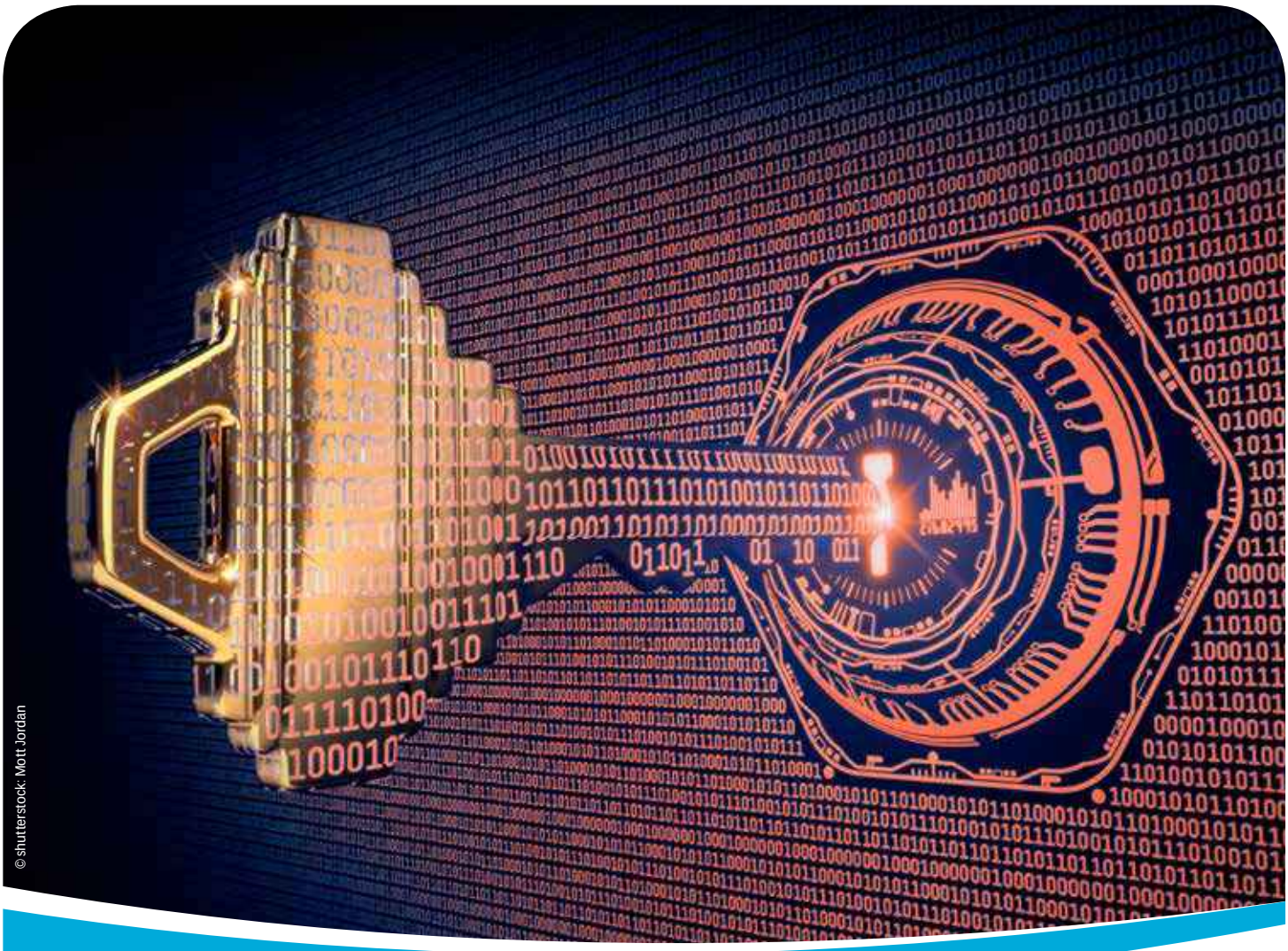


© shutterstock: Mott Jordan

Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks

STUDY

European Economic and Social Committee

Cybersecurity

Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks

General information

STUDY FOR	The European Economic and Social Committee (EESC)
REQUESTING SERVICE	The Employers' Group
STUDY MANAGING SERVICE	Relations with Organised Civil Society and Forward Studies Unit Information and Studies Centre
DATE	March 2018
MAIN CONTRACTOR	The Hague Centre for Strategic Studies
AUTHORS	Katarina Kertysova, Erik Frinking, Koen van den Dool, Aleksandar Maričić, Kumar Bhattacharyya
CONTRIBUTORS	Hannes Rõõs, Louk Faesen, Nicholas Farnham
CONTACTS	Lange Voorhout 1 2514 EE The Hague The Netherlands info@hcss.nl

IDENTIFIERS

		ISBN	
PRINT	QE-01-18-515-EN-C	978-92-830-4104-7	doi:10.2864/917494
PDF	QE-01-18-515-EN-N	978-92-830-4105-4	doi:10.2864/98090

Abstract

This study examines the impact of cyber-related threats and challenges on corporate Europe and the degree of engagement of European businesses in tackling issues at stake. Although the new digitization era offers huge economic and social opportunities, it also changes the nature and magnitude of cyber risks and creates new vulnerabilities cyber attackers seek to exploit. European countries and businesses are targeted with growing frequency. Many companies, however, remain unaware or seem to underestimate, and even neglect the vulnerabilities they are facing through and in cyberspace. An open, safe and secure cyberspace is indispensable for the reliable functioning of European economies. Recognizing the importance of corporate cybersecurity for the economic wellbeing of Europe, this study presents the challenges European companies face in implementing good cybersecurity practices and offers recommendations on how to overcome them. The study first looks into the current cyber threat environment, and assesses its impact on the private sector. The second part addresses the level of awareness, preparedness and resilience against mounting cyber threats at the European, national and corporate level. Third, key challenges and bottlenecks that inhibit implementation of good cybersecurity practices are presented and analyzed. The final part outlines good practices and inspiring examples observed across the EU that could help overcome the aforementioned bottlenecks.

