aware of a case of more cases of a company/research organisation that suffered attemps or cyber attacks with the aim of stealing trade secrets?
Yes
52,95%
No
47,06%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

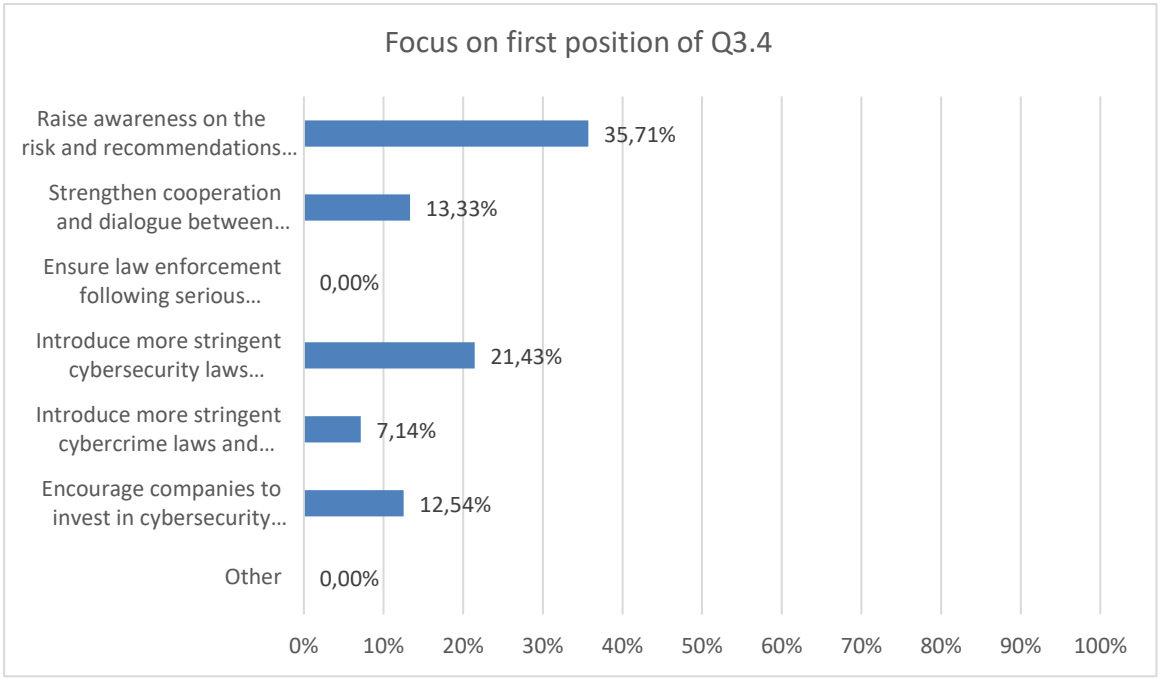
Q3.2


Do you agree with the fact that SMEs are exposed to risk related to the theft of trade secrets though cyber?
Strongly Agree
40,00%
Agree
57,14%
Neutral
0,00%
Disagree
2,85%
Strongly Disagree
0,00%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

