Study on the Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber

Dissemination report on measures to tackle and prevent cyber-theft of trade secrets
Methodology

In order to develop an in-depth understanding of the current situation with regard to industrial espionage and cyber-theft of state secrets, a robust methodological framework for the analysis was required. **Methodological triangulation** is a data gathering process that involves more than one method to gather data; the different approaches complement each other, enabling confirmation and validation of findings, more comprehensive data and enhanced understanding. **Three different approaches** were adopted for the preparation of the final report: **Desk Research, Stakeholder Interviews** and an **Online Questionnaire**. The study team collected and examined all publicly available data on the topic with analysis of more than 150 sources of documents (e.g. reports, surveys, publications, conference papers, etc.). To obtain additional information that was not publicly available a total of **78 responses** were obtained through stakeholder consultation, namely from stakeholder **interviews** or responses obtained through the **online questionnaire**.
Introduction to the Study

Nowadays, digital connectivity and pervasive integration are introducing a wide array of security risks for all types and sizes of organisations. Cyber-theft of trade secrets represents a serious and growing threat to companies, particularly with respect to their investments in Research and Development (R&D) and economic sustainability.

This study aims at defining the scale and impact of cyber-theft of trade secrets on European businesses. Trade secrets are defined as valuable knowledge and information that companies treat as confidential, relying on it as a fundamental asset for their market competitive advantage. The study examines why business competitors and foreign countries are so interested in carrying out acts of cyber-espionage on European industrial companies, which own key know-how in strategic production sectors.

Today, perpetrators can steal trade secrets from any location globally, while often remaining anonymous and unidentified for long periods of time. The main issue in defining how companies are affected is that in many cases companies are unable to detect or report the incidents. In addition, 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 subject.

Through an extensive literature review and stakeholder consultation, the report has processed the most up to date data and information available, including cases affecting European businesses in recent years. Main findings highlight both public and private sectors concerns about the increasing risks associated with cyber-theft of trade secrets in Europe. Small and medium-sized enterprises (SMEs) deserve specific attention, given their greater vulnerability and lack of technical and investment capacities to counter cyber-threats, while representing the most widespread category of businesses in Europe.

Findings from the analysis support the formulation of four primary recommendations addressed to the European Union (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 and the subsequent serious impacts on European businesses. This requires a synergic and coordinated effort also at international level, given the cross-border dimension of the problem.
Current Risks and Growing Concern

A substantial number of cyber-intrusions target valuable knowledge and information, such as details about the business, know-how and technology that companies treat as confidential. Cyber-theft of trade secrets is among the main threats to the stability and economic growth of companies and organisations in the European Union. It is an issue that affects both the public and private sector on a regular basis, with serious economic and reputational impacts. Europe is widely attractive for emerging countries as its economy has an industrial and academic base specialised in automotive, biotech, infrastructure equipment and aerospace.

With respect to all data breaches it is possible to observe an upward trend in cyber-espionage between 2010 and 2016. This concern is expected to become even greater in the future. Verizon, according to its own data and analysis, report that in 2016, 25% of all cyber-espionage incidents resulted in the confirmed disclosure of data to an unauthorised party. All stakeholders interviewed confirmed the same trend: cyber-theft of trade secrets represents a real and growing threat to all types and sizes of companies and organisations that hold confidential information.

Relevant factors

Relevant factors that contribute to the existence and persistence of the threat include:

- Lack of awareness;
- Wider online exposure of companies;
- 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;
- Rise of cyberattacks by competitors, foreign government and hacktivist groups.

(In)Ability to Detect and Companies Lack of Awareness

European businesses and organisations endure more extensive consequences because of the time-lag between an intrusion and its detection registered in the continent; in Europe the time-lag is indeed three times longer than in the rest of the world, 469 days against an average of 146. Such a time discrepancy originates from a lack of funding allocated to cybersecurity measures and general unawareness, both at management and employees level, of the risks associated with the cyber-theft of trade secrets. The majority (65%) of stakeholders interviewed were of the view that still too many companies are still unaware of the risks they are incurring and that top management tend to look at cybersecurity expenditure as a cost rather than a desirable investment.