Table of contents

List of tables

List of figures

Executive Summary

The fourth industrial revolution, also known as the era of digital transformation, will fundamentally change our personal lives, professional activities and societal environment. We are not living in an era of change, but in a change of era.

While this new digitization era offers vast economic and social opportunities, it also alters the nature and magnitude of cyber risks and creates new vulnerabilities that cyber attackers seek to exploit. European countries and businesses are targeted with growing frequency. According to the 2017 Global State of Information Security Survey, at least 80% of companies in Europe have experienced at minimum one cybersecurity incident over the last year and the number of security incidents across all industry worldwide increased by 38% in 2015 compared to the preceding year.[1] According to some estimates, theft of commercial trade secrets, business information and personal data as well as disruption of services and of infrastructures result in economic losses of billions of euros each year.[2] Although the use of ransomware is hardly a new occurrence, (non)Petya and WannaCry ransomware attacks of the past year crippled businesses across Europe and serve as a reminder of the need for continued vigilance.

Many companies, however, remain unaware or seem to underestimate and even neglect the potential impact on their businesses. A survey conducted by Marsh revealed that as much as 69% of European companies have either no or only basic understanding of their exposure to cyber risks.[3] This is not only crucial to their own commercial performance, the European economy at large will also benefit from a more cybersecure and cyberaware environment.

In addition to the rapidly changing cyber threat landscape, companies also have to keep pace with the dramatically changing regulatory environment. With the implementation of the EU's General Data Protection Regulation (GDPR), companies will soon be required to report data breaches to national data protection authorities and – where the threat of harm is substantial – to affected individuals.[4] As the failure to do so could result in staggering fines, organizations should be preparing to comply with all aspects of the GDPR. However, according to the results of Symantec's State of European Data Privacy Survey, a large number of companies remain unaware of the new regulation and its implications, and are underprepared for its implementation.[5]

---

1 PwC, "The Global State of Information Security® Survey 2017," www.pwc.com, n.d., http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html.

2 European Commission, "Commission Boosts Cybersecurity Industry and Steps up Efforts to Tackle Cyber-Threats," europa.eu, July 5, 2016, http://europa.eu/rapid/press-release_MEMO-16-2322_en.htm?locale=FR.

3 Marsh, "Continental European Cyber Risk Survey: 2016 Report," October 2016, 7, http://www.hkbb.ch/uploads/6869.

4 "FireEye - Marsh & McLennan Cyber Risk Report 2017 - Cyber Threats: A Perfect Storm About to Hit Europe?" (Milpitas, CA, USA: FireEye, Inc., 2017), 15.

5 Symantec, "Businesses Underprepared for GDPR | Symantec," www.symantec.com, October 18, 2016, https://www.symantec.com/en/uk/about/newsroom/press-releases/2016/symantec_1018_01.

This study looks into the current state of European cybersecurity from a business perspective, and the degree of engagement of companies in tackling issues at stake. The report assesses the current cyber threat and vulnerability landscape in Europe and the level of awareness, preparedness and resilience against mounting cyber attacks at the European, national and corporate level. It then examines main challenges and bottlenecks that companies face in implementing good cybersecurity practices, both from an internal, company perspective, as well as from an external, public policy perspective. Concluding, the study offers inspiring initiatives and good practices that have been implemented across the EU.

1.1 Key findings: Current cyber threat and vulnerability landscape

Organizations find themselves in an increasingly complex cyber threat environment, having to face multifaceted cyber risks, both internal and external. These risks affect business continuity, intellectual property, and personal and professional integrity.

The most prevalent threat categories are 1) Malware and phishing; 2) Distributed Denial of Service (DDoS); and 3) Data breaches.

Malware and phishing constitute the most common type of threat encountered by companies across Europe. Although costs of a malware incident are relatively low in comparison to other types of attacks, its high rate of occurrence makes malware the most costly attack vector overall. Businesses across Europe should be particularly wary of emerging trends in ransomware attacks. As a result of the rise in IoT devices, DDoS attacks have increased in size, sophistication and frequency. Although DDoS attacks most often target large organizations and digitized economies, inadequate mitigation strategies make SMEs and less digitized economies relatively vulnerable. Although the number of data breaches has declined, the average size of a data breach (number of records lost) is on the rise. Sensitive personal information – such as financial and health records – remains the key focus of cyber attacks. Each in their own way, they have the potential to cause physical damage, operational disruptions and reputational damage.

With regards to economic sectors, finance, healthcare, retail, business services and information technology are most frequently hit by data breaches. Although all sectors are susceptible to cyber attacks, healthcare stands out in terms of its exposure. In contrast to financial services, energy sector or telecommunications that have long been targeted by cyber attacks and have developed sophisticated defense mechanisms, healthcare lags behind in terms of its awareness and preparedness for cyber attacks.

Small and medium-sized enterprises (SMEs) constitute the weak link in cyber attacks. They face rising threat levels and pay the highest price for operating online. Despite growing threat levels, they remain ill-prepared for cyber attacks, showing lower than average maturity levels. SMEs struggle not only due to a lack of awareness, but also because they perceive cybersecurity as a costly endeavor. Although the average performance in terms of awareness and preparedness is generally low, SMEs in northern Europe perform marginally better than those in southern Europe.

The true economic costs of a lack of cybersecurity are difficult to determine. Review of reports on costs assessments highlight incoherence of methodologies, definitions and indicators of cost measurements. However, estimates indicate that indirect losses, such as reputational damage or loss of customer trust, tend to be much larger than direct costs and expenses for protection measures.

1.2 Key findings: The state of awareness and resilience across Europe

Governments play an important role in providing a secure business climate. This business climate, however, varies from one Member State to another. Our findings show that there is still a visible gap between countries in terms of knowledge, awareness and capacity to deploy strategies, programs and capabilities in the field of cybersecurity. While Estonia, France, Norway and the United Kingdom lead by example, countries of Southern and Eastern Europe – notably Slovenia and Slovakia – generally lag behind. The implications are twofold. First, heterogeneity of security and privacy regulations across the EU presents a hurdle to effective cross-border collaboration. Second, the fact that certain Member States lack the necessary capabilities to defend against emerging trends makes the European cybersecurity architecture disparate and vulnerable to potential attacks.