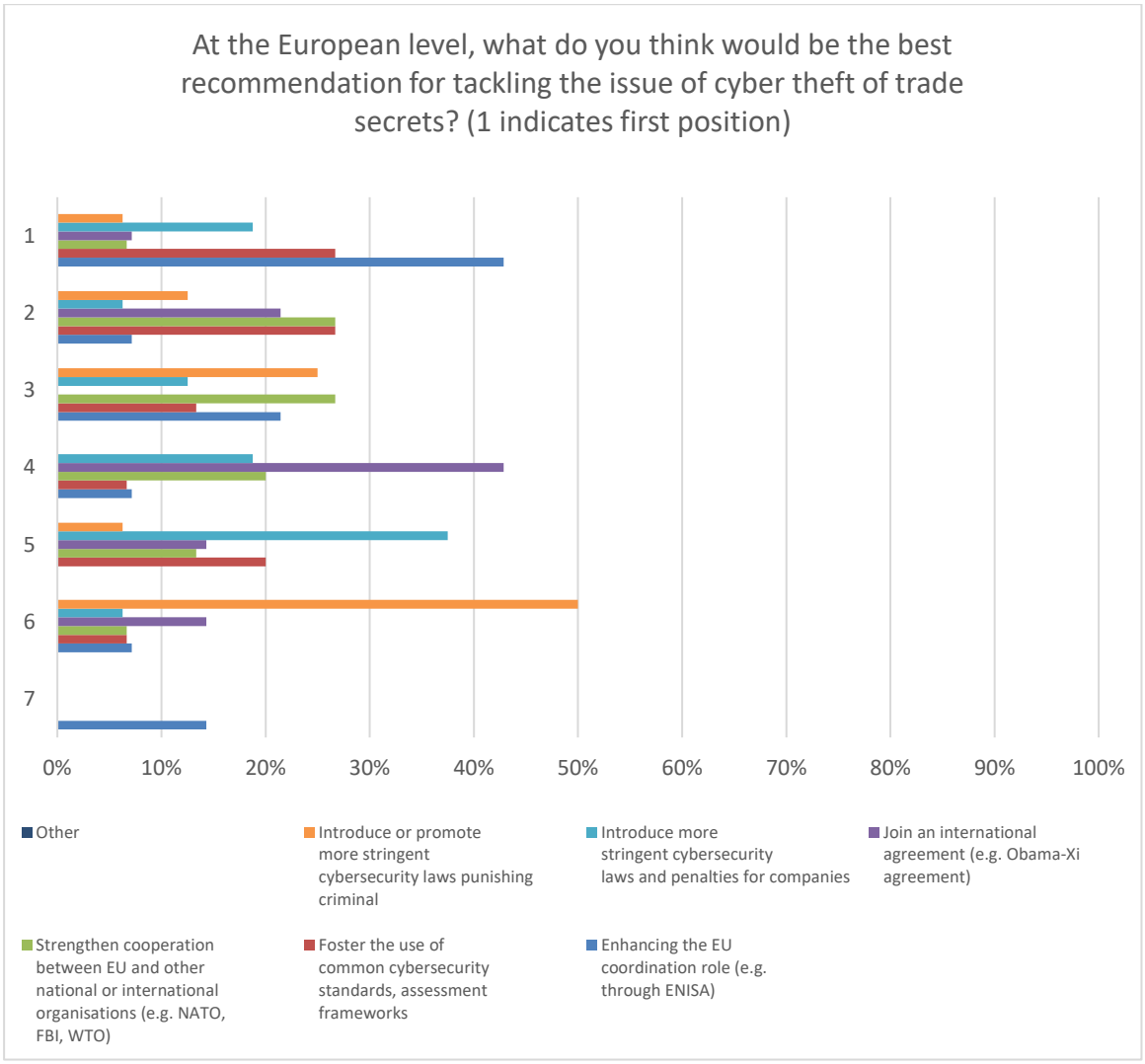
Q3.4



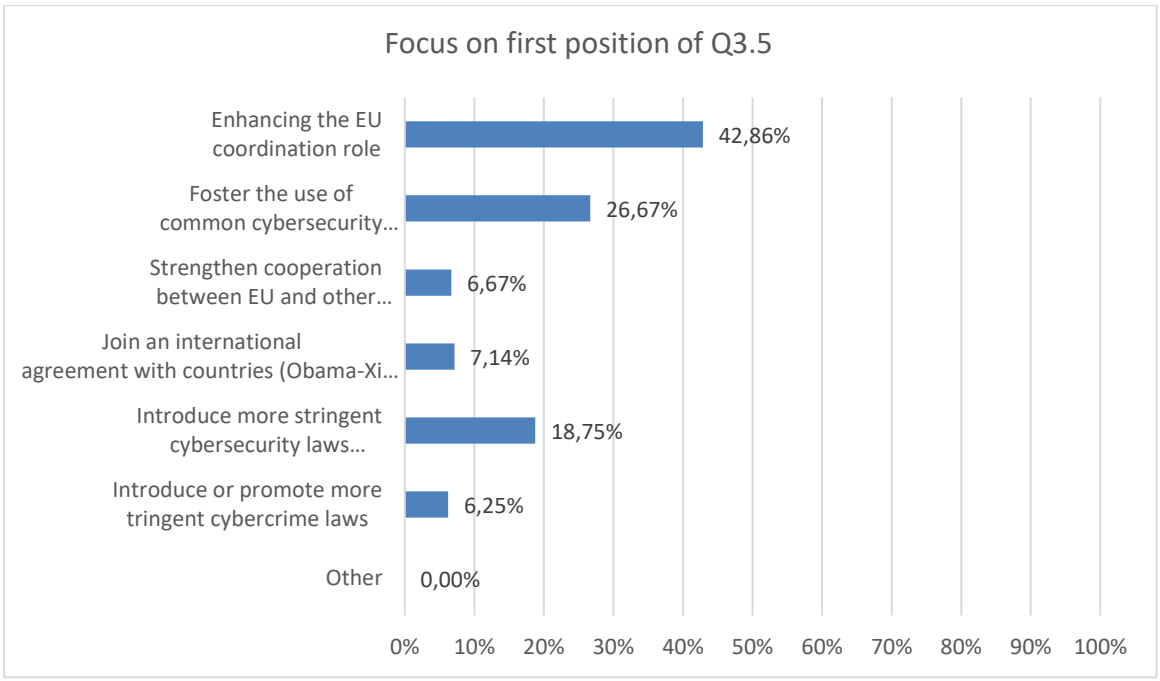
Focus of first position



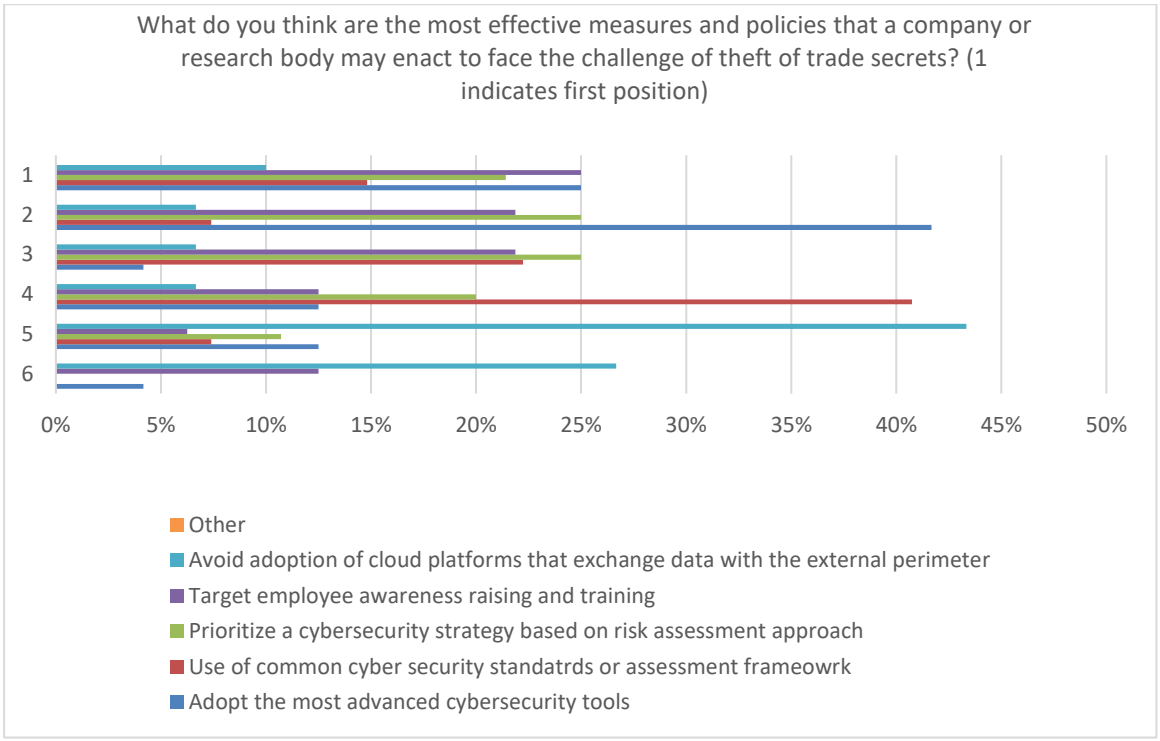
Q3.5



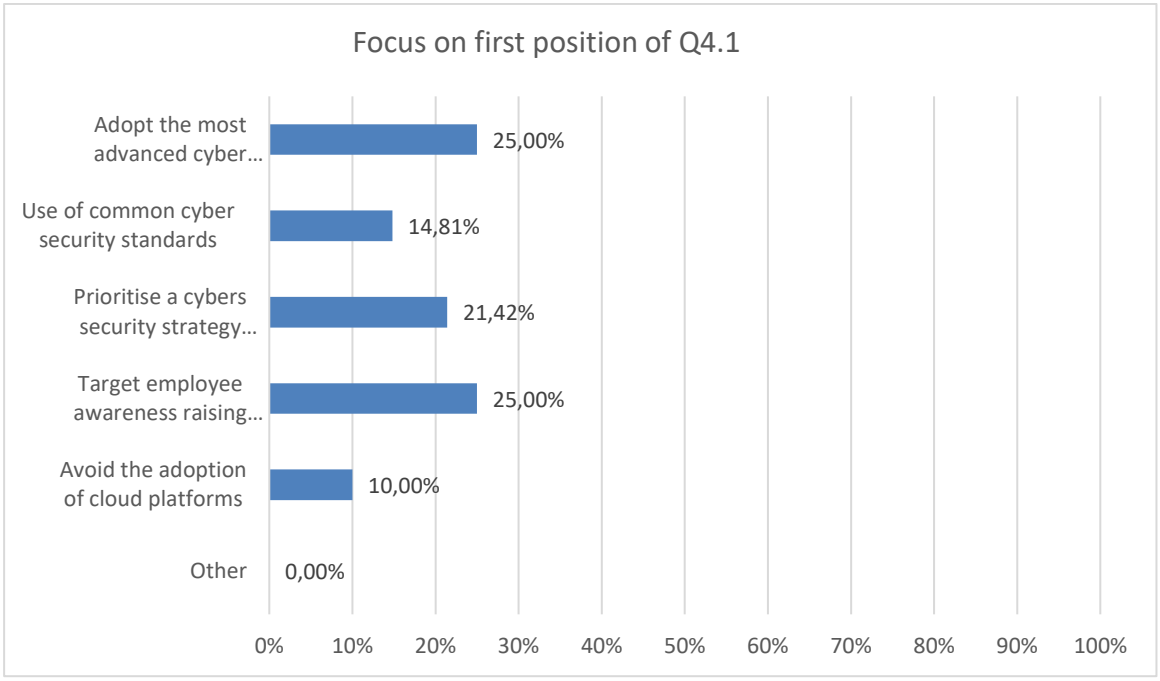
Focus on first position



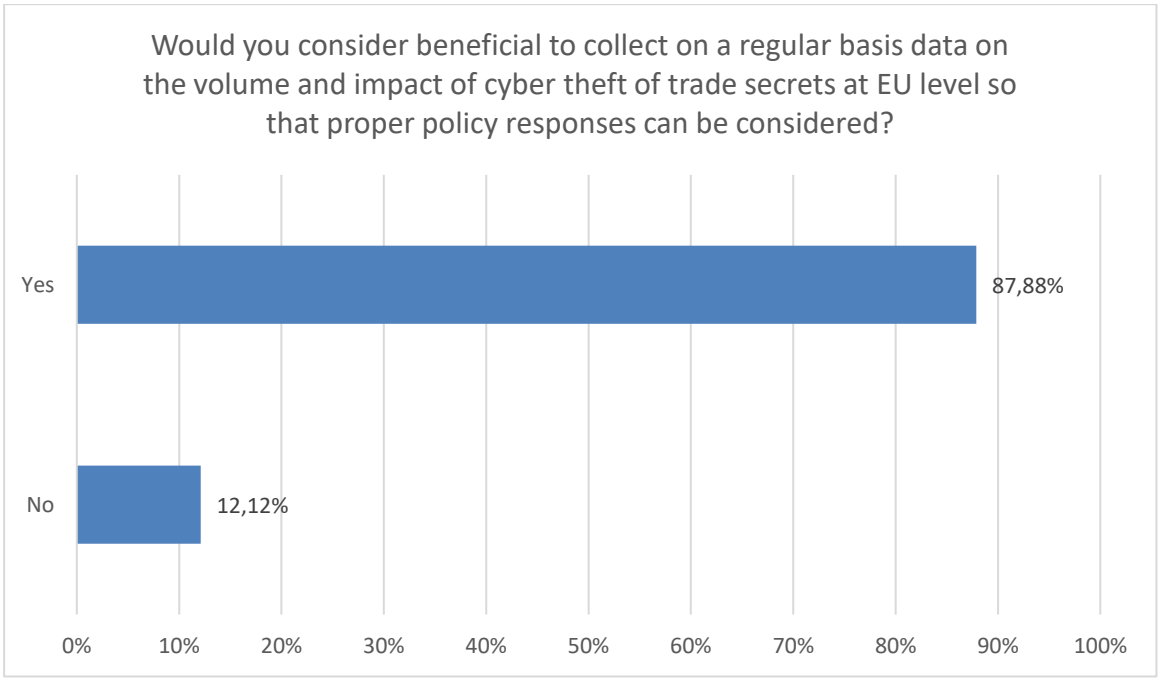
Q4.1



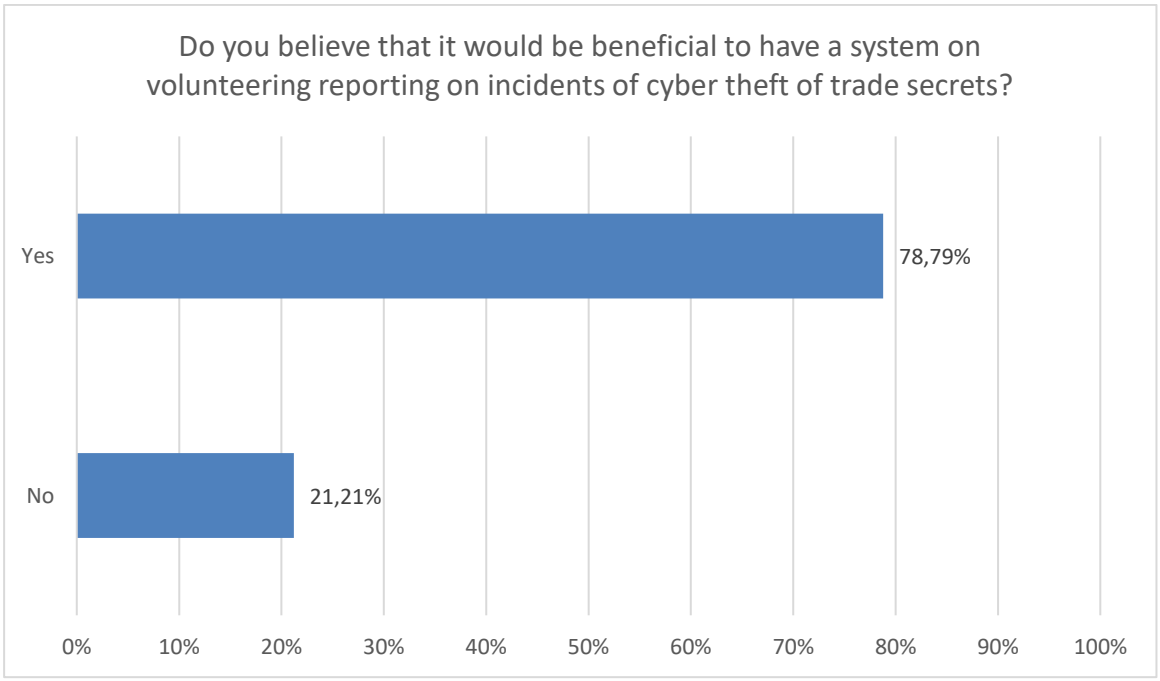
Focus on first position



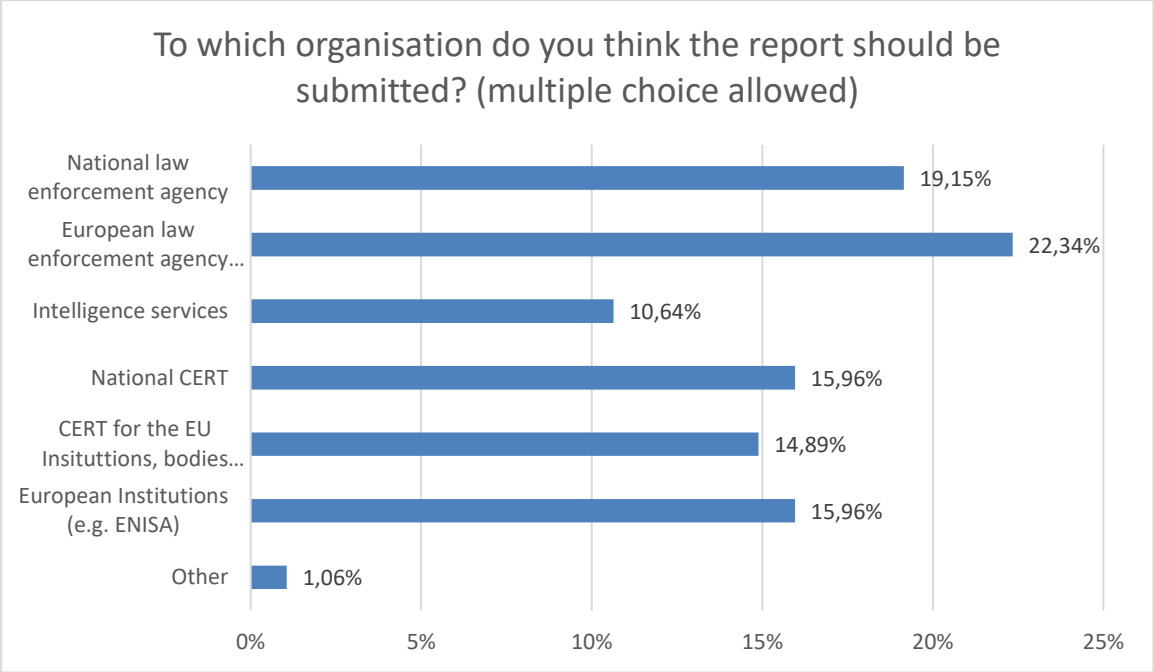
Q4.2


Would you consider beneficial to collect on a regular basis data on the volume and impact of cyber theft of trade secrets at EU level so that proper policy responses can be considered?
Yes
87,88%
No
12,12%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

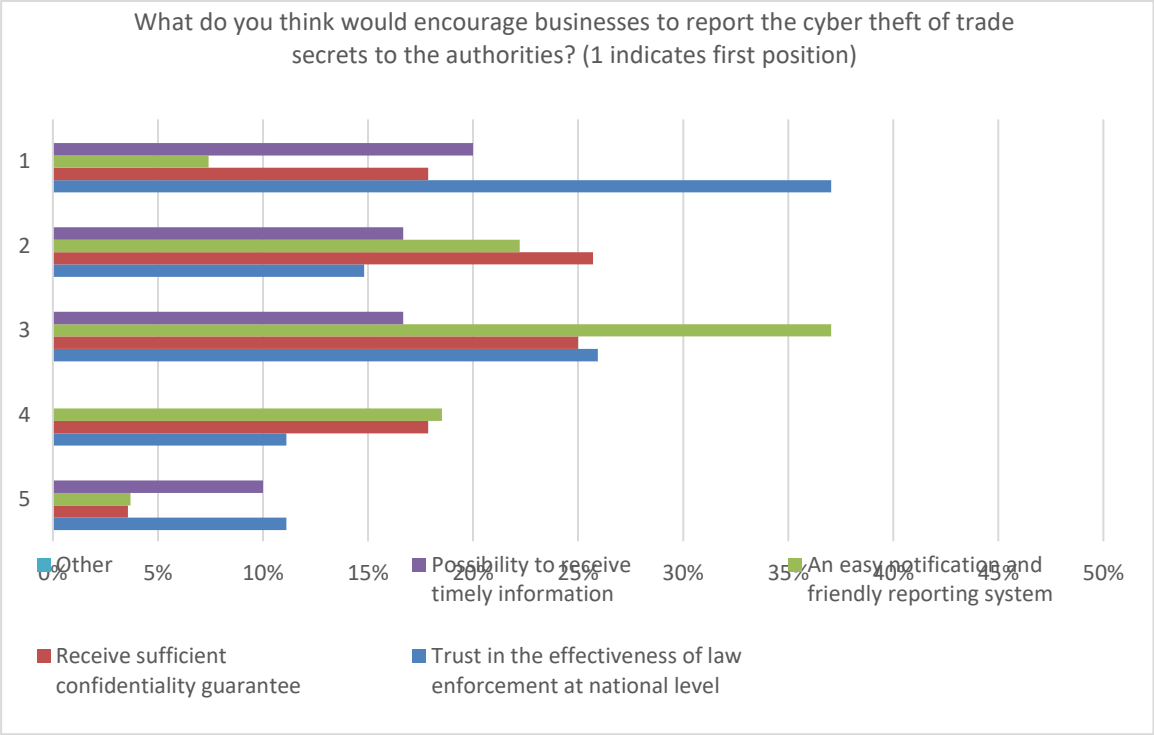
Q4.3


Do you believe that it would be beneficial to have a system on volunteering reporting on incidents of cyber theft of trade secrets?
Yes
78,79%
No
21,21%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