Who are the perpetrators?

The majority (61%) of CISO employees surveyed by Bitdefender were of the view that competitors would be the most likely party to target their organisation for corporate or industrial espionage. Just over half (56%) were of the view that Hacktivists would target them, followed by foreign state-sponsored attackers (48%). There has been an increasing trend in the latter (foreign state-sponsored attacks) in more recent years both in Europe and worldwide.
A Sectorial and Geographical Phenomenon

Distribution of Incidents Across Sectors
Cyber-theft of trade secrets affects all sectors - none are spared. The industrial sectors that appear to be most affected are manufacturing, information and communication technologies (ICT), finance and insurance and health and medical technology. The threat becomes particularly damaging if the targeted company is focused on R&D.

94%

In some sectors, such as manufacturing, industrial espionage and cyber-theft of trade secrets constitutes up to 94% of all cyber-attacks.

The geographical distribution of Incidents

Germany is the most affected country among EU Member States. 17% of companies report theft of sensitive data between 2015 and 2017. This trend is driven by the reluctance of German SMEs to invest in cybersecurity because of excessive costs.

Spain registered an increase in economic cyber-espionage in 2016, in particular against the ICT, defence, chemical and healthcare sectors.

The 2018 Verizon Data Breaches Investigation Report states that cyber-espionage in the public sector constitutes up to 77% of all cyber-intrusions. The number of cyber thefts affecting academia and research centres has risen in the past few years - the European Union Institute for Security Studies emphasizes that sensitive data sources will increasingly be targeted as well as long-term research fields.

Given its relevance, finance sector is victim to a high number of incidents in the UK.

The Swedish defence sector has been subject to thefts or attempts to steal trade secrets.

In Denmark, the national Centre for Cybersecurity indicates in its latest report that the threat is very high.

Italy reports on average more incidents or attempts of cyber-theft in the luxury sector.
Impacts on Companies

Estimating the impact

The theft of trade secrets is a major factor when calculating the cost of cybercrime. Estimates from ECIPr for 2018 foresee a possible loss of €60 billion in economic growth and almost 289,000 jobs in Europe alone due to cyber-theft of trade secrets. The exposure increases with digitalisation and by 2025, the losses are expected to be equivalent to one million jobs. Quantifying the negative impact relating to cyber-theft of trade secrets is very difficult. There are many reasons, such as the time delay in recording impacts, the lack of awareness of being cyber-attacked, and the challenges relating to valuation of the trade secrets held.

Based on stakeholders’ feedbacks, the direct impact of cyber-theft of trade secrets accounts for only around 10% of costs; the remaining 90% depends on indirect long-term impacts such as the loss of know how, competitive advantage and loss of jobs. In real numbers, stakeholders reported that the management of the crisis following a cyber-attack is usually associated with costs that can be somewhere between €50 million and €200 million. Almost 70% of stakeholders consider economic and reputational losses as the most relevant impacts suffered because of cyber theft of trade secret.

Economic impacts are proportionate to the value of the information and data stolen. Losing information or data of significant value can have a direct impact on turnover and can even lead to bankruptcy. This was the case when one company went bankrupt partially due to cyber-theft of relevant technologies for the production of military airplanes. There are many cases where SMEs have ceased trading, because they had lost a significant market share, directly due to the subtraction of proprietary information.

OPPORTUNITY COSTS
These 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. 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.

NEGATIVE IMPACTS ON INNOVATION
R&D does generate a competitive advantage if its results are appropriated by those that invested in R&D. If the results are misplaced and freely used by all, including competitors, then R&D does not bring substantial competitive advantages. Additionally, as long as the threat of cyber-theft continues to grow, companies may become less keen to invest in innovation, due to the risk of misappropriation of their R&D.