The EU has become an important initiator of cybersecurity and data protection across the EU, as demonstrated by numerous actions, measures and initiatives put in place to improve cyber resilience and response. The adoption of the NIS Directive and the GDPR are of particular relevance. While the NIS Directive imposes notification requirements around security incidents, the GDPR focuses on personal data breaches. As such, the EU acts as an important driver for the development of cybersecurity in both the public and private sector settings. The GDPR, in particular, is expected to change the current regulatory environment profoundly. However, it first needs to be accepted, then implemented, and only then we can judge its effectiveness in practice. On the whole, key European strategies and legislation have – up until now – primarily tackled the protection of personal data, security of operation of large scale and publically accessible information networks, and protection of operation of key infrastructures (of vital importance). The importance of cybersecurity in industrial settings has only been recognized marginally, and deserves increased attention.

At the corporate level, cybersecurity preparedness of individual enterprises increased across all company sizes. In 2015, 32% of companies had a formally defined ICT security policy in place, which represents a 6% increase since 2010. With regards to company size, the share of large enterprises with a formally defined ICT security policy was almost three times the share of small ones. Geographically, the highest percentages were recorded in Sweden and Portugal.

With regard to cybersecurity investment, there is a discrepancy between the growing digitization of society and resources dedicated to cybersecurity. Neither individual Member States nor private enterprises seem to be backing their cybersecurity with appropriate resources. At the same time, there seems to be an inverse relationship between state-level preparedness and private-level preparedness.

This study also assesses supply and demand for cybersecurity professionals. The available supply of ICT personnel has been declining and the gap is expected to reach 755,000 potential vacancies in 2020. In addition to ICT professionals, there is a shortage of cyber experts in academia and civil society, who would be responsible for educational activities.

1.3 Key findings: Bottlenecks in public and private policies

Corporate Europe faces a wide range of structural challenges in identifying, preparing for and responding to cyber threats and incidents. From the external, public policy perspective, the bottlenecks relate to the fragmented regulatory environment, lack of sufficient financial support, absence of national educational programs, discrepancies in threat intelligence sharing policies, the absence of a coordinated vulnerability disclosure (CVD) process in Europe, and lack of trust to share information between the public and the private sector. The challenges associated with the implementation of the GDPR, which can negatively impact businesses across the EU, are currently most prevalent.

From the internal, company perspective, challenges include the general lack of awareness about cyber risks exposure and the implications of the GDPR, lack of skills and training, inadequate cybersecurity spending, corporate under-reporting, technological vulnerabilities, long dwell times, challenges pertaining to organisational design, lack of incident response plans and lack of trust to share information.

1.4 Key findings: Good practices and lessons learned

Numerous inspiring examples have been put in place to improve cybersecurity of the private sector across Europe.

Public-private partnerships have proven effective in dealing with cyber threats. Such partnerships can draw from strengths that private and public agencies possess, which are often complementary. Private entities control much of the critical infrastructure that is vulnerable to cyber threats and have developed their own cybersecurity programs. Compared to their public counterparts, private companies are capable of mustering more cyber expertise, and can do so more rapidly, which makes them agile and enables them to respond faster. The public sector, in turn, possesses large resources and can facilitate the transfer of information from other states. In Europe, public-private partnerships exist in varying forms, with varying degrees of integration between the two actors. The Dutch case is used to illustrate the positive impacts of public-private partnerships in practice.

‘Cyber communities’ have been successful in bringing a broad selection of stakeholders together, enhancing trust among them, encouraging the exchange of information and experience, as well as the pooling of knowledge and resources. Initiatives of professional associations and collectivities across Europe have been particularly effective in increasing the awareness of, and resilience against, cyber attacks among private companies – both large and small. Such communities extend beyond industry and government and incorporate universities as well as civil society.

Educational activities, both public and private, have been successful in raising the awareness of cybersecurity issues and enlarging the pool of highly qualified ICT professionals, including cybersecurity specialist and data experts, who are tailored to meet the needs of the cybersecurity market. Germany, UK, and Czech Republic lead by example with regard to cybersecurity education programs offered at the national level. By means of certifications, courses, on-the-job trainings and consultancy services, the private sector also plays an important role in educating cybersecurity specialists. The majority of successful educational/training initiatives currently take place at the associational level, as evidenced by the positive impact generated by the #DigitalSME4skills campaign.

Cybersecurity challenges, competitions, hackathons and prizes constitute another strategy embraced by both the private and the public sector. On a national level, they have been successful in helping to increase the pool of ICT talent, stimulating interest in cybersecurity and combating the shortage of e-skills. They also provide the cybersecurity industry with an advertising platform and a means to come into contact with potential future employees.

The uptake of cybersecurity insurance constitutes another approach observed in Europe that has helped companies address cyber risks. Although the cyber insurance market is still very young, the implementation of both the NIS Directive and the GDPR are expected to positively influence its growth.

1. Introduction

The advent of networked technology has spurred innovation, cultivated knowledge, encouraged free expression, and increased our economic prosperity. Like the steam engine, electricity and automation before it, new digital technologies permeate every aspect of our lives, fundamentally impacting economy and society as a whole.

Although the new digitization era offers huge opportunities, it also changes the nature and magnitude of cyber risks and creates new vulnerabilities that cyber attackers seek to exploit. Organizations now find themselves in an increasingly complex cyber threat environment. Traditional means of attack, such as malware and spam – seen as major threats a few years ago – have been supplanted by larger and more devastating threats. Ransomware or sophisticated denial of service attacks targeting critical infrastructure – manufacturing plants, aviation systems, power stations, transportation networks, water systems and even nuclear facilities – have become the new reality in Europe.[6]

European countries and businesses are being targeted with growing frequency. According to PwC's 2017 Global State of Information Security Survey, at least 80% of companies in Europe have experienced at minimum one cybersecurity incident over the last year and the number of security incidents across all industry worldwide increased by 38% in 2015, in comparison with the preceding year.[7] According to some estimates, theft of commercial trade secrets, business information and personal data, disruption of services and of infrastructures results in economic losses of billions of euros each year.[8] Although the use of ransomware is hardly a new occurrence, the past year alone recorded two major ransomware attacks that crippled businesses across Europe. In Spain, telecommunications fell victim to targeted attacks. In Germany, train systems were affected. In the UK, the public health system was hit hard.[9] In sum, no sector of any economy is immune from attack.