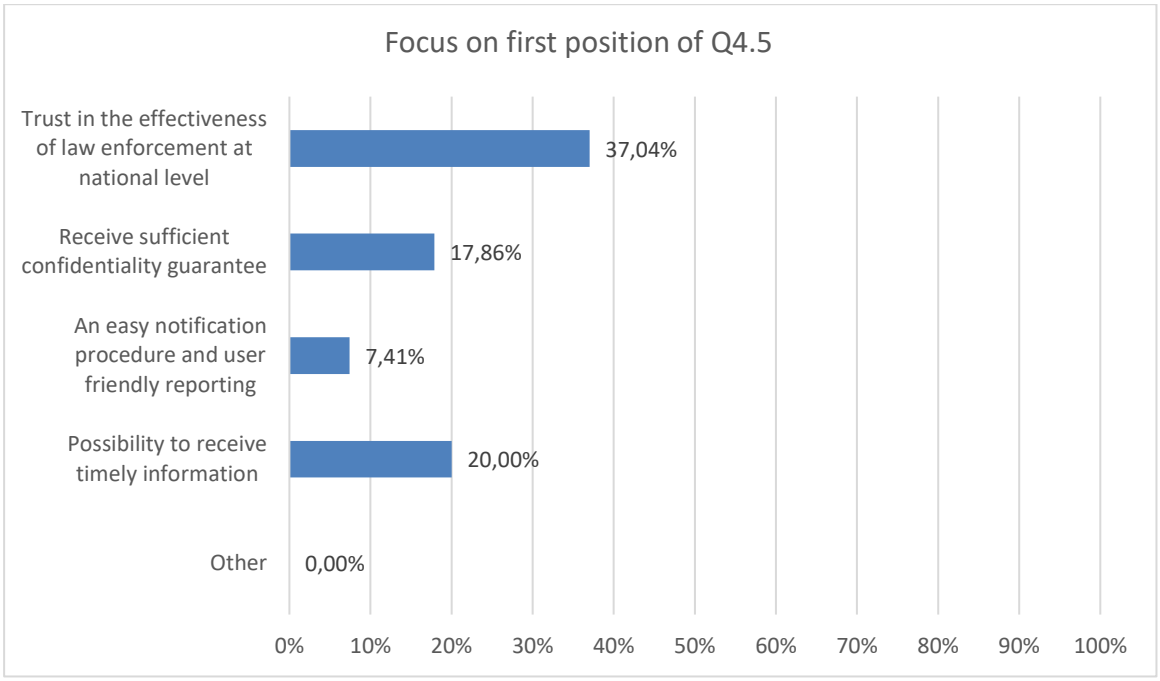
Q4.4



Q4.5



Focus on first position


Focus on first position of Q4.5
Trust in the effectiveness of law enforcement at national level
37,04%
Receive sufficient confidentiality guarantee
17,86%
An easy notification procedure and user friendly reporting
7,41%
Possibility to receive timely information
20,00%
Other
0,00%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

ANNEX E: WORKSHOP REPORT – INDUSTRIAL ESPIONAGE IN A DIGITAL WORLD

Presentation of the Workshop

The Workshop was organised as part of the study on the "Scale and Impact of Industrial Espionage of Trade Secrets through cyber" that PwC is carrying out for the European Commission DG GROW[156]. The main objectives of the event were to:

- Present the preliminary findings of the study to a restricted pool of experts;
- Share case studies and views of businesses and policy responses of a selected group of administrations
- Gather suggestions on how to improve recommendations developed in the course of the study

The Workshop took place on the 4th October 2018 in Brussels, within EU Commission premises (Rue de la Loi 102), from 9:30 till 17:15. In total some 50 participants attended, representatives of EU institutions and agencies; EU Member States; the US delegation in Brussels and private stakeholders from the Intellectual Property, Cyber Security and SME communities, from individual companies and associations both at national and EU level.

In order to meet the set objectives a restricted panel of relevant speakers was involved.

Workshop's speakers were Slawomir Tokarski, Director - Innovation and Advanced Manufacturing (GROW F), Giovanna Galasso, Director at PwC Government & Digital Innovation Team, Federica Magna, Manager at PwC in the Cybersecurity Unit, Alpha Barry - Head of Group Infrastructure & Security – ThyssenKrupp, Kris McKonkey - Global Lead for Threat Intelligence and Incident Response - PwC UK, Christopher Henny – Managing Director at Maxess Spr representing CSO Alliance and the Maritime Cyber Alliance, Patrick Grant - Digital Economy Adviser – Business Europe, Lucia Ling Ket On, The Netherlands, Permanent Representation to the EU, Wiktor Staniecki, Head of Cyber Sector, Security Policy Division, European External Action Service (EEAS), Stephen Purser, Head of Core Operations, ENISA, Agata Gerba, Deputy Head of Unit, Intellectual Property and Public Procurement, DG TRADE, European Commission, Susan Wilson, United States IP Attaché to the EU. The overall moderator was Harrie Temmink – Deputy Head of the Unit Industrial Property and Fight against Counterfeiting (GROW F3).

In the morning session PwC introduced preliminary findings. Afterwards a series of case studies and business views were presented on some critical cyber theft of trade secrets incidents.

In the afternoon session of the event, PwC presented preliminary recommendations of the study. The goal was to share findings and collect information from workshop participants.

[156] 622/PP/GRO/IMA/17/1131/9942

In the second part of the afternoon session all participants were divided in three groups, each assigned three main recommendation topics to discuss, namely:

i) prevention: awareness and standards/guidelines;
ii) data collection and reporting system;
iii) cooperation & enforcement

The discussions took place on the basis of papers with questions which were distributed in advance to participants. The discussion papers reflected the most relevant PwC draft recommendations.

All workshop participants reconvened in a plenary session. The moderators wrapped up the key outcomes of the discussion for the respective panels.

The full agenda below describes the different phases of the workshop.

The Agenda

	Morning session
09:00-09:30	Registration and Coffee
9:30-9:35	Welcome remarks • Slawomir Tokarski, Director for Innovation and Advanced Manufacturing, DG Internal Market, Industry, Entrepreneurship and SMEs (GROW), European Commission
09:35-10:00	Preliminary results PwC study "Scale and impact of industrial espionage and theft of trade secrets through cyber" • Giovanna Galasso and Federica Magna, PwC
10:00–11:15	Case-studies and business views • *Alpha Barry - Head of Group Infrastructure & Security – ThyssenKrupp* • *Kris McKonkey - Global lead for Threat Intelligence and Incident Response - PwC UK* • *Christopher Henny - Maxess Spr representing CSO Alliance and the Maritime Cyber Alliance* • *Patrick Grant - Digital Economy Adviser – BusinessEurope*
11:15-12:15	Government responses to industrial espionage • *Lucia Ling Ket On, The Netherlands, Permanent Representation to the EU* • *Wiktor Staniecki, Head of Cyber Sector, Security Policy Division, European External Action Service (EEAS)* • *Stephen Purser, Head of Core Operations, ENISA (by video-conference)* • *Agata Gerba, Deputy Head of Unit, Intellectual Property and Public Procurement, DG TRADE, European Commission* • *Susan Wilson, United States IP Attaché to the EU*
12:15-13:15	Lunch –EC building "Philippe le Bon" in Rue Philippe Le Bon 3
	Afternoon Session

13:15-13:30	Preliminary recommendations PwC study "Scale and impact of industrial espionage and theft of trade secrets through cyber" • Giovanna Galasso and Federica Magna, PwC
13:30-13:50	Next steps: brainstorming in sub-groups Introductory presentations Chris Henny, Alliance Maritime (on trusted reporting channels)
13:50-16:15	Topic 1 Prevention through awareness & standards/guidelines • Facilitators: José Daniel Ugarte (EASME) and Giovanna Galasso (PWC) Topic 2 Data collection • Facilitators: Jorge Novais (EC) and Giorgio Garbasso (PWC) Topic 3 Cooperation & Enforcement • Facilitators: Elena Kostadinova (EC) and Francesco Mureddu (PWC)
16:15-17:00	Wrap-up and discussion
17:00-17:15	Concluding remarks

Introductory greetings

Slawomir Tokarski - Director for Innovation and Advanced Manufacturing, DG Internal Market, Industry, Entrepreneurship and SMEs (GROW), European Commission

In recent years, the European Commission has been increasing its focus on the protection of trade secrets, considering in particular the growing global digitalisation that is introducing both new opportunities and new threats to European economic stability and growth.

The European Commission is working to introduce modern rules, collect information, spread awareness and design public policies to protect trade secrets. In 2016 the European Parliament and the Council adopted the EU Directive for the "Protection against the unlawful acquisition of undisclosed know-how and business information (trade secrets)". The Directive contains a number of key definitions and a common set of civil law remedies in case of misappropriation. But the threat of cyber theft of trade secrets is growing and more needs to be done to ensure that European companies will remain competitive. It is absolutely necessary to increase awareness on the problem and understand the real scale and impact of cyber theft of trade secrets.

Giovanna Galasso & Federica Magna - Preliminary results PwC study "Scale and impact of industrial espionage and theft of trade secrets through cyber"

The study team explained the different objectives of the study and the challenges they had to overcome. While it was easy to identify publications reports on cybersecurity in general, it was more difficult to find something specifically related to cyber theft of trade secrets. The reasons being clear: companies in Europe are not willing to disclose these kind of breach and there is a lack of information comparing those available from other continents.

Data available, such as the one quoted by ECIPE, estimate that in 2018 around €60 billion were lost in economic growth and 289,000 jobs due to cyber espionage in the continent. SMEs result among the weakest of European companies. No matter the nature of a SME's economic area, every company is seen as a lucrative target. Hackers are attracted not much by the gain that they can make but rather from the minimal effort needed to access SMEs' confidential data. Furthermore, cyber criminals often view SMEs as an entry point for intrusions against larger businesses. Many smaller businesses enjoy 'trusted partner' status with high profile enterprises – and criminals are increasingly keen to exploit those relationships. The so-called "supply chain attack" is one of the three most used techniques hackers put in place when penetrating an IT system.

As there is a difference in the number of intrusions depending on the size of the company, the same goes with the sector the business operates in. Manufacturing and ICT are indicated as the most affected by cyber theft of trade secrets. These are followed by financial and insurance activities as well as health and medical technology. Industrial sectors have, nevertheless, a different prestige depending on the member state they are located. As examples, the UK usually suffers more intrusions in its financial sector, while Italy's weakness lies in the luxury industry.

Businesses have an inadequate knowledge of the threat, which leads to their inability to detect intrusions. Even when detected, the time taken to identify what was stolen from the moment the intrusion took place is, in Europe, three times longer than in the average of all other continents – 469 days against 146.

The second phase of the study was based on stakeholders' engagement involving four categories:

- business,
- research bodies,
- cybersecurity experts,
- governmental bodies and think tank.

All stakeholders agreed on the growing trend of the threat. Among the most relevant factors impacting on the issue, Stakeholders identified:

- lack of awareness,
- rising online exposure,
- hackers' faster pace of malicious creation,
- Policy makers' slowness in facing the problem,
- technology advancement,
- geopolitical changes and globalization.

On the basis of the analysis carried out, awareness raising represents the basic step to foster companies' ability to protect themselves and increased the overall understanding of the issue at all staff levels. Once this first and fundamental goal will be implemented, also other measures shall be performed easier and better. Among these: governments' support to companies through funds and incentives; enhancement of IT risk management resilience

by assessing the future lost revenue and the intangible adverse impact; assessment of cybersecurity frameworks that could support in managing risks related to the cyber theft of trade secrets; cooperation among business associations.

In addition to the preventing measures, other actions can be performed to enhance the fight against cyber theft of trade secrets, intervening in mitigating current measures already adopted. In detail, law enforcement adjustments can be fulfilled, by creating an investigative ad hoc cybersecurity unit and providing for judges specialised in IP to decide on cases involving trade secret infringements.