INCREASED COSTS FOR SECURITY
These 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 (with a growing rate of almost 10% since 2016).

REPUTATIONAL DAMAGE
Companies can suffer substantial value depreciation if it becomes public that they have been hacked, including lost value of customer relationships, loss of contracts, and devaluation of trade name. 600 mid-sized businesses across six European countries reported the occurrence of reputational damage in 48% of incidents and financial loss in 33% of cases.
Policy background

European Policy and Strategy in the EU

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)". Member States are in the process of transposing it through the adoption of new laws on trade secret protection. The Directive contains a number of key definitions (what trade secret are, what can be considered as misappropriation, etc.) and a common set of civil law remedies in case of misappropriation.

In 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 aimed at strengthening Europe’s cyber resilience system and at fostering a competitive and innovative cybersecurity industry in Europe, with particular reference to the need to protect trade secrets from cyber-intrusions.

European institutional set-up for cybersecurity

- ENISA: since 2013, with the adoption of the "EU Cybersecurity Act", ENISA has become the EU agency for cybersecurity and has been awarded with new tasks in supporting EU Member States, EU institutions and other stakeholders on cyber issues. The 2017 proposal on a “Regulation of the European Parliament and of the Council on the future of ENISA” reinforces the role of ENISA and enables the Agency to better support Member States;
- EDA: EU agency for defence tasked with the provision of support to EU Member States in the development of their defence capabilities. It moreover cooperates in the area of cyber security and cyber defence;
- EUROPOL EC3: manages outreach and support for cybersecurity, coordinates prevention and awareness measures and prepares strategic analysis; the formulation of policy and legislation.

The business community and national government bodies regard the EU agencies positively, especially ENISA, because of their coordination role with regard to cybersecurity.

The Directive 2016/943 on "the protection of undisclosed know-how and business information (trade secrets)":
- Harmonises key definitions such as "trade secret", "unlawful acquisition, discloser and use of a trade secret".
- Contributes with a set of civil law remedies (injunctions, damages, destruction of tainted goods, etc.)
- Provides for safe harbours (reverse engineering), exceptions (ex: whistleblowing) and safeguard clauses (ex: proportionality) to prevent abuse
- Supplies courts with means to protect the confidentiality of trade secrets disclosed to the court

The Directive does not:
- Establish criminal sanctions
- Interfere with EU/national rules governing disclosure of information

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

In 2013 The Commission on the Theft of American Intellectual Property estimated that trade secret thefts equate to 1% - 3% of US GDP per year.

The Obama Administration:
- Released in February 2013 the “Administration Strategy on Mitigating the Theft of US Trade Secrets”
- Signed in 2015 the Bilateral Economic Cyber-espionage Agreement with the Chinese counterpart;
- Issued the “Defense Trade Secrets Act” in 2016, which creates a private civil action against misappropriation of trade secrets.

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 cyber-attacks deterrence” contains a report incorporating the deterrence agenda and an additional document, explaining the Administration’s international engagement strategy.
Prevention & Mitigation Measures

Five Main Areas to Limit the Risk of Cyber-intrusion

There are five fundamental cybersecurity measures, which companies and organisations can employ to limit the risk or extent of damage arising from cyber-intrusion.

1. **Identity and Access Management**
   - The security discipline that enables the right individuals to access the right resources at the right times for the right reasons.

2. **Data Security Measures**
   - Particular cybersecurity protections that deal with how confidential data may or may not be stored and transferred.

3. **Perimeter and Network Defences**
   - Firewalls, data encryption and online use restrictions are examples of perimeter and network defenses that companies can implement.

4. **Communication and Training**
   - Clear communication protocols and training employees in cybersecurity and other aspects are vital best practices.

5. **Monitoring**
   - Cybersecurity efforts need to be monitored, measured and improved over time as incidents arise, technology advances, staffing changes and business models evolve.