The responsibility is threefold: the public sector, private sector and individuals all have a role to play in ensuring and promoting their own cybersecurity. Many companies, however, remain unaware or seem to underestimate and even neglect the subject. As the former director of Cisco Systems John Chambers once said:[10] "there are two types of companies: those that have been hacked and those who don't know they have been hacked".[11] Ransomware attacks of the past year served as a reminder of the need for continued vigilance. Other attempts are likely to follow and preparedness is crucial.

6 Marsh & McLennan Companies, "2017 Cyber Threats: A Perfect Storm about to Hit Europe?" (FireEye, Inc., January 2017), 3.

7 PwC, "The Global State of Information Security® Survey 2017."

8 European Commission, "Commission Boosts Cybersecurity Industry and Steps up Efforts to Tackle Cyber-Threats."

9 Daniel M. Gerstein, "The WannaCry Virus, a Lesson in Global Unpreparedness," Text, May 17, 2017, http://nationalinterest.org/feature/the-wannacry-virus-lesson-global-unpreparedness-20719.

10 PwC, "The Global State of Information Security® Survey 2017."

11 Zeus Kerravala, "John Chambers' 10 Most Memorable Quotes as Cisco CEO," Network World, July 24, 2015, https://www.networkworld.com/article/2952184/cisco-subnet/john-chambers-10-most-memorable-quotes-as-cisco-ceo.html.

In addition to the rapidly changing cyber threat landscape, companies also have to keep pace with the dramatically changing regulatory environment. With the implementation of the EU's General Data Protection Regulation (GDPR), companies will soon be required to report data breaches to national data protection authorities and – where the threat of harm is substantial – to affected individuals.[12] As the failure to do so could result in staggering fines, organizations should be preparing to comply with all aspects of the GDPR. However, according to the results of Symantec's State of European Data Privacy Survey, a large number of companies remain unaware of the new regulation and its implications, and are underprepared for its implementation.[13]

The following study intends to offer a better understanding of the current state of European cybersecurity from a business perspective, and of the degree and engagement of companies in tackling issues at hand. The findings proceed in four parts. Part one assesses the current cyber threat and vulnerability landscape across corporate Europe. Part two illustrates the current level of resilience and awareness at the European, national and corporate level. Part three lists the main challenges and bottlenecks that companies face in implementing good cybersecurity practices, both from an external public policy perspective, and from an internal (company) perspective. The fourth and final part provides good practices and illustrative examples for corporate Europe to follow.

12 Marsh & McLennan Companies, "2017 Cyber Threats: A Perfect Storm about to Hit Europe?" 15.

13 Symantec, "Businesses Underprepared for GDPR | Symantec."

2. Methodological approach

Given the limited size of the project, we conducted our analysis primarily on the basis of existing literature (official documents and secondary sources) and available data. Having identified our knowledge gaps, a desk research was supplemented by a limited number of interviews with relevant stakeholders to help us get a better understanding of the challenges and practices experienced within the business communities in Europe. The interview questionnaire (see Annex 4) was designed to fill in the gaps not available via desk research. In the next step, the interview results were complemented by information gleaned by participating at the Europol-ENISA Internet of Things Security Conference, held on 18-19 October 2017 in The Hague, the Netherlands. Interviews and interaction with security professionals and IT specialists during the conference helped us retrieve 'the story behind the story' of some of the identified challenges and practices that surfaced in desk research.

Research questions were grouped into the following four categories:

Risk Analysis: what is the likelihood that businesses across Europe get affected by cyber attacks and cyber threats and what would their effects be? What is the current cyber threat and vulnerability landscape?

Awareness and Resilience: what actions are businesses across Europe taking in order to become more aware of the risk factors and to protect against them?

Bottlenecks in public and private policies: what challenges do private enterprises across Europe face in implementing cybersecurity practices, both from an internal, company perspective, as well as from an external, public policy perspective?

Good practices and other inspiring examples to improve cybersecurity: are there effective public policy instruments to support businesses in improving their cybersecurity? Are there public-private partnerships or private sector initiatives that can provide examples for businesses across Europe to follow, and help them increase awareness and reduce vulnerabilities to cyber threats and incidents?

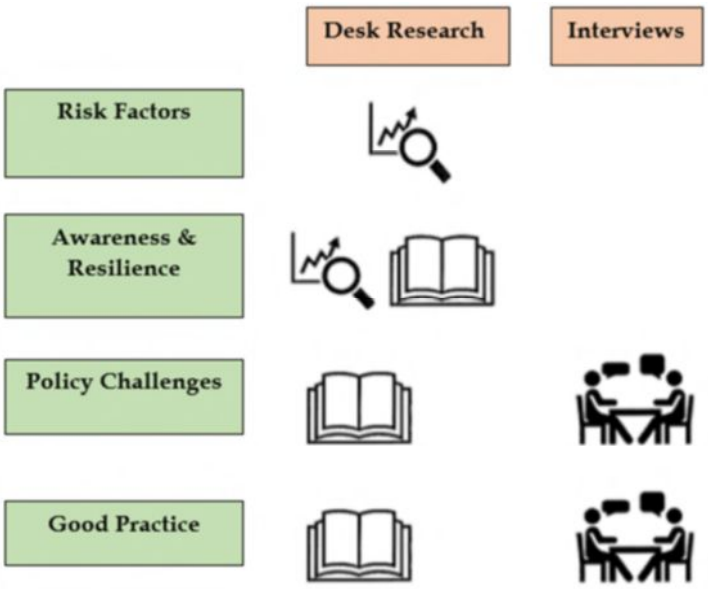


Figure 1: Methodological Approach

2.1 Overview of the available information and data sources

The following table offers an overview of the strengths and weaknesses of various sources of information consulted for the purpose of this study.