Case-studies and business views

Case Study 1 – Alpha Barry - Head of Group Infrastructure & Security – ThyssenKrupp

ThyssenKrupp is one of the world's leading suppliers of carbon steel flat products. With around 27,000 employees, the company produces around over 13 million tons of crude steel per year – making it Germany's largest flat steel manufacturer. ThyssenKrupp's business operations are organized in five business areas: Components Technology, Elevator Technology, Industrial Solutions, Materials Services and Steel Europe. ThyssenKrupp is present in 79 countries and the growth and economic stability of the business is based on multimillion euros investments in R&D and their protection.

The Germany's largest flat steel manufacturer invest around 30-50 million € a year on central initiative on cybersecurity out of an IT budget of 1 billion euros.

Despite the relevant investments in cyber security, everyone can get hacked. Indeed, in April 2016, ThyssenKrupp's CERT identified a cyber intrusion into the systems: the detection took place 45 days after the start of the cyber-attack thanks to the monitoring activities of CERT technicians.

When investigating on the cyber-intrusion, they realized that hackers were going from one system to the other system until they found the information they were looking for. Their goal was likely to identify the servers containing files and R&D data.

There is no certainty as to whether and which R&D data was stolen, but the remediation alone costed around 5-10 million euros.

ThyssenKrupp adopted a proactive approach, informing media on what happened and reassuring customers. Communication and cooperation with law enforcement were of great benefit. They considered that it is indeed helpful to coordinate with prosecutors and law enforcement agencies that can help identifying the issue with intelligence researches.

The identity of perpetrators is not certain. The attack was conducted from outside the EU. ThyssenKrupp has some indications on the origin of the attack, but no conclusive evidence. Attribution remains a challenge.

ThyssenKrupp welcomed the European Commission activities to counter the threat of cyber theft of trade secrets and highlights the importance of training people with strong skills in cyber security, raising awareness on the issue and the importance to enhance international cooperation.

Case Study 2 – Kris McKonkey - Global Lead for Threat Intelligence and Incident Response - PwC UK

Starting in 2016, PwC UK has been investigating cyber espionage activities originating in particular from APTs based in China. In 2015-2016 numerous cyber espionage activities were recorded against the aviation industry: Chinese hackers were targeting industries that produce numerous aircraft components in order to steal their trade secrets and then manufacture the same components for the Chinese market.

In April 2018, PwC UK published a detailed report, "Operation Cloud Hopper", detailing cyber espionage campaigns conducted by APT10 – allegedly a Chinese cyber espionage group based in Tianjin. APT10 targeted Managed IT Service Providers (MSPs), demonstrating an unprecedented potential access to the IP and sensitive data of those MSPs and their clients globally. APT10 is considered one of the most significant industrial espionage threats in the world.

Operation Cloud Hopper leveraged on well-researched spear-phishing messages aimed at compromising MSPs. Multiple MSPs were both victims of the cyber intrusion and in particular the entry vector to penetrate the IT systems of their clients. Indeed, APT10 had such a persistent route going from the MSPs to their clients and then back to the providers to outsource information outside. The hackers used this technique to obtain legitimate credentials to access the client networks of MPSs and exfiltrate sensitive data.

Analysing the malicious activities of the Chinese hackers, it was possible to notice that the cyber-intrusions followed a pattern of working hours: the cyber-espionage activities started at 8:00 am until 12:00 pm, when the hackers took a "coffee break", to then resume from 13 pm to 17 pm.

Countries affected by the APT10 group include at least, the following: Brazil, USA, Canada, UK, France, Switzerland, Sweden, Finland, South Africa, and India.

Chinese APTs have attacked several sectors in the course of the years, showing interest for any kind of innovation, including: energy and mining, engineering construction, metals, industrial manufacturing, telecommunications and professional services.

To develop the report, PwC UK cooperated closely with law enforcement and intelligence agencies. The reluctance of companies to talk about this issue was among the main difficulties in conducting the study.

Case Study 3 – Christopher Henny – Managing Director at Maxess Spr representing CSO Alliance and the Maritime Cyber Alliance

The **CSO Alliance**, a maritime community of Company Security Officers (CSOs), **partnered with Airbus Defence and Space** to build a tailor-made and secure online reporting platform to help counter maritime crime on a global scale.

Shipping is a critical industry and Europe alone represents 1/3 of the entire shipping industry. Despite the shipping industry being important, most of the companies operating in this sector are small and medium enterprises. There are many systems digitally controlled that can be hacked in a ship, for example the cooling systems or the air conditioning systems. If the air conditioning system stops working, the engines of the ship will stop as well. Moreover, small and medium enterprises lack skilled personnel: usually they have only one person with IT capabilities.

There are different kinds of threats and vulnerabilities that affect the shipping industry. However, around 70% of the problem could be tackled through programmes and training courses for staff.

The second problem is related to the obsolescence of the IT systems: every time a new system is built upon an old system, a new hole is created and leveraged from hackers. The third problem is related to the lack of awareness on the issue.

The kind of cyber-attacks conducted against the maritime sector are: 77% malware, 57% phishing campaign, 23% spear-phishing campaign. The kind of data stolen are personal data and operational data (e.g. route plans, next ports, supplies to be ordered, fuel orders, etc.).

Talking about a reporting system for such kind of cyber-intrusion, Airbus/ CSO Alliance have developed an anonymous reporting system accessible via the internet.

Incidents reporting in the CSO Alliance works by sending information to some servers in Iceland. The anonymity of the transferred data is totally guaranteed. Users of the reporting platform benefit from alerts, news and assistance in the event of a cyber-intrusion.

Business View – Patrick Grant - Digital Economy Adviser – BusinessEurope

BusinessEurope is the leading advocate for growth and competitiveness at European level, standing up for cross sectorial companies and organizations across the continent and campaigning on the issues that most influence their performance. BusinessEurope represents companies in the international arena, ensuring that Europe remains globally competitive.

In recent years, cyber espionage has become a concrete threat for millions of people, who have fallen victim of such kind of cyber-intrusion. Indeed, Cyber security issues are affecting Europe on 3 principal dimensions: the geo-political dimension, the economic dimension and the personal dimension.

Businesses across Europe are constantly cyber-attacked and the cyber threat of trade secrets continues to grow.

Since 2010, many cyber-espionage campaigns have taken place. One example occurred in 2010, when Chinese hackers exploited vulnerabilities to cyber-attack 20 international companies. In 2011, through the use of hacking tools, businesses in the U.S. energy sector suffered cyber-intrusions. Also, many Danish IT companies suffered the theft of various sensitive data.

Once a hacker gets hold of such sensitive information, stealing for example blueprints, they immediately produce or give the possibility to place in the market identical products. Moreover, for businesses and organizations, understanding what information and data have been exactly stolen is very challenging. It is therefore important to properly prepare the European industry network to counter upcoming cyber-espionage campaigns. New forces are now coordinating such kind of cyber-attack and state sponsored actors are increasingly becoming dangerous for European economic stability.

Government responses to industrial espionage

Lucia Ling Ket On - The Netherlands, Head of Unit Justice and Security Affairs Permanent Representation to the EU

State sponsored cyber-attacks are increasing and there are several countries that are conducting these kind of cyber-espionage activities. At the same time cyber-attacks are

becoming increasingly complex. In the Netherlands, companies in different industry sector such Energy, Hi Tech and Chemical, are suffering cyber espionage the most. In the digitalised context where companies work, terabytes of confidential data are stolen, representing potential economic failures.

In April 2018 The Dutch Minister of Justice and Security presented the new National Cyber Security Agenda, consisting of ambitious challenges.

The Netherlands is at the forefront of digital secure hardware and software, has successful barriers against cybercrime and leads the way in the field of cyber security knowledge development. Such challenges will be addressed considering the public-private cooperation environment, creating a platform in which they can cooperate. The Netherlands wants to raise awareness with all relevant partners (central government, regional, local and private partners including critical infrastructures).

The Netherlands also employs diplomatic tools to address the issue. The Dutch intelligence and secret services agency have organized about 200 workshops to promote measures to protect relevant information for national security. The Dutch government also published guidelines to coordinate and publish vulnerabilities disclosures, noting that there is an increase in cyber espionage activities.

Chris Gow – Director, EU Public Policy, Government Affairs at Cisco and Member of the Board at DigitalEurope

During the panel discussion, there was the presentation of a practical case study of cyber-espionage. This was developed by Talos, one of the largest commercial threat intelligence teams in the world, comprised of world-class researchers, analysts and engineers. The Talos teams share lots of information and telemetry with their clients, securing enterprises all over the world with more than 20 billion threats blocked.

Today, it is possible to discuss two examples of harm: cyber-espionage and cyber-sabotage. Cyber-espionage consist in stealing information, while cyber-sabotage attempts to disrupt the network or the operations of a business. There are also different kinds of threat actors: Delinquents, Criminals, and APTs. APTs are often state actors or state affiliate actors with geopolitical aims. Behind an attack there is always someone trying to achieve an objective. Another kind of threat, and probably the most common one, are employees.

In 2017 CCleaner suffered a massive supply-chain malware attack, where hackers compromised the company's servers for more than a month and replaced the original version of the software with the malicious one. Hackers were spying on specific type of users, spying on institutions and organizations. During the installation of CCleaner 5.33, the 32-bit CCleaner binary that was included also contained a malicious payload. This led to 2.3 million of devices being infected and 20 High Tech companies targeted (e.g. Google, Microsoft, IBM, Cisco etc.). Avast, with the help of the FBI, was able to shut down the attackers' command-and-control server within three days of being notified of the incident. The identity of the perpetrators is uncertain but the attack was carry out reusing the malicious code from APT72, a China based actor. APT72 is a group, presumably state-sponsored, affecting primarily Tech Companies in USA and south-east Asia.

Steve Purser, Network and Information Security Expert – ENISA

ENISA presented the current Cyber security policy context from their perspective. ENISA has a role in the preventive sphere only. In other words it has no role in the response dimension. At present, ENISA is composed of 83 people and works hand-in-hand with Member States, governments, public and private sectors.

ENISA works on three main areas. The first consists in the release of recommendations and papers to advise governments on their standing with regard to cybersecurity. Secondly, it supports the formulation of policies related to cybersecurity and their implementaton. Finally, it implements a hands-on approach by, for example, organising the "CyberChallenge" with Universities across the EU.

ENISA is now working on aligning industries through pragmatic solutions, to reduce the cost for businesses when they suffer a cyber-security breach.

Looking at the current cyber security policy, it is possible to note two major streams: the CIP resilience stream and the GDPR one. They work together well but are not based on the same principles and the same approach. Moreover, in 2013, the new cyber security strategy introduced the NIS Directive. In general, it is possible to note a quite good stream of policies but there are some aspects that are not covered. Indeed, ENISA believes that in the next decade some aspects will impact the cyber security context:

- Enhancing cybersecurity skills. It is extremely important to have more skilled people in cyber security. There is a need for skilled people able to use security technologies properly;
- There is a general lack of understanding of the economic drivers of cyber security. Cyber security will be a fundamental economic opportunity and issue for Europe;

Wiktor Staniecki - Head of Cyber Sector, Security Policy Division, EEAS

Digital transformation is introducing new opportunities but also new security challenges to consider. As explained by the PwC Study, the clandestine acquisition of trade secrets is becoming easier thanks to cyber means and, in this context, it is important to consider foreign relations because many cyber-attacks have also a geopolitical goal. .

Cyber theft of trade secrets is not yet fully addressed, especially regarding the impact on national security. It is difficult for individual countries to understand the scale and the impact of cyber-theft of trade secrets. For the complexity of the issue and the sensitivity of data exposed, public and private bodies are often reluctant to share information on such incidents. The attribution is also very rare in such cases. Trust, knowledge sharing and cooperation are key words in this sense.

Last year, the "cyber diplomacy toolbox" set up a framework in order to push for a joint EU diplomatic response to malicious cyber activities. Cyber diplomacy toolbox is a framework for mitigation of cyber security threats and it is expected to encourage cooperation, facilitate mitigation against medium and long-term threats.

Agata Gerba – Deputy Head of Unit, Intellectual property and Public procurement – DG TRADE

Industrial espionage is an area largely unregulated under international law, which poses a number of problems for states intending to challenge another state for industrial espionage. A number of aspects need to be considered as part of such challenge: whether the state acts against a company established in the state's territory or against a company in another state (and consequently whether domestic or international law applies), the principles of state sovereignty and state immunity, the level of protection of trade secrets in the domestic law of the state in question and available remedies, etc.