A good strategy comprises a multidisciplinary approach

A poor risk management strategy influences the overall security of a company and can potentially lead to greater vulnerability to cyber-intrusions. Experts point out that a company’s risk culture is the cornerstone of a resilient enterprise. A risk assessment, taking into consideration all of the security controls available, should lead the company to review its policies and, very likely, adopt new technologies. Appropriate technological tools and mechanisms assist a company in being able to identify cyber-intrusion.

Specific technological measures reported during interviews

- Intrusion detection tools
- Log monitoring tools
- Penetration testing activities
- Encryption

Supply chain risk management represents another crucial issue for companies, as all the constituent actors of the supply chain must protect trade secrets; especially considering that SMEs are less aware and protected and therefore more vulnerable to cyber-intrusion.

Companies need to raise awareness among their own workforce on the topic and emphasise the importance of training at all levels. A good way of raising awareness among senior management is to run an attack simulation with them to ensure that the company’s processes are suitably robust in the event of an attack.

38% of attacked companies increased security awareness training among employees

In the last few years, some reports point out an increase in the level of risk awareness among CEO and management board members. This is partly attributable to the introduction of the GDPR and NIS Directive, and also cybercrime-related legal frameworks.

**Cybersecurity Frameworks**

A Cybersecurity Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk, thus promoting the protection and resilience of companies. In the last few years important initiatives have been undertaken at national level, such as: the CIIP Framework in France, the Italian National Cyber Security Framework (based on the NIST Framework), the “Esquema Nacional de Seguridad” in Spain and the “Cyber Assessment Framework” in UK. However, the rate of adoption of these tools is still very limited.
Incident Notification

The NIS Directive, together with the Framework Directive for Electronic Communications sets out obligations concerning the notification of incidents, however these are exclusively for operators of essential services and providers of electronic communications, leaving aside all other companies and organisations operating across the EU.

Computer Emergency Response Teams

In recent years, Computer Emergency Response Teams (CERTs or CSIRTs) have been developed in both private and public sectors as small teams of cyber-experts who can effectively and efficiently respond to security incidents and cyber-threats. National CERTs act as security points of contact (PoC) for the country, having a role either as support to national law enforcement institutions or as the first entry point of reports, as these are best placed to collect and share information.

Not all CERTs established across Europe are member of the CERTs network and they do not report information on cyber incidents in a standard manner at European level through CERT-EU.

CERT-EU

Awareness-raising actions are needed so that companies and organisation are conscious of the CERT’s existence and its powers. For example, in 2018 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, with an increasing number of entities and organisations.

Stakeholder’s Opinions

The majority (two thirds) of stakeholders interviewed were of the view that creating a standard process for information and assessment of cyber-thefts of trade secrets would be a positive outcome. The creation of a reporting system framework represents one practical way to improve the level of information and general awareness about cyber-theft of trade secrets incidents and assess the impacts of the phenomenon. On the other hand around 15% of stakeholders interviewed felt that it would be difficult to implement such a system as companies are often unable to detect an intrusion or are unwilling to share information for reputational reasons. Another option discussed was that business associations could be responsible for the creation of an information exchange platform. This would be a favourable solutions as companies tend to trust business associations with whom they are members.

Mandatory Vs Voluntary

More than 60% of stakeholders who agreed with a reporting system suggested that it should be mandatory, rather than on a voluntary basis.

As reporting is already mandatory when it comes to communicating other kinds of cyber incidents, the rule should be extended to trade secrets and Intellectual Property Rights (IPRs) and should apply to all companies and organisations, or at least to all publicly listed companies in order to avoid repercussions in the stock market.

A voluntary reporting system was supported only by around 20% of stakeholders. 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 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 of the attack, but the tools and methods used by hackers and those adopted in response.
Cyber-espionage in ThyssenKrupp

On 8th December 2016 the German industrial conglomerate ThyssenKrupp revealed that technical trade secrets were stolen in a cyber-intrusion of its systems. 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.