Source type	Examples	Strengths	Weaknesses
Public statistics and reports	Eurostat, ENISA, World Economic Forum, ITU, reports from national or governmental CERTs.	- Many databases cover all EU Member States. - Availability of country-specific data - Robust and presumably bias-free.	- Quality of data - Lack of private sector data
Independent Research Reports	Ponemon, Potomac, Harvard Belfer Center, etc.	- Relatively unbiased approach - Sound research, often based on quantitative data	- Lack of EU-specific data - Varying methodologies, frameworks and conclusions
Private (cybersecurity) sector reports	Comodo, McAfee, FireEye, Symantec, PwC, Kaspersky, Verizon reports, etc.	- Wide coverage (according to market share). - Numerous reports available covering the causes, dynamics and	- Biased data and "misaligned incentives": cyber-security companies have an interest in framing threats in a way that supports demand for their

		effects of cyber risks.	products. - The focus is generally global, rather than on Europe. - Data collection depends on market share of an individual company.
Interviews	Representatives of HSD, ECP, ECSO, Digital SME Alliance, etc.	Interview questions tailored to meet our needs and fill in the gaps in terms of content available.	Limited audience (limited selection of business representatives in Europe; 3 interviews took place).
Anecdotal evidence	European Political Strategy Centre; Dataloss db; Hackmageddon; Shadowserver Foundation, etc.	Detailed information on individual breaches. Can help contextualize and illustrate trends.	Less suited for (comparative) analysis. Data collection relies on available open-source information. Lack of uniform standards for reporting incidents. Selection bias: media outlets base their choice of incidents to report on their access to suitable corroborating detail and level of interest of their audience.

Table 1: Overview of the available information and data sources[14]

2.2 Identified challenges

A number of issues challenge a comprehensive and comparable analysis of each of the categories of research questions identified. We list these issues and our methodological approach in tackling them.

2.2.1 Risk analysis

When conducting desk research, we came across numerous reports covering the causes, dynamics, and effects of cyber risks. This proliferation of reports is an important sign of the increasing

14 This table was inspired by methodology used in the: Neil Robinson et al., "Data and Security Breaches and Cyber-Security Strategies in the EU and Its International Counterparts" (Directorate General for Internal Policies Policy Department A: Economic and Scientific Policy Industry, Research and Energy, September 2013).

prominence of cybersecurity for private and public entities alike. However, while there is no shortage in the number of reports available, well defined and comparable cyber threat data and risk assessments across the EU is currently missing. To address the variability of outcomes, we examined a variety of sources for similar or identical indicators and provided the spread of their assessment.

2.2.2 Determining economic costs

Whether we are talking about cybercrime, cyber incidents, or cyber breaches, we have found that it is a very demanding task to determine their overall impact on the economy. In estimating the economic impact of cybercrime and/or incidents, there are various reports that use different approaches. Some reports focus on the costs incurred by cybercrime, such as malware and social engineering. Other reports cover the costs of data loss and/or incidents without malicious intent per se. The following study will aim to present the spread of the available assessments. Because of this lack of coherence in methodologies, definitions and indicators in cost measurements, it is hard to present a clear-cut overview of economic costs of cybersecurity incidents across the EU. The data is more useful for understanding general trends such as the overall rise of costs associated with cybercrime. To be able to determine the true economic costs of cybercrime, there is a need for standardized working definitions, a methodology and structured data collection.

2.2.3 Awareness and resilience

Similar to the threat landscape, assessments about governments' and companies' spending on cybersecurity and prevention differ widely. Determining the size of investments in ICT and cybersecurity is challenging because of: (i) the lack of reliable and consistent reporting and data sets; (ii) the absence of a shared definition of 'cybersecurity', which makes it difficult to determine which costs are attributed to cybersecurity per se; (iii) varying methodologies used to estimate the size of the cybersecurity market; (iv) the fact that cybersecurity is increasingly evolving into an integral part of business operations – rather than being a separate unit cost. As a consequence, estimates of cybersecurity spending and the scope of the cybersecurity market differ widely. In addition, most of the reports are globally oriented and lack data focusing specifically on the EU or its individual Member States.

2.2.4 Corporate underreporting

Even if data on certain issues is available from the private sector, there is still no guarantee that this data is complete. On the one hand, due to the fear of espionage, corporations are likely to be hesitant to share sensitive information about cybersecurity threats they have faced, vulnerabilities they have perceived and approaches they are implementing or envision to implement. On the other hand, due to fear of reputational damage, a significant proportion of incidents and related costs are never reported to competent authorities. This should be taken into consideration when interpreting available information.

2.2.5 Good practices

Identifying good practices would require a more thorough benchmarking process, which can be a lengthy/time consuming process that goes beyond the scope of this project. Instead, we identify good practices based on more circumstantial data gathered through literature review, participation at the Europol-ENISA Internet of Things Conference, and interviews with relevant stakeholders.

2.2.6 Index limitations

Over the past years, various indices and rankings have been developed in order to assess the cybersecurity performance of a given country or region. Even though indices provide interesting and potentially useful information on the progress of countries on the cybersecurity front, their results need to be taken with a grain of salt. Moreover, differences in methodologies, approaches and geographic coverage obstruct a comprehensive comparison of different indices and their resulting outcomes. In light of these limitations, our analysis is based on the results of the ITU's Global Cybersecurity Index (GCI) – the only recently updated index covering the entire European region.

We address these challenges as described above, but the mere fact that they exist is a worthwhile observation by itself and a situation that requires improvement. Moreover, it is important to note that the research for the work presented was conducted between May and November 2017. As a result, figures and data that are presented may have been updated and some of the recommendations put forward may already be under consideration or implementation by the date of its publication.

3. Current cyber threat and vulnerability landscape across Europe

Each and every organization faces multifaceted cyber risks, both from external and internal sources. The first section of this study attempts to assess the current cyber threat and vulnerability landscape across corporate Europe. Where information is available, types of threats, sources and targets of threats and modus operandi used are assessed. This section looks at the scale of the identified threats, key cybersecurity challenges for European businesses, and contrasts the situation across different sectors, regions and company sizes. It equally offers an assessment of the economic impact of cybercrime and a distinction of different costs related to cybercrime.