As regards international rules, Article 39 of the TRIPS Agreement provides a possible legal basis for cyber theft of trade secrets. It states "In the course of ensuring effective protection against unfair competition, Members shall protect undisclosed information in accordance with paragraph 2 and data submitted to governments or governmental agencies in accordance with paragraph 3. Natural and legal persons shall have the

possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices…"

This means that natural or legal persons should have the possibility of preventing information lawfully within their control from being disclosed without their consent. A number of questions arise in this context: can this provision be read as a prohibition of economic espionage by a state? In other words: does a state violate Article 39 when it engages in industrial espionage? Could it apply to industrial espionage in another country? There is certainly potential to rely on Article 39. But to do so it is important to have evidence. Finally, a question to consider is whether new rules taking into account developments in digital technology are not needed to properly address the problem of industrial espionage.

Susan Wilson, US IP Attaché for the European Union and European Commission

The US government is committed to support the European Commission in the fight against cyber theft of trade secrets, as this is a shared threat. The European Commission and the US should not be discouraged in the fight against cyber theft of trade secrets given that there is much more to do to prevent such kind of incidents. What is most important is to focus the attention on specific problems and prioritize them; if the attention is on multiple problems it will be difficult to solve them.

An American Superconductor called EMC was hacked by a Chinese state sponsored hacker stealing software. The theft resulted in the loss of 700 jobs, including jobs from its Austrian subsidiary, and the loss in stock value for over one billion dollars.

In the United States, cyber issues related to the protection of intellectual properties have been discussed and taken into consideration for the past 30 years. As there are not enough economic data on cyber theft of trade secrets, it is important to have a dialogue and share information as much as possible. Sharing information is relevant in order to establish a reporting system, although it does not help in defining how to structure the system, leaving the question of having a mandatory or voluntary system open.

Any success that could be reached in this field directly translate in a more secure economic stability in the future.

Christopher Henny – Managing Director at Maxess Spr representing CSO Alliance and the Maritime Cyber Alliance (second speech on trusted reporting channels)

CSO Alliance developed an online cybercrime reporting platform for the maritime sector. Through the use of the reporting platform, it is possible to report cyber-attacks in a totally secure and anonymous manner accessible and usable by everyone – and not just by IT professionals. The average time to report an incident is about 1 minute. The reporting platform also generates statistics, discovering criminal trends, and offers the possibility to the CSOs members to collaborate globally against cybercrime. Information asked to report a cyber-attack includes:

- Date and time;
- Incident location;
- Country;
- Nearest port;
- Type of attack;
- Impact;
- Consequence of attack;

- Severity of attack;
- Estimated cost.

Businesses are aware that it is impossible to calculate the risks unless statistics are provided to prove that theft of trade secrets takes place. Without properly calculating the risks it is also impossible to establish an insurance policy. A reporting scheme allows to build a critical mass of data that can help predict the risks and, in case of confidential data, it provides forensic capabilities. Insurance companies also need to have an understanding of what is the infringement and who are the perpetrators. CSO Alliance believes that a reporting scheme must remain voluntary.

Preliminary recommendations PwC study "Scale and impact of industrial espionage and theft of trade secrets through cyber"

Preliminary PwC recommendations were presented in the afternoon session. These were described according to four clusters:

- Awareness and Training
- Facilitate businesses in addressing the challenge
- Enhance Institutional Capabilities
- Strengthen Law Enforcement

Awareness and Training

Strengthen management-level awareness of the risk of cyber-theft of trade secrets.

- Organise targeted events.
- Disseminate content via multi-media sources.
- Disseminate case studies among senior executives.
- Provide a public repository of best practices and guidelines.

Increase awareness of policy makers and high-level officials of the risk of cyber-theft of trade secrets.

- Strengthen communication campaigns to policy-makers
- Organise high-level meetings and roundtable events.

Boost training of professionals and relevant civil servants.

- Support the creation of multidisciplinary teams responsible for cyber theft of trade secrets.
- Establish regular training and certification.

Facilitate businesses in addressing the challenge

Encourage and support SMEs to invest in prevention and countermeasures.

- Consider the opportunity of funding a study on the impact of cyber theft of trade secrets for SMEs only.
- Provide incentives to SMEs.
- Disseminate guidelines for SMEs.

Push the development of new tools and technologies.

- Increase public funding in research and innovation;
- Boost private funding in research and innovation.

Promote collaborative innovation at sector level with cooperation between established businesses and start-ups

Enhance Institutional Capabilities

Foster the use of common cybersecurity standards and assessment frameworks.

- Adoption, implementation and support for a common assessment framework.
- Develop a tool-kit supporting businesses in identifying, classifying and protecting their confidential information.
- Consider the adoption of a framework for the assessment of value of trade secrets.

Strengthen institutional capabilities.

- Strengthen the role of ENISA.
- Foster the role of the CSIRTs network.

Strengthen cooperation between key players as well as with other national or international organisations and governmental entities.

- Foster cooperation on prevention of cyber theft of trade secrets with national and international organisations.
- Engage in bilateral negotiations and agreements.
- Strengthen cooperation and dialogue between key players.
- Push for a renewal in the international debate on FIN 48 IFRS[157]. Consider a tax relief provision for companies complying with certain safety standards. In this regard, the European Union should coordinate the elaboration of a common position for Member States, fostering a greater international consensus calling for the adoption of the measures.

Strengthen Law Enforcement

Introduce more stringent cybersecurity laws and penalties.

- The EU and national authorities could build on the existing legislative framework to produce as an addendum guidelines and tool-kits directing companies in properly addressing the challenge.

Consider the purposefulness of adopting a system of reporting and notification of incidents.

- Consider the adoption of a reporting system at EU level;
- Define a pilot reporting system for a specific industrial sector.

Boost investigation capabilities at national and European level to counter cyber theft of trade secrets.

- Create a National Cybersecurity Investigative Department responsible for prosecuting cyber-theft of trade secrets.

Group brainstorming

In the afternoon session of the event, participants were divided in three groups, each assigned three main recommendation topics to discuss, namely: i) prevention: awareness

[157] FIN 48 attempts to provide guidance on accounting for uncertainty in tax positions.

and standards/guidelines; ii) cooperation & enforcement; iii) data collection and reporting system. Below, each recommendation topic is presented in an aggregated manner in order to highlight what were the main feedbacks received by the Commission and the study team.

Summary of outcomes from Prevention: awareness and standards/guidelines

Best practices for awareness raising in specific industry, Member State, environment

There are several best practices on cybersecurity topics and for/in different sectors (an example came from the shipping industry). However too many best practices could prove not useful as they may generate confusion and would not be effective.

Incentives to stimulate awareness within SMEs in particular

Regarding the possibility for the EU to be involved in strengthening management-level awareness, all groups confirmed that this needs to increase, especially for SMEs. It is important to keep in mind that SMEs need easy, clear and specific messages on cybersecurity. They do not have the experience on this topic as large companies do. They often do not have an internal IT Department but external advisors only.

A good strategy could be at first to raise awareness on what trade secret is and make SME aware of the importance of the information they own. Then it would be useful to work on an easy and simple wording to disseminate basic rules on cybersecurity measures to protect information and supply chain IP and trade secrets.

Some of the participants, in order to disseminate good practices and raise awareness, suggested to deploy existing platform or business support communities as the European IPR Helpdesk (that offers free-of-charge, first-line support on IP matters to beneficiaries of EU-funded research projects and EU SMEs involved in transnational partnership agreements), the Enterprise Europe Network (that provides support for Small and Medium-sized Enterprises and aims at helping and supporting business to innovate and grow internationally) and all business association dedicated to support specific industrial sectors. These communities could help businesses organising seminars or define user friendly guidelines to share concrete and simple rules to protect themselves from cyber theft of trade secrets.

All participants agreed on the need to raise awareness on cyber theft of trade secrets among policy makers and key staff in Member States. The main suggestion was to use large companies, with the coordination of the EC, to push governments and national authorities to be more aware of the threat and support SMEs in investing in cybersecurity. It could also be effective to raise awareness among Top Management of large companies in order to work together with institutions and cooperate on specific topics. Generally speaking, all participants recognised the need to invest in trainings on the risks of cyber theft of trade secrets, and providing understandable by all stakeholders by means of "examples" and using the local languages.

"The Essentials on what You Need to Know and Do to Protect Your Know-how against Cyber Theft" A toolkit.

With regard to the identification of a useful set of measures to increase awareness and protect trade secrets, participants underlined the need to define level of confidential information and make easy rules at sectorial level. Language and wording are important and the proposed toolkit should be translated in all EU official languages. It could also be

useful to create knowledge centres to disseminate good practices to protect trade secrets and prevent their theft through cyber intrusions.

The most suited partners that could reach SMEs and disseminate the toolkit would be industry associations and SMEs associations. The toolkit could be composed of module with different level of complexity and should be tailored to different sectors.

Standards and guidance to fight against cyber theft of economic information

All groups involved agreed on the fact that there are many standards and guidelines on cybersecurity in general and new standards might easily create confusion and overlapping of messages. Furthermore, some participants underlined that "trade secrets" has a broad meaning, especially in some sectors. Therefore, standardization might not be efficient in these cases, in particular due to the need of flexibility. The suggestion gathered from different stakeholders is to deploy existing cybersecurity standards and channels to address the risks on cyber theft of trade secrets, one of the example given was the so-called ISO/TC 292, that is a technical committee of the International Organization for Standardization formed in 2015 to develop standards in the area of security and resilience, this could be one of the channel to efficiently address the topic of cyber theft of trade secrets.

Other suggestions on raising awareness

During the group brainstorming came up other suggestions to make companies more aware of the risks related to cyber theft of trade secrets:

- Companies should become aware that they have trade secrets which are protected by law;
- Companies should become aware of the value of their secrets and that their use by an unauthorized person means theft;
- Companies should be advised to look at a broader strategy for protecting their secrets of which cyber security is a small part.

Summary of outcomes from Data collection and reporting system

The goal of the session was to investigate stakeholders' perception and explore ideas on possible reporting system.

Reasons for adopting (or not) a reporting system

Benefits for the reporter and the *reportee* are very different. In fact participants all understood and shared the purpose for policy maker of having a critical mass of data in order to craft policies and have a better understanding of the problem.

However, from the business point of view, having to report information was perceived as a hurdle. Reporting obligations require employment of resources and added costs. In order to adhere to a reporting system companies need to clearly see a tangible benefit and a return of investment. For example, when reporting criminal activities to public authorities, people expect a follow up. In the absence of incentives, no cooperation can be expected from citizens and companies. Companies report if they can have some degree of trust that their effort contributes to law enforcement.

Additionally, special concerns were raised for SMEs. As previously stated, reporting obligations require employment of resources and added costs so, for SMEs such kind of effort could be totally unsustainable. Moreover, SME do not have the appropriate skills and capabilities to face the problem. Actually, companies are unsure of the authority they have to report an intrusion at. For example, there are government platforms to report cyber intrusions but there are also CERTs.

Considering that SMEs are more exposed to cyber intrusion than large companies, by introducing a mandatory reporting scheme, adequate assistance should be provided to SMEs.

Therefore, in order to participate in a reporting system, companies would have to be ensured that the reporting would trigger an action or response from authorities. The mere contribution to the development of general knowledge and statistics would not be sufficient, even if this would support for better policy response. Businesses would need a more immediate return, such as concrete help in dealing with incident and its impact; or follow-up enforcement actions, or, as a minimum, receive technical information on how to protect their company against a cyber intrusions, new malware campaigns and possible patches for vulnerabilities.

Some stakeholders mentioned that there are already sufficient peer alert systems in place, and if victims want follow up actions they should report to enforcement authorities. Setting up another reporting system on top of others, would not bring real added value.

One participant suggested that if the EC needs more insights on the topic it could use different data collection methods which are also reliable such as surveys.

What should be reported

A key issue lays in understanding what exactly the object of the reporting is. It is rarely the case where companies can be certain that the target of the attack was to steal intellectual property, it is generally an assumption based on traces left by the hacking. Also not being able to easily attribute the incident to a particular entity makes it difficult to report.

The problem is even more true for SME. Awareness cannot be raised within SMEs by a reporting system – if they are not aware, they are really unsure on what they should report.

Report should be precise and specific and should have a definition on what is cyber theft, clearly documented and report behind it should be specific. A stakeholder suggested that ENISA could amend guidelines. They have a list of what needs to be reported but it is not explicit about trade secrets.

To whom should the information be reported?

It was generally stated that, if it was to exist, a reporting system should not be directed to the European Commission. Alerting peers is about time and speed – so putting this in an EU wide report is unlikely to trigger fast reports.

Participants explained that law enforcement agencies are the right body to report to. The most reliable reporting systems would be criminal justice systems in general, but these channels are not well equipped.

Trusted reporting channels within a sector received more support by stakeholders. In fact in specific business fields there is the need to share knowledge. In Germany, there is an automotive reporting system with a state entity, the incentive is sharing among peers – if you notify anonymously, the entity will put you in contact with whom can help.