It is understood that the company discovered the attacks in April, though the criminal activity apparently occurred in February. The Company said it could not estimate the scale of the loss of trade secrets. At the time, ThyssenKrupp also said the intrusion should not be blamed on security deficiencies within 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."

Operation Cloud Hopper
UK managed IT service providers

Since late 2016, the espionage campaign, which we refer 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). 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 MSPs and exfiltrate sensitive data.

When the Hacking Team got Hacked

Hacking Team is an Italian software firm company that creates digital surveillance tools for government departments, the Federal Bureau of Investigation (FBI) and UK National Crime Agency (NCA).

On 6th July 2015, a post on the company's Twitter account revealed the intrusion, compromised by an unknown individual who published an announcement of a data breach against Hacking Team's computer systems.

Links to over 400 gigabytes of data

Hacking Team lost around 20% of its clients, experiencing an estimated direct economic loss of approximately $8.2 million per year.

-20% Loss of Clients

-8.2m $/year
Estimated Economic Loss
Recommendations: Awareness and Technology

Awareness and Training

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

- Organise targeted events. Setting up events in collaboration with industrial associations and organization 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 be published in specialist magazines and programmes;
- Disseminate case studies among senior executives. Case studies are fundamental for achieving widespread comprehension of the threat of cyber-theft of trade secrets;
- Provide a public repository of best practices and guidelines. A possible model tool can be the UK NCSC, which offers guidelines to SMEs. Best practice measures include classification of internal departments, appointment of an employee person responsible for cybersecurity, running exercises and simulations, running regular vulnerability assessments, encryption on trade secrets, role of national CERTs and ENISA, and log and monitor marking.

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

- 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;
- 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 EU Member States and with EU officials.

Boost training of professionals and relevant civil servants:

- Support the creation of multidisciplinary 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. This should be encouraged in tandem with the development of specific units tackling the issue across EU institutions;
- Establish regular training and certification. EU Member States 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.

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. The EU should consider 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.
- Provide incentives to SMEs. EU institutions should push national governments to provide incentives, subsidies or tax relief to SMEs investing in the adoption of countermeasures for cyber-theft of trade secrets. Another suggested mechanism would be a "technology welfare" to allow SMEs access to basic technologies protecting their critical information. Promotion of national incentive policies enabling companies to improve their reputation when receiving security certifications. Award extra points at public tenders should the company demonstrate an increase in cybersecurity standards following a past attack;
- Disseminate guidelines for SMEs. Issue guidelines specific for businesses at risk and the ones working within a supply chain. Guidelines should indicate what are the minimum requirements 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 with their technological knowledge SMEs.

Push the development of new tools and technologies:

- Increase public funding in research and innovation. Launch within the Horizon 2020 programme an EU "Cyber Theft of Trade Secrets" topic in the focus area "Boosting the effectiveness of the Security Union". New Research and Innovation Actions in the next framework programme Horizon Europe can boost the development of new tools and technologies. Specific funding for the development of new solutions could be included in the new Digital Europe programme;
- Boost private funding in research and innovation. EU institutions 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 EU 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 focused on attracting innovation contributors to define and develop practical tools for the prevention of cyber-theft of trade secrets.
Recommendations: Coordination and Law

Enhance Institutional and Coordination Capabilities

- **Adoption, implementation and support for a common assessment framework.** Partner with Member States to foster companies’ adoption of a common vulnerability assessment framework for identifying weaknesses in their IT systems and secure their trade secrets. To this end, PPP could be a driver.
- **Develop a tool-kit supporting businesses in identifying, classifying and protecting their confidential information.** Such a tool-kit 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.
- **Consider the adoption of a framework for the assessment of value of trade secrets.** EU institution could coordinate with MSs 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

- **Strengthen the role of ENISA.** The Commission and Member States through the ENISA Management Board should equip the Agency with adequate resources and executive competences, which would consider specific coordinating powers over national authorities in order to prevent cyber theft of trade secrets;
- **Foster the role of the CSIRTs network.** CSIRT’s should strengthen its centralisation role and share across all affiliated national CERTs facts and trends on cyber theft of trade secrets incidents.