3.1 Threats

The costs and impact of cyber threats to companies vary per threat type. Cyber threats are numerous and come in different forms for different purposes. They can originate from external sources as well as from company insiders. Cyber incidents do not always need to result from malicious intent, but can also occur out of mere negligence. Many threats can be seen as complementary elements of a single attack 'vector' – e.g., phishing can be used as a means to deliver and install malware or to obfuscate data. As a result of this complexity, threat categorization and assessments differ significantly across published reports. This section presents an assessment of the most prevalent threat categories, namely 1) malware and phishing; 2) Distributed Denial of Service (DDoS); and 3) data breaches. It should be noted that this list is not exhaustive and some categories may overlap. Even though much of the data and reports on cyber threats are globally oriented and lack EU-specific data, the following findings may nevertheless serve as a useful indication of the current threat landscape across Europe.

3.1.1 Malware and phishing

Malware and phishing are grouped together as they often occur simultaneously as a single attack vector. Malware is essentially a catch-all phrase for malicious software that knows many different varieties. Malware commonly enters a targeted server or a computer as an attachment to phishing emails to deliver a 'payload' – i.e. execute a program to steal or corrupt data. Malware can serve many different purposes, with just as many potential consequences for businesses. It can disrupt business continuity by corrupting or denying access to data. It can also lead to financial damages as a result of the costs of detection, mitigation and recovery. In the long term, malware may cause reputational damage and/or reduce a firm's competitiveness.

Malware constitutes the most common type of cyber threat encountered by companies. It is estimated that 98% of companies worldwide have encountered malware at some point in time.[15] Nevertheless, cybersecurity incidents involving malware are considered to inflict relatively low costs to companies compared to other types of attacks and incidents.[16] Although the damage caused by a single malware

15 Ponemon Institute, "2016 Cost of Cyber Crime Study & the Risk of Business Innovation," October 2016, 8.

16 Kaspersky Lab, "Measuring Financial Impact of IT Security on Business - IT Security Risks Report 2016," 2016, 8.

incident is relatively low, its high rate of occurrence actually makes it the most costly attack vector overall.[17]

Some of the most prevalent types of malware are trojans, worms, viruses, and backdoors (see Figure 2). Trojans are files that appear benign – such as invoices attached to emails – which actually contain malicious code. They require entry strategies such as email phishing to enter a target location. Worms are files that can operate autonomously and are capable of lateral movement between locations within a network. Viruses are programs that can self-replicate and infect other programs. Backdoors are loopholes built into a program or a software – both intentionally and unintentionally – so that an attacker can enter a computer or a network clandestinely.[18]

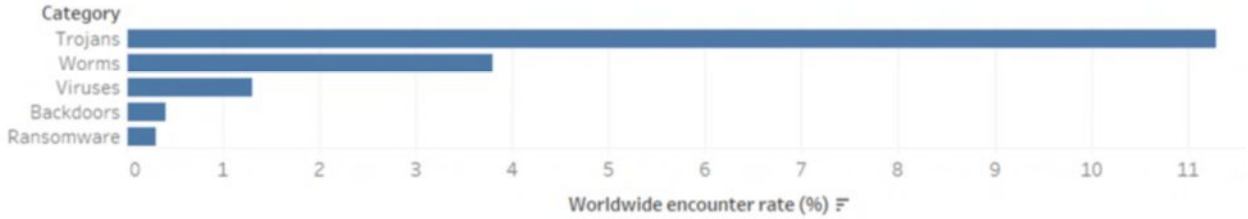


Figure 2: Malware Encounter Rate in the first half of 2016[19]

A specific sub-category of malware is ransomware – malicious encryption of personal data to extract a ransom. Relative to other types of malware, ransomware encounters remain fairly unique. According to Microsoft's *Security Intelligence Report*, ransomware was still one of the least encountered cyber threats in the first half of 2016 (see **Figure 2**).[20] Nevertheless, ransomware has received increased attention, especially in the aftermath of the WannaCry pandemic that spread across the world in May 2017.[21] In 2016, EUROPOL already called ransomware a 'dominant concern' for EU law enforcement, referring to the examples of CryptoWall, CTB-Locker, TeslaCrypt, and Locky.[22] In addition, ENISA considers ransomware as one of the main areas of 'malware innovation'.[23] Private sector reports have also paid increased attention to ransomware as an emerging threat in 2017. Google Research has shown that ransomware became a multimillion dollar business

17 Ponemon Institute, "2016 Cost of Cyber Crime Study & the Risk of Business Innovation," 10.

18 Comodo Threat Research Labs, "Comodo Threat Research Labs - Q2 2017 Report," Quarterly Report, 2017, 6,7.

19 Charlie Anthe et al., "Microsoft Security Intelligence Report - Volume 21 | January through June, 2016" (Redmond, WA, USA: Microsoft, 2016); Comodo Threat Research Labs, "Comodo Threat Research Labs - Q2 2017 Report"; Panda Security, "Pandalabs Quarterly Report Q1 2016," 2016.

20 Anthe et al., "Microsoft Security Intelligence Report - Volume 21 | January through June, 2016," 82–84.

21 The CyberWire Staff, "The WannaCry Ransomware Pandemic: Perspective, Reactions, and Prospects," The CyberWire, accessed November 17, 2017, https://thecyberwire.com/articles/the-wannacry-ransomware-pandemic-perspective-reactions-prospects.html.

22 Europol, "The Internet Organised Crime Threat Assessment (IOCTA) 2016" (The Hague, Netherlands, 2016), 17.

23 ENISA, "ENISA Threat Landscape Report 2016 - 15 Top Cyber-Threats and Trends," Report/Study (Heraklion, Greece: European Union Agency For Network and Information Security, January 2017), 21.

over the last year, creating profits of up to $25 million.[24] Malware reports by Verizon[25], Pandalabs[26], and Comodo[27], among others, all recognize the surge of ransomware attacks in 2017, but also indicate that the EU remains relatively unharmed by ransomware when compared to countries like Russia or Iran.