Summary of outcomes from Enforcement and Cooperation

Enforcement

It is very difficult to identify the "hacker" of a trade secret stolen by cyber means and it is very difficult to prove that the "user" of the trade secret acquired it illegally. Therefore, there is little application of the Trade Secrets Directive in cases of theft of such secrets through cyber.

With regard to criminal liability, participant felt that a lot has already been done with the e-evidence, Budapest convention on cybercrime and others. There was no call for further action.

Prevention is thus crucial but participants felt that the burden is placed on business, while the diplomatic solutions were underused.

Process: The internal company processes to protect the trade secrets could be built around the legal obligations stemming from the NIS Directive, the Directive on the Security of Networks and the GDPR.

Political and technical support:

- Support industry in collaborating for the development of affordable and scalable service for SMEs (subject to competition rules), as the main obstacle is the cost for the SMEs
- Provide guidance with regard to which standard helps an SME to comply with which obligation.

Cooperation

A number of presentations pointed out that the "hackers" who acquire valuable information are usually well funded or supported. Logically, action would be required against those that fund and support such activities.

In terms of government supported cyber espionage, policy makers were invited to take a more offensive approach:

- Unilateral action – imposing economic sanctions (justification could be security threat);
- Bilateral action – including respective provisions in regional trade agreements similar to those in the new US-MEX-Canada agreement. (DG Trade noted that our bilateral agreements deal with trade secrets, refinement might be necessary to take into account the cyber aspect.)
- Multilateral action – code of conduct for governments to abstain from cyber theft or funding such theft.
- Discussion with MS/EU on vulnerability equity process and source, encryption (some clarifications are needed)

If information from businesses is required in order to pursue diplomatic or other international trade-related channels, the best option would be to adopt legislations to oblige companies to provide such information. In that case, companies can refer to the legislation and seek to avoid retaliation in markets outside the EU.

ANNEX F: THE DIRECTIVE ON SECURITY OF NETWORK AND INFORMATION SYSTEMS (NIS DIRECTIVE)

The Directive on Network and Information Systems (NIS Directive) aims at achieving a high common level of network and information systems security across the EU[158]. It applies to Operators of Essential Services (OESs) that are established in the EU, and Digital Service Providers (DSPs) that offer services to persons within the EU. More in detail, the sectors affected by the NIS Directive are:

- Energy;
- Transport;
- Health;
- Water;
- Digital infrastructure;

The Directive requires these clusters to take appropriate technical and organisational measures to secure their networks and information systems in relation to the latest development and potential risks, and to notify the relevant competent authority of any security incident having a significant impact on service continuity without undue delay;[159]

Like the General Data Protection Regulation (GDPR),[160] organisations must "without undue delay and, where feasible, no later than 72 hours after having become aware of an incident" report incidents to the Competent Authority.

The incident reporting structure has been broken down into two sections:

- Incident response – acts as a support function where National competent authorities should be approached for cyber-related incidents;
- Incident notification – acts as a regulatory process wherein incidents must be reported to the competent authority and they will then decide if a follow-up investigation is required.

Other main objectives of the NIS Directive are:[161]

- Managing security risks: Appropriate organisational structures, policies, and processes put in place to understand, assess and systematically manage security risks to the network and information systems supporting essential services;
- Protection against cyberattacks: Proportionate security measures put in place to protect essential services and systems from cyberattacks;
- Detecting cyber security events: Capabilities to ensure that security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential services;
- Minimising the impact of cyber security incidents: Capabilities to minimise the impact of a cyber-security incident on the delivery of essential services including the restoration of those services where necessary.

Moreover, the Directive requires EU Member States to establish a National Computer Security Incident Response Team (CSIRT or CERT) responsible for receiving, reviewing, and responding to cyber security incident reports and activity. The Directive recognises the need for an incident reporting method but, on one side, some EU Member States are yet

[158] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
[159] https://www.itgovernance.eu/nis-directive
[160] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=IT
[161] https://www.ncsc.gov.uk/guidance/nis-directive-top-level-objectives

to adopt legislation on security measures and, on the other side, among the ones who have adopted legislation, there are big differences among national approaches. In order to contribute to the development of confidence and trust between the Member States and to promote swift and effective operational cooperation, a network of the national CERTs is hereby established. The CERTs network shall be composed of representatives of the Member States' CERTs and CERT-EU.

ANNEX G: THE EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA)

The European Union Agency for Network and Information Security (**ENISA**) is the **centre of expertise for cyber security in Europe** working closely together with Member States and the private sector to deliver advice and solutions[162].

Its main tasks relate to:

- The support of the **development of a Union policy law** by assisting (providing preparatory work and analysing the one already available) and advising on all matters relating to the NIS Directive;
- The facilitation of capacity building by assisting the Union institutions, bodies, offices and agencies in the **prevention, detection and analysis** of the capability to respond to network and information security problems and incidents;
- The support for the establishment of a national/governmental Computer Emergency Response Team (CERT or CSIRT) in all EU Member States and the **assistance of these teams' efforts to reach a baseline level of capabilities** as they mature. In 2013 ENISA introduced its **training courses** for CERTs in the EU Member States in order to promote and support CERT maturity in the MS by having **exercises and technical hands-on training on different services**, and **operations and cooperation in daily work of the teams**.[163] Moreover, ENISA provides the secretariat of the CERTs Network[164] and actively supports the cooperation among the CERTs. The Agency organises meetings of the CERTs Network, and provokes discussion by proposing discussion topics;
- The **cooperation with Union institutions, bodies, offices** and **agencies**, including those dealing with cybercrime and the protection of privacy and personal data, with a view to **addressing issues of common concern**.[165]

Union institutions, bodies, offices, agencies and Member State bodies may request advice from the Agency in the event of breach of security or loss of integrity with a significant impact on the operation of networks and services.[166]

The **2016-2020 ENISA Strategy** underlines that, by 2020, ENISA will act as **focal point for EU Institutions, CERTs and national authorities** collating, analysing and making available information on global cyber issues with a view to developing insights on issues of high added-value for the EU".[167]

Taking this into consideration, as part of the "Cybersecurity Package", the EC tabled in September 2017 a proposal on a "**Regulation of the European Parliament and of the Council on the future of ENISA**"[168] reinforces the role of ENISA and enables the Agency to better support Member States. The European Parliament, through three of its Committees (LIBE, BUDG and IMCO) has provided between March and May 2018 a set of amendments to be considered by the EC.[169] The proposal has been positively evaluated by the **Transport, Telecommunications and Energy Council** (European Council) during the meeting of 8th June 2018 and is due to be voted by the European Parliament during the plenary sitting of September 2018.[170]

---

[162] https://www.enisa.europa.eu/about-enisa
[163] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/baseline-capabilities
[164] https://www.enisa.europa.eu/topics/csirts-in-europe/capacity-building
[165] Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004; pp. 43-44
[166] Regulation (EU) No 526/2013; pp. 49
[167] ENISA (2016). ENISA Strategy 2016-2020. Available at: https://www.enisa.europa.eu/publications/corporate/enisa-strategy
[168] ENISA (2017). European Commission proposal on a Regulation of the European Parliament and of the Council on the future of ENISA. Available at: https://www.enisa.europa.eu/news/enisa-news/european-commission-proposal-on-a-regulation-on-the-future-of-enisa
[169] http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2017/0225(OLP)#tab-0
[170] http://www.consilium.europa.eu/en/meetings/tte/2018/06/08/

ANNEX H: THE US STRATEGY IN PREVENTING AND MITIGATING CYBER THEFT OF TRADE SECRETS

Looking at the biggest world economy, the US Government engagement in fighting against cyber threats has its more recent roots in the globalized world and the opening to cyber espionage. The **Commission on the Theft of American Intellectual Property** estimated back in 2013 that the costs of trade secret thefts equate to 1% - 3% of US GDP[171] per year. Following this, the Obama's administration, concentrated on methods and best practices to protect trade secrets, both at national and international level.

The same year, the United States, and in particular the National Institute for Standards and Technology **(NIST)** started developing a **policy Framework** consisting in **standards, guidelines, and best practices to manage cybersecurity-related risk** including cyber theft of trade secrets. "The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security."[172] The main intent of the NIST Framework is to provide a common language for companies to raise their maturity level of cybersecurity, but also to raise cyber resilience.

The Framework has been developed and promoted through ongoing engagement with, and input from, stakeholders in government, industry, and academia. The NIST framework is a flexible tool that overall encompasses all measures identified, grouped in its **five "Functions": Identify; Protect; Detect; Respond; Recover.**

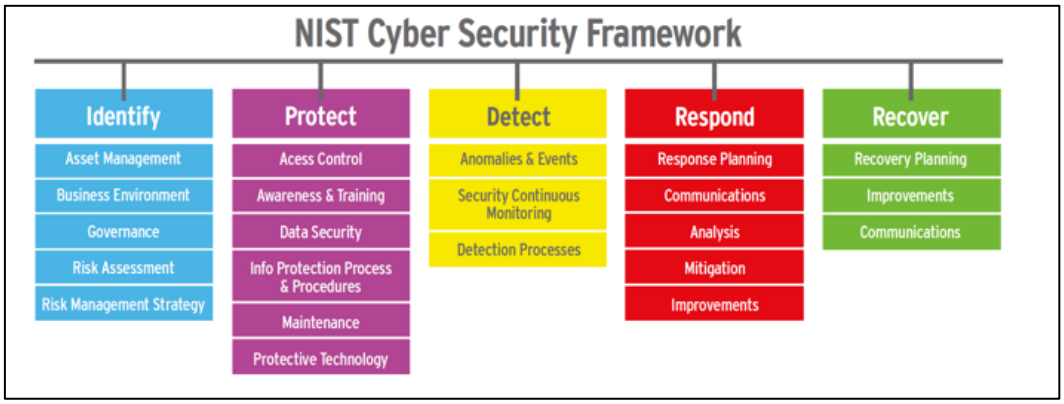


Figure 4 - NIST Cyber Security Framework

Results from research conducted by Dimensional Research of more than 300 IT and security professionals in the US,[173] indicates that 29% of organisations leverage the NIST Cybersecurity Framework (CSF) and overall security confidence is higher for those using this framework. Additionally, more than 70% of respondents who have adopted or plan to adopt the NIST CSF view it as an industry best practice. The framework is made up of five key milestones of its development and continued advancement. The latest updated is of April 2018.

A first development undertaken by the Obama's administration was the **signing in 2015 of the bilateral economic cyber espionage agreement with the Chinese counterpart**, Xi Jinping. It is unclear how efficient the international agreement is, as Chinese espionage activity has recently ramped right back up to pre-2016 levels. This is supposedly incited by to the high interest for Western intellectual property and R&D and the need of the Chinese Government to enact a precise economic strategy aiming at

[171] PwC. (2014). Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential threats. Available at:https://create.org/wp-content/uploads/2014/07/CREATe.org-PwC-Trade-Secret-Theft-FINAL-Feb-2014_01.pdf
[172] https://www.nist.gov/cyberframework
[173] https://www.tenable.com/blog/nist-cybersecurity-framework-adoption-on-the-rise

supporting ICT national firms, such ZTE and Huawei, through financial and regulatory support over the past three decades.[174]

The same year, the FBI launched a campaign to sensitise businesses and organisations on the risks of economic espionage and cyber theft of trade secrets, and developed a **checklist for reporting on Economic Espionage and Cyber theft of Trade secrets**.[175] The checklist provides some means to establish the economic value of the secret stolen and requires the trade secret owner to describe the security measures, both technical and legal, taken to secure the knowhow.