Strengthen cooperation between key players as well as with other national or international organisations

- **Foster cooperation on prevention of cyber theft of trade secrets with national and international organisations.** The EU should enhance cooperation and exchange of information with sectoral organisations, such as law enforcement, military, and economic, to strengthen cross-border cooperation.
- **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;
- **Strengthen cooperation and dialogue between key players.** The next Horizon Europe could stimulate the implementation of coordination and actions, along the lines of the FP7 project EU Cyber Security Protection Alliance (CYSPA).
- **Push for a renewal in the international debate on FIN 48 IFRS.** Consider a tax relief provision for companies complying with certain safety standards.

Strengthen Law Enforcement

- **Introduce more stringent cybersecurity laws and penalties.** Extend the objective of current legislation. While at national and EU level several pieces of IP law address trade secrets misappropriation, there is no specific legal focus on its cyber dimension. This uncertainty limits companies legal predictability and law enforcement capacities. The EU and national authorities could thus 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.** The EU could launch a wider stakeholder engagement process targeting companies and SME in order to understand their perceptions on the advantages and disadvantages of having a reporting system. It would also be relevant to understand views on the possible structure of such reporting system, whether it should be voluntary or mandatory.
- **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.

Boost Investigation capabilities

- **Create a National Cybersecurity Investigative Department responsible for prosecuting cyber-theft of trade secrets.** This could operate as an independent law enforcement organisations, 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.
Conclusions

The threat is concrete
The study shows that cyber theft of trade secrets is one of the main threats for companies and organisations in the European Union, both in terms of prevalence and in terms of impact.

Prevalence of the phenomenon
Analyzing quantitative data available, they clearly show how the threat is concrete, especially for some particularly affected sectors. Verizon shows that in 2016, 105 cyber-espionage incidents occurred in the manufacturing sector, which is the most affected sector in EU, out of which 93% perpetrated by external actors, and in 91% of the cases reported regarding trade secrets. Data gathered in the study also show how cyber theft of trade secrets affects more SMEs than large companies, due to their low budget dedicated to cybersecurity, the lack of awareness of being a target and the lack of skilled IT professionals.

Lack of awareness
One of the key reason for the lack 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 make the challenge even more daunting. Many companies do not believe they are a target for this type of cyber-intrusions 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.

Negative Impacts suffered by companies
Estimates of February 2018 provide details of the negative impacts at the European level of cyber theft of trade secrets: about €60 billion lost in economic growth, resulting in a loss of competitiveness, jobs and reduced R&D investments. More specifically, 269,000 jobs could be at risk in 2018 in Europe and 1 million jobs could be at risk by 2025. Stakeholders emphasized that direct impacts account for about 10% of costs the company will have to face. Therefore, the remaining 90% of costs are due to indirect impacts that are effectively measured and assessed 5-6 years after the cyber-intrusion.

Preventing, mitigating and reporting systems
The regulatory framework and institutional set up at member state and EU level is quite developed, even though it seems more aimed at countering cyber threats in general, rather than cyber theft of trade secret specifically. Actually, obligations are very limited or non-existent and companies do not report incident in a standard manner. A common and coordinated reporting system at EU level would be helpful for timely response intervention, and based on interviews (65% of stakeholders), it should have a mandatory nature. Regarding the European institutional set-up for cybersecurity, there are three main agencies (ENISA, EDA and EUROPOL-EC3) and the CERT-EU.

Actionable recommendations
To cope with the shortcomings found, the study provides a final set of actionable recommendations to be implemented by the European Commission. The recommendations are identified on 4 main areas of improvement, namely: Awareness and Training, Facilitate business in addressing the challenge, Enhance the institutional and coordination capabilities, Strengthen Law Enforcement.