The annual Microsoft Security Intelligence Report provides country specific data about encountered computer security threats. **Figure 3** outlines the malware encounter rate in all 28 EU Member States, including the European and world average. With the exception of Bulgaria and Romania, almost all EU Member States are below the global average. According to the country specific reports by Microsoft, Trojans constitute by far the most encountered malware in these two countries.[28] It is difficult, however, to infer an explanation as to why Romania and Bulgaria stand out. A possible explanation could be the countries' history in cybercrime, which has been frequently investigated by various news reports.[29]

24 Elie Bursztein, Kylie McRoberts, and Luca Invernizzi, "Tracking Desktop Ransomware Payments," accessed September 20, 2017, https://www.blackhat.com/docs/us-17/wednesday/us-17-Invernizzi-Tracking-Ransomware-End-To-End.pdf.

25 Verizon, "2017 Data Breach Investigations Report 10th Edition" (Verizon, 2017), 39.

26 Panda Security, "Pandalabs Quarterly Report Q1 2017," 2017, 14.

27 Comodo Threat Research Labs, "Comodo Threat Research Labs - Q1 2017 Report," Quarterly Report, 2017, 28.

28 Microsoft, "Microsoft Security Intelligence Report Bulgaria," 2017, https://www.microsoft.com/en-us/security/Intelligence-report; Microsoft, "Microsoft Security Intelligence Report Romania," 2017, https://www.microsoft.com/en-us/security/Intelligence-report.

29 Author: Yudhijit Bhattacharjee Yudhijit Bhattacharjee Magazine, "How a Remote Town in Romania Has Become Cybercrime Central," WIRED, January 31, 2011, https://www.wired.com/2011/01/ff_hackerville_romania/; Mirel Bran, "Romania: 'Hackerville', Capital of Global Cybercrime," France 24, December 7, 2012, http://www.france24.com/en/20121207-reporters-romania-hackerville-ramnicu-valcea-cyber-crime-fraud-scams-hackers-internet-police-fbi-cia-bitdefender; Lorenzo Franceschi-Bicchierai, "Inside 'Hackerville,' Romania's Infamous Cyber Crime Hub," Motherboard, June 17, 2015, https://motherboard.vice.com/en_us/article/4x3jnd/inside-hackerville-romanias-infamous-cyber-crime-hub; Jeffrey Roman, "17 Indicted in International ATM Fraud Scheme," March 28, 2014, https://www.bankinfosecurity.com/17-indicted-in-international-atm-fraud-scheme-a-6689; "ProCredit - New Computer Malware Targets Clients of Bulgarian Banks," August 31, 2015, http://www.procreditbank.bg/en/new-computer-malware-targets-clients-of-bulgarian-banks/page/300/item/28323.

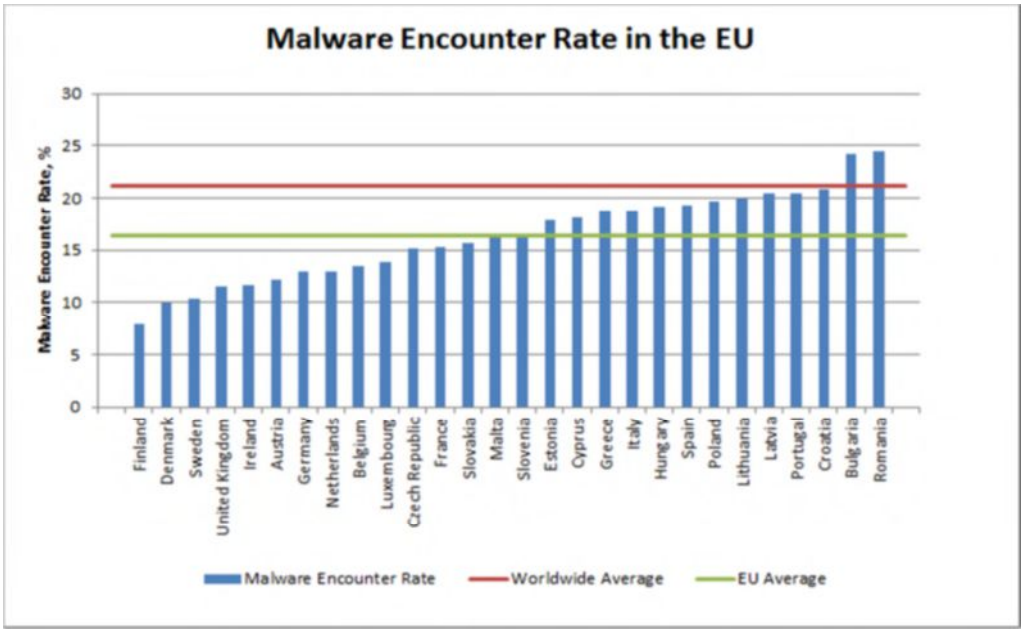


Figure 3: Malware encounter rate in the EU-28[30]

3.1.2 (Distributed) Denial of Service

Over the past few years, DDoS attacks have not only increased in frequency, but also in size and sophistication. A notable example is the DDoS attack on DNS-services by Dyn in October 2016, which temporarily shut down web access to large internet companies such as Facebook, Netflix, Twitter, and Amazon in large regions of the United States and the EU. The attack strength was a record-breaking 1.2 TB/s.[31] This trend will likely continue in the future, potentially disrupting the core of Internet's functions or critical infrastructures.

The rise of Internet of Things (IoT) constitutes an important development with a multiplying effect on the size and impact of DDoS attacks.[32] The exponential growth of poorly protected IoT devices worldwide has opened new avenues for cybercriminals looking to maximize the impact of DDoS campaigns. IoT devices function as proxies (also referred to as 'bots' or 'zombies') that can be compromised and consequently used to flood a designated target with internet traffic. Another recent development is the use of multiple vectors in a single DDoS attack, what increases an overall attack potency. This trend has been observed in nearly 70% of all attacks, what illustrates the increasing sophistication of attacks, as well as the need for more technologically advanced mitigation strategies.[33]

30 Anthe et al., "Microsoft Security Intelligence Report - Volume 21 | January through June, 2016."

31 Nicky Woolf, "DDoS Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say," The Guardian, October 26, 2016, sec. Technology, http://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

32 Nexusguard, "Distributed Denial of Service (DDoS) Threat Report Q1 2017," Threat Report (San Francisco, CA, USA: Nexusguard, 2017), 12.