In 2016, the **"Defend Trade Secrets Act"**[176], which originates from two previous legislations, the Uniform Trade Secrets Act of 1985[177] and the Economic Espionage Act of 1996,[178] created a private civil action against misappropriation of trade secret, being the civil seizure the most distinct feature.[179]

In 2017, the Commission on the Theft of American Intellectual Property issued an **update of the 2013 report**, estimating that the cost of cyber theft of trade secrets to the US economy was between $180 billion and £540 billion in 2015. It states: "Of all the forms of IP theft, **trade secret theft**—in an increasing number of cases enabled by cyber espionage—**might do the greatest damage to the U.S. economy**."[180]

More recently and as a consequence of the increase in cyber espionage from third parties, the "United States Director of National Intelligence (DNI), Dan Coats, identified Russia, China, Iran, and North Korea as key global cyber-threats, consistent with DNI reporting since at least 2012."[181] As underlined by the DNI, "Government sponsored cyber espionage continues unabated across all four of these countries, serving each country's national development and strategic priorities; but, in a trend toward hybridisation, state-sponsored actors increasingly rely on tools and techniques normally used by financially motivated cyber criminals, complicating both attack attribution and assessments of motive for launching attacks."[182]

On one hand, the US Admiration intensified its attention on China and in March 2018, the President issued a "**Memorandum on the Actions by the United States Related to the Section 301 Investigation**" pointing out how "China conducts and supports unauthorized intrusions into, and theft from, the computer networks of U.S. companies. These actions provide the Chinese government with **unauthorized access to intellectual property, trade secrets, or confidential business information**, including technical data, negotiating positions, and sensitive and proprietary internal business communications policies."[183] On the other hand, the Trump Administration officially presented in May 2018 its **new strategy for cybersecurity and cyberattacks deterrence**, mentioning as main global threats Russia and North Korea. The strategy

[174] US Gov - U.S.-China Economic and Security Review Commission.
[175] FBI (2015). Checklist for Reporting Economic Espionage and Cyber-Theft of Trade Secrets. Available at: https://www.fbi.gov/file-repository/checklist-report-economic-espionage.pdf/view
[176] Congress of the United States. (2016). The Defend Trade Secrets Act. Available at: https://www.gpo.gov/fdsys/pkg/PLAW-114publ153/html/PLAW-114publ153.htm
[177] http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf
[178] https://www.justice.gov/usam/usam-9-59000-economic-espionage
[179] Tilburg University (2016). TRADE SECRET PROTECTION IN THE U.S. AND EU. Available at: http://arno.uvt.nl/show.cgi?fid=141634
[180] The Commission on the Theft of American Intellectual Property (2017). The theft of American intellectual property: reassessments of the challenge and United States policy. Available at: http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf
[181] Accenture security (2017). Cyber-Threatscape report. Available at: https://www.accenture.com/t20171010T121722Z__w__/us-en/_acnmedia/PDF-63/Accenture-Cyber-Threatscape-Report.pdf
[182] Ibidem
[183] The White House (2018). Memorandum on the Actions by the United States Related to the Section 301 Investigation. Available at: https://www.whitehouse.gov/presidential-actions/presidential-memorandum-actions-united-states-related-section-301-investigation/

results from two principal documents: a report containing the **deterrence agenda**[184] and an additional document[185], explaining the **Administration's international engagement strategy**, in relation to cyber theft of trade secrets and cyber espionage.

The deterrence agenda provides for a four-part plan: writing a policy for what types of cyber activities the US will try to prevent; crafting a "menu of options" for deterring and responding to those activities; convening interagency discussions to evaluate specific responses; and strengthening international partnerships with the goal of doing joint deterrence operations.

Finally, the report points out the following four points as pivotal for the Trump's cyber-deterrence strategy implantation:

- Creating a policy for when the United States will impose consequences: The policy should provide criteria for the types of malicious cyber activities that the US government will seek to deter. The outlines of this policy must be communicated both publicly and privately, in order for it to have a deterrent effect.
- Developing a range of consequences: The US should prepare a menu of options for swift, costly, and transparent consequences below the threshold of the use of force that it can impose, consistent with US obligations and commitments, following an incident that merits a strong response that can have downstream deterrent effects. As the United States develops these options, it should assess and seek to minimize the potential risks and costs associated with each of them.
- Conducting policy planning for imposing these consequences: In addition to developing consequences themselves, the United States should conduct interagency policy planning for the time periods leading up to, during, and after the imposition of consequences. Such planning, which should include the development of appropriate interagency response procedures, will help ensure consistent responses to different incidents and assist in managing the risk of escalation.
- Building partnerships: The imposition of consequences would be more impactful and send a stronger deterrent message if it were carried out in concert with partners. Partner states could, on a voluntary basis, support each other's responses to significant malicious cyber incidents, including through intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken following an incident, and/or actual participation in the imposition of consequences against perpetrator governments.

[184] "Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats", available at: https://www.politico.eu/wp-content/uploads/2018/06/282253.pdf?utm_source=POLITICO.EU&utm_campaign=eb7ab01634-EMAIL_CAMPAIGN_2018_06_01_07_25&utm_medium=email&utm_term=0_10959edeb5-eb7ab01634-189157965

[185] "Recommendations to the President on Protecting American Cyber Interests through International Engagement", available at: https://www.politico.eu/wp-content/uploads/2018/06/282224.pdf?utm_source=POLITICO.EU&utm_campaign=eb7ab01634-EMAIL_CAMPAIGN_2018_06_01_07_25&utm_medium=email&utm_term=0_10959edeb5-eb7ab01634-189157965

ANNEX I: COMPREHENSIVE BIBLIOGRAPHY

1. Accenture. (2015). Making your Enterprise Cyber Resilient.
2. Accenture. (2017). Cost of Cyber Crime Study.
3. Accenture. (2017). Cyber Threatscape Report.
4. AIVD and MIVD. (2017). Cyberespionage: are you aware of the risks?
5. AIVD. 2016. Annual report 2016.
6. AIVD. Analysis of vulnerability to espionage - Espionage risks and national safety and security.
7. Alex Cox. (2012). The Cyber Espionage Blueprint: Understanding Commonalities In Targeted Malware Campaigns. RSA FirstWatch.
8. Anderson, R. Barton, C. Bohme, R. Clayton, R. Eeten (van), M. J.G. Levi, M. Moore, T. Savage, S. (2012). Measuring the Cost of Cybercrime. University of Cambridge.
9. ANSSI (2017). The Ambition of European Union Member States on the 'Cybersecurity Cyber-package'.
10. B7 Business Summit. (2018). 2018 B7 Declaration.
11. Baker McKenzie. (2017). The rising importance of safeguarding trade secrets.
12. Barrachina, A., Tauman, Y., Urbano, A. (2013). Entry and espionage with noisy signals. Universitat de Valencia.
13. Baseline Capabilities of National/Governmental CERTs
14. Basic. (2017). Hacking Uk Trident: A Growing Threat.
15. Becrypt. (2014). Protecting your business from IP theft.
16. Benham, R. (2017). Cyber Security: Ensuring business is ready for 21st Century. Institute of Directors.
17. Bhatti,H. J., Alymenko, A. (2017). A Literature Review: Industrial Espionage. Halmstad University.
18. Bitdefender. (2015). Companies blame competition for corporate cyberespionage.
19. Bitdefender. (2017). Companies blame competition for corporate cyberespionage.
20. Bitkom (2017). Wirtschaftsschutz in der digitalen Welt.
21. Booz Allen Hamilton. (2017). Foresight Cyberthreat Analysis for 2017.
22. Brooking institution - Cyber Theft of Competitive Data: Asking the Right Questions.
23. BSA (2015). BSA feedback on European Commission 'inception impact assessment' on the 'Proposal for a Regulation revising the ENISA Regulation (No 526/2013) and laying down a European ICT security certification and labelling framework'.
24. Bundesamt für Verfassungsschutz. (2016). Report on the Protection of the Constitution.
25. Business Europe (2017). The proposal for a Cybersecurity Act - a BusinessEurope position paper.
26. Canada National Security and Intelligence. (2017). Joint Communiqué - 2nd Canada-China High-Level National Security and Rule of Law Dialogue.
27. CCDCOE (2015). Economic Aspects of National Cybersecurity Strategies.
28. Center for Responsible enterprise and trade. (2016). The importance of Cybersecurity for Trade Secret Protection.
29. Center for Strategic and International Studies (CSIS) and McAfee. (2013). The economic impact of cybercrime and cyber espionage.
30. Center for Strategic and International Studies (CSIS) and McAfee. (2014). Net Losses. Estimating the Global Cost of Cybercrime.

31. Center for Strategic and International Studies (CSIS) and McAfee. (2018). Economic Impact of Cybercrime – No Slowing Down.
32. Center for Strategic and International Studies (CSIS). (2017). Cyber Policy Task Force Working Group Discussion Papers.
33. Centro Nacional de Inteligencia. (2017). Cyber-Threats and Tendencies 2017 edition.
34. CERT Polska (2016), "The security landscape of the Polish Internet",
35. Cisco (2017). "017 Annual Cybersecurity Report.
36. Clusit. (2017). Rapporto Clusit 2017 sulla sicurezza ICT in Italia.
37. Congress of the United States. (2016). The Defend Trade Secrets Act.
38. Council on Foreign Relations. Cyber Operations Tracker.
39. Cox, A. (2012). The Cyber Espionage Blueprint: Understanding Commonalities In Targeted Malware Campaigns. RSA FirstWatch.
40. CREATE. Org. (2018). Protecting trade secrets from cyber and other threats.
41. Crook, J. R. (2013).U.S. Efforts to Enhance Cybersecurity and to Counter International Theft of Trade Secrets. The American journal of international law.
42. Crosby, M. Supply. (2014). The SME Cyber Market: How your business can benefit.
43. CSO. (2017). Germany warns of nation-state cyber espionage threat.
44. Danish Centre for Cyber Security – The cyber threat against Denmark 2017
45. Danks,D., Danks J.H. (2015). Beyond Machines: Humans in Cyber Operations, Espionage, and Conflict. Carnegie Mellon University.
46. De Schepper, K., Vandebroek, E. and Verbruggen, F. Centre for Global Governance Studies. Leuven. (2016). Countering economic espionage and industrial spying: a Belgian criminal law perspective.
47. Deloitte (2016). The hidden costs of an IP breach: Cyber theft and the loss of intellectual property.
48. Deloitte. (2016). Beneath the surface of a cyberattack. A deeper look at business impacts.
49. Deloitte. (2016). Global Defense Outlook 2016.
50. Deloitte. (2017). Industry 4.0 and cybersecurity.
51. Department for Business, Innovation and Skills (2013). 2013 Information Security Breaches Survey.
52. Department of Defence, THE DEPARTMENT OF DEFENSE CYBER STRATEGY 11–12 (2015).
53. Department of Homeland Security. (2016). Cyber Incident Reporting. A Unified Message for Reporting to the Federal Government.
54. Diplomacy Data. (2015). Cyber Security and Cyber Espionage in International Relations.
55. Directive (EU) 2016/1148 of the European Parliament and if the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
56. Dutch Ministry of Security and Justice, National Coordination for Security and Counterterrorism – Cyber Security Assessment 2017
57. ECIPE. (2018). Stealing thunder, Cloud, IoT and 5G paradigm for protecting European commercial interests. Will Cyber espionage be allowed to hold Europe Back in the global race for industrial competitiveness?
58. ENISA (2012), Baseline Capabilities of n/g CERTs - Updated Recommendations 2012
59. ENISA (2016). ENISA Strategy 2016-2020.

60. ENISA (2017). European Commission proposal on a Regulation of the European Parliament and of the Council on the future of ENISA.
61. ENISA, Incident Reporting, https://www.enisa.europa.eu/topics/incident-reporting
62. ENISA. (2009). Baseline capabilities for national / governmental CERTs
63. ENISA. (2014). Technical Guideline on Incident Reporting.
64. ENISA. (2016). Cyber Europe 2016: After Action Report.
65. ENISA. (2017). Incident notification for DSPs in the context of the NIS Directive.
66. ENISA. (2017). Threat Landscape Report 2017 - Final Version 1.
67. ENISA. CERT Cooperation and its further facilitation by relevant stakeholders.
68. ESET. (2018). Tendencias En Ciberseguridad 2018: el Costo De Nuestro Mundo Conectado.
69. EUISS. (2015). The threat of state-sponsored industrial espionage.
70. European Commission (2016). Brussels, 5.7.2016. Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry. Available at:
71. European Commission (2016). Communication 2016/410 "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry".
72. European Commission, (2013). Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Cybersecurity Strategy of the European Union: An open, Safe and Secure Cyberspace;
73. European Commission, Brussels, 5.7.2016 COM(2016) 410 final.
74. European Commission. (2013). Impact Assessment on a proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against misappropriation.
75. European Commission. (2013). Study on Trade Secrets and Confidential Business Information in the Internal Market.
76. European Commission. (2016). Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union
77. European Commission. (2016). Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.
78. European Commission. (2017). Building an Effective European Cyber Shield.
79. European Council - Council of the European Union. (2017). Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU
80. European Council. (2017). 9621/17 Information from the commission.
81. European Parliament and the Council. (2013). Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing regulation (EU) 526/2013, and on Information and Communication Technology and Cyber Security Certification ("Cybersecurity Act").
82. European Parliamentary Research Service. (2017). Cybersecurity in the EU Common Security and Defence Policy (CSDP).