33 Nexusguard, 8.

Reports further show that DDoS attacks pose a significant fiscal threat to the financial sector, which is facing increasing attack rates.[34] During New Year's Eve of 2014/2015, the Finnish bank OP-Pohjola Group was hit by a DDoS attack that denied customers money withdrawals and other services.[35] In addition, the London-based bank HSBC was hit by a DDoS attack in January 2016, which temporarily disrupted customer banking services.[36] In both cases, there were no direct costs in the form of stolen money or corrupted transactions. However, the attacks caused significant mitigation and investigation costs, not to mention the secondary effects of reputational damage and business disruption.

DDoS attacks may serve several purposes. First, a DDoS attack can be part of a simple extortion campaign carried out by cybercriminals for financial gain. Second, DDoS attacks constitute a service that companies can hire to disrupt online business processes of their competitors. Lastly, DDoS attacks may serve as a 'smoke screen' for other intrusions, such as data theft, malware instalment, and network penetration.[37] [38]

With regard to the impact of DDoS attacks, large organizations are disproportionately targeted, accounting for 98% of all reported cases.[39] DDoS attacks have the biggest impact on those companies that are heavily dependent on their communications infrastructure, or companies that provide critical infrastructure services. Although DDoS attacks are most often associated with large organizations, research shows that 51% of all companies (regardless of their size) have experienced a DDoS attack.[40] However, in contrast to SMEs, large companies often have better mitigation structures and policies in place, making them better prepared and less vulnerable in the event of an attack.

With regard to geographic location, reports by Nexusguard and Kaspersky Labs show a general consensus that servers used for DDoS attacks can be most commonly traced to the Netherlands, Germany, France, UK and Romania.[41] [42] Regarding victims of such attacks, the most targeted

34 VeriSign, "Verisign Distributed Denial of Service Trends Report Volume 4, Issue 1 – 1st Quarter 2017" (VeriSign, Inc., 2017), 9.

35 Aleksi Teivainen, "OP Targeted in a Denial of Service Attack," Helsinki Times, January 2, 2015, http://www.helsinkitimes.fi/finland/finland-news/domestic/13102-op-targeted-in-a-denial-of-service-attack.html.

36 Karl Flinders, "HSBC Online Services Hit by DDoS Attack," ComputerWeekly.com, January 29, 2016, http://www.computerweekly.com/news/4500272109/HSBC-online-services-hit-by-DDoS-attack.

37 Nexusguard, "Hidden Danger Behind DDoS Attacks | Nexusguard," nexusguard.com, accessed October 16, 2017, https://www.nexusguard.com/genius/whitepapers/hiddendangerbehindddosattacks.

38 Warwick Ashford, "DDoS Is Most Common Cyber Attack on Financial Institutions," ComputerWeekly.com, accessed October 16, 2017, http://www.computerweekly.com/news/4500272230/DDoS-is-most-common-cyber-attack-on-financial-institutions.

39 Verizon, "2017 DBIR," 44.

40 Tim Matthews, "The Anatomy of a Distributed Denial-of-Service Attack," Incapsula Blog, January 12, 2016, https://www.incapsula.com/blog/anatomy-of-ddos-attack.html.

41 Nexusguard, "Distributed Denial of Service (DDoS) Threat Report Q1 2017," 9.

42 Alexander Khalimonenko and Oleg Kupreev, "Kaspersky Securelist DDOS Attacks in Q1 2017," www.securelist.com, May 11, 2017, https://securelist.com/ddos-attacks-in-q1-2017/78285/.

countries are the UK, the Netherlands, and Germany.[43] This shows that the threat of a DDoS attack is not dependent on the geographic location, but rather on the general level of development of a country's digital economy. More digitized economies and larger companies tend to be hit more often than SMEs or less digitized economies. Nevertheless, in the absence of adequate response capabilities, a DDoS attack may have more profound consequences on the latter category.

3.1.3 Data breaches

Data breaches involve the loss or compromise of corporate data, which can be both intentional and unintentional. With regard to the former category, cyber criminals are increasingly targeting the application and data layers of companies, which are most vulnerable to attack.[44] The vast majority of data breaches that are caused by hacking attacks involve the use of stolen and/or weak passwords to gain access to information.[45] The main driver for these attacks is identity theft, which accounts for over half of all attacks, followed by financial and account access.[46] Assuming a person's identity or accounts is mostly used for financial gain (almost three quarters of all recorded cases) and, to a lesser extent, espionage.[47]

Although reporting shows that the majority of cyber attacks originate from external sources, the 'insider threat' should not be underestimated. Kaspersky Labs considers careless employees as the 'second biggest cause of security incidents and single biggest cause of data leaks'.[48] According to Verizon, 25% of all data breaches involve internal actors.[49] A Ponemon survey states that about 50% of all data breaches are caused by malicious attacks, but human error and system glitches each account for about 25%.[50] Lastly, a study by Gemalto also indicates that after malicious outsiders, accidental loss and malicious insiders come in second and third, respectively, as frequent sources of data breaches.[51]

For businesses, loss of data constitutes the most expensive consequence of cybercrime, exceeding the costs associated with the disruption of business activities by denial of services, for example.[52] This could be related to the high frequency of malware and attempted phishing attacks that target corporate

43 Imperva Incapsula, "Global DDoS Threat Landscape | Q1 2017 | Incapsula," www.incapsula.com, 2017, https://www.incapsula.com/ddos-report/ddos-report-q1-2017.html.

44 Ponemon Institute, "2016 Cost of Cyber Crime Study & the Risk of Business Innovation," 2.

45 Verizon, "2017 DBIR," 3.

46 Gemalto, "2016 Mining for