83. European Parliamentary Research Service. (2017). European Parliament Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level.
84. European Political Strategy Centre (EPSC). (2017). Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level.
85. EUROPOL (2017). European Internet Organised Crime Threat Assessment (IOCTA) (2017). Internet organised crime assessment.
86. Europol. (2016). IOCTA 2016 Internet Organised Crime Threat Assessment.
87. EY. (2018). Cybersecurity regained: preparing to face cyber-attacks.
88. Farley, R.(2016). Intellectual Property, Cyber Espionage, and Military Diffusion. Global Security and Intelligence Studies.
89. FBI (2015). Checklist for Reporting Economic Espionage and Cyber-Theft of Trade Secrets.
90. FBI. (2015). Counterintelligence strategic partnership intelligence note (spin).
91. FBI. (2017). Checklist for Reporting an Economic Espionage or Theft of Trade Secrets Offense.
92. FE - Center for Cyber Security (2017). Threat Assessment.
93. FE - Centre for Cyber Security. (2016). The cyber threat against Denmark.
94. Finnish Security Service Intelligence. (2017). SUPO 2017.
95. FireEye. (2018). APT37 (REAPER)
96. FireEye/Marsh & McLennan Companies, Inc. (2017). Cyber Threat: a perfect storm about to hit Europe.
97. Fortinet. (2017). Threat Landscape Report.
98. French Government. (2015). French National digital Security Strategy.
99. Friedman, A.A. (2013). Cyber Theft of Competitive Data: Asking the Right Questions. Brooking Institutions.
100. Friedman, A.A., Mack-Crane, A., Hammond, R.A. (2013). Cyber-enabled Competitive Data Theft: A Framework for Modelling Long-Run Cybersecurity Consequences. Brooking Institutions.
101. Frost & Sullivan. (2017). 2017 Global Information Security Workforce Study
102. FSB. (2017). Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices.
103. G20 Turkey. (2015). G20 Leaders' Communiqué Antalya Summit, 15-16 November 2015.
104. G7. (2017). ICT and Industry Ministers' Declaration.
105. Glitz, A. Meyersson. E. (2017). Industrial Espionage and Productivity. IZA Institute of Labor Economics.
106. Grayling Public Affairs. (2017). Navigating cyber threats to business competitiveness.
107. Handelsblatt. (2018). Aufstieg mit Spionage?
108. Hewlett Packard Enterprise. (2016). HPE Security Research Cyber Risk Report 2016.
109. IBM. (2016). Survey of Cybersecurity Landscape.
110. Insikt Group. (2017). Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3.
111. Institute for National Security and Counterterrorism. (2015).Countering State-Sponsored Cyber Economic Espionage Under International Law.
112. Institute of Directors, Cyber Security: Ensuring business is ready for 21st century, 2017,
113. Intellectual property. (2017).Best and Worst Countries for Intellectual Property Protection.

114. International Telecommunication Union. (2017). Global Cybersecurity Index (GCI) 2017.
115. IZA – Glitz, A., Meyersson, E. (2017) Industrial Espionage and Productivity DP No. 108 2017
116. Journal of Cybersecurity (2016). Examining the costs and causes of cyber incidents.
117. Kaspersky. (2013). Who's spying on you? No business is safe from cyber espionage.
118. Kaspersky. (2016). Kaspersky DDoS Intelligence Report Q2 2015.
119. King, K. (2017). The Value of Intellectual Property, Intangible Assets and Goodwill. WIPO.
120. KPMG. (2017). Cyber Crime Survey Report.
121. Kroll (2017), Global Fraud & Risk Report,
122. Letizia Paoli, Jonas Visschers, Cedric Verstraete & Elke van Hellemont. (2018). The Impact of Cybercrime on Belgian Businesses.
123. L. Gordon, M. Loeb, (2002). The Economics of Information Security Investment.
124. London Stock Exchange Group. (2017). London Stock Exchange Group's response to the European Commission's proposal for a regulation on ENISA and on ICT cybersecurity certification.
125. MalwareBytes. (2017). Cybercrime tactics and techniques.
126. Mandiant / FireEye. M-TRENDS 2017 (2017),
127. Mannheimer swartling – National Intelligence Law. (2017). General Introduction of the Draft National Intelligence Law.
128. Marsh & McLennan. (2018). MMC Cyber Handbook 2018.
129. Massimo Pellegrino. (2015). The threat of state-sponsored industrial espionage. EUISS.
130. McAfee, CSIS. (2018). Economic Impact of Cybercrime— No Slowing Down.
131. Microsoft (2017). Microsoft Response to the European Commission's Proposal for a Regulation on ENISA and ICT Cybersecurity Certification Framework.
132. Morgan Stanley. (2016). Cybersecurity: Time for a Paradigm Shift.
133. N. van der Meulen, (2015), Investing in Cybersecurity, RAND Europe,
134. National Cryptology Centre - Cyber threat and tendencies, 2017 Edition
135. National Cyber Security Centre. (2016). Cyber Security Assessment Netherlands csan2016.
136. National Cyber Security Centre. (2017). Cyber Security Assessment Netherlands 2017.
137. National Defence Radio Establishment. (2016). Årsrapport 2016: Oförutsägbar omvärld (FRA 2016 Annual Report)
138. NCSC. (2017). Cyber Security: Small Business Guide.
139. New Swedish Act on the Protection of Trade Secrets (2018), Revision of the Swedish Act on the Protection of Trade Secrets (1990).
140. NHS Digital. (2015). Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation.
141. NIST. (2017). Cybersecurity Framework.

142. Office of the United States Trade Representative. (2018). Findings of the investigation into china's acts, policies, and practices related to technology transfer, intellectual property, and innovation under section 301 of the trade act of 1974.
143. Pellegrino, M. (2015). The threat of state-sponsored industrial espionage. EUISS
144. Presidenza del Consiglio dei Ministri. (2016). Sistema di Informazioni per la Sicurezza della Repubblica. (2017). Relazione sulla politica dell'informazione per la sicurezza.
145. Presidenza del Consiglio dei Ministri. (2017). Piano Nazionale per la Sicurezza Cibernetica e la Sicurezza Informatica.
146. Prime Minister of Australia. (2017). Australia And China Agree To Cooperate On Cyber Security.
147. PWC (March 2012), Beyond cyber threats: Europe's First Information Risk Maturity Index, A PWC report in conjunction with Iron Mountain, March 2012
148. PwC and Create.org (2014). Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential threats.
149. Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats".
150. Recommendations to the President on Protecting American Cyber Interests through International Engagement".
151. Red Line Drawn. (2016). Red Line Drawn: China recalculates Its use of cyber espionage.
152. Regulation (EC) No 544/2009 of the European Parliament and of the Council of 18 June 2009 amending Regulation (EC) No 717/2007 on roaming on public mobile telephone networks within the Community and Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services.
153. Republic of Estonia, Information System Authority. Annual Cyber Security Assessment 2017.
154. Research Center of Cyber Intelligence and Information Security, Laboratorio Nazionale CINI di Cyber Security. (2016). 2015 Italian Cyber Security Report.
155. Reynold, S. (2016). How to Protect Your Company's Trade Secrets in the Industrial IoT. IceMiller.
156. Rose Sarah, For all this tea. Hutchinson. 2009
157. S. Jahner, H. Krcmar (2005), Beyond Technical Aspects of Information Security: Risk Culture as a Success Factor for IT Risk, in: Association for Information Systems AIS Electronic Library, AMCIS 2005 Proceedings;
158. Saias, M. S. (2014). Unlawful acquisition of trade secrets by cyber theft: between the Proposed Directive on Trade Secrets and the Directive on Cyber Attacks. Journal of Intellectual Property Law & Practice.
159. Scott J. Shackelford, Eric L. Richards, Anjanette H. Raymond, Amanda N. Craig. (2015). Using BITs to Protect Bytes: Promoting Cyber Peace by Safeguarding Trade Secrets Through Bilateral Investment Treaties. American Business Law Journal.
160. SecureWorks. (2018). Bronze Butler Targets Japanese Enterprises.
161. Søilen, K. S. (2016) Economic and industrial espionage at the start of the 21st century – Status quaestionis. Journal of Intelligence Studies in Business.

162. Swedish Security and Defense Industry Association. (2018). State Sponsored Cyber Attack.
163. Symantec. (2017). ISTR – Internet Security Threat Report.
164. Telstra Corporation Limited. Telstra Cyber Security Report 2017.
165. The Commission on the Theft of American Intellectual Property (2017). The theft of American intellectual property: reassessments of the challenge and United States policy.
166. The Council of Economics Advisers (2018). The Cost of Malicious Cyber Activities to the US Economy.
167. The National Bureau of Asian Research. (2017). The theft of American intellectual property: reassessments of the challenge and United States policy.
168. The Sydney Morning Herald. (2017). George Brandis considers new laws cracking down on Chinese spying in Australia.
169. The United States - Department of Justice. (2017). U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage.
170. The Wall Street Journal. (2017). Hit by Chinese Hackers Seeking Industrial Secrets, German Manufacturers Play Defense.
171. The White House (2018). Memorandum on the Actions by the United States Related to the Section 301 Investigation.
172. The White House. (2015). FACT SHEET: President Xi Jinping's State Visit to the United States.
173. The White House. (2016). US Strategic Plan on Intellectual Property Enforcement FY2017-19.
174. Thorleuchter, D., Van den Poel, D. (2013). Protecting research and technology from espionage. Expert systems with applications. Universiteit Gent.
175. Tilburg University. (2016). Trade Secret Protection in the U.S. and EU. Available at:
176. Trend Micro. (2017), Challenges and Opportunities for 2017: Trend Micro Global.
177. U.S. Government. (2013). Supply Chain Risk Management - A Framework for Assessing Risk.
178. U.S. Government. (2018). U.S.-China Economic and Security Review Commission.
179. U.S. House of Representatives. (2012). Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE.
180. UK Government, Ipsos MORI, University of Portsmouth. (2016). Cyber Security Breaches Survey.
181. UK Government. (2015). UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk.
182. UNICRI. (2015). Guidelines for IT Security in SMEs.
183. Verizon (2016). 2016 Data Breach Investigation Report.
184. Verizon. (2012). Dbir Snapshot: Intellectual Property Theft.
185. Verizon. (2017). 2017 Data Breach Investigations Report.
186. Verizon. (2018). 2018 Data Breach Investigations Report.
187. Villasenor, J. (2015). Corporate Cybersecurity Realism: Managing Trade Secrets in a World Where Breaches Occur. Hoover Institution.
188. Wangen. G. (2015). The Role of Malware in Reported Cyber Espionage: A Review of the Impact and Mechanism.

189. Will Yakowicz (2015), "Companies Lose $400 Billion to Hackers Each Year," Inc., September 8, 2015.
190. William M Fitzpatrick, Samuel A Dilullo. Cyber Espionage and the S.P.I.E.S. Taxonomy. Competition Forum.
191. WIPO. Paris Convention for the Protection of Industrial Property 1979 (amended)
192. WirtschaftsWoche. (von Berke Jurge). (28 March 2018). Aufstieg mit Spionage?
193. World Economic Forum. (2018). The Global Risks Report 2018
194. World Trade Organisation. (1994). Agreement on Trade Related Aspects of Intellectual Property Rights.
195. WTO. (1994). Agreement on Trade-Related Aspects Of Intellectual Property Rights.
196. Zurich. (2016). Potential effect on business of small and medium enterprises (SMEs) due to cybercrime in 2016

Online sources:

- http://cert.europa.eu/
- http://www.consilium.europa.eu/en/meetings/tte/2018/06/08/
- http://www.jelfsmallbusiness.co.uk/business-network/blog/2015/08/2016/10/smes-struggling-to-protect-intellectual-property/
- http://www.leonardocompany.com/-/cyber-risks-intellectual-property
- http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf
- https://administracionelectronica.gob.es/ctt/ens#.W2mpktIzZPa
- https://www.eda.europa.eu/Aboutus/Missionandfunctions
- https://www.enisa.europa.eu/topics/csirts-in-europe/capacity-building
- https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map
- https://www.enisa.europa.eu/topics/incident-reporting
- https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
- https://www.europol.europa.eu/newsroom/news/four-eu-cybersecurity-organisations-enhance-cooperation
- https://www.justice.gov/usam/usam-9-59000-economic-espionage
- https://www.msb.se/en/Tools/News/Nordic-cyber-security-exercise-was-conducted-in-Linkoping/
- https://www.ncsc.gov.uk/guidance/introduction-cyber-assessment-framework
- https://www.nist.gov/cyberframework
- https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/
- https://www.tenable.com/blog/nist-cybersecurity-framework-adoption-on-the-rise

ET-01-18-013

Publications Office

doi: 10.2873/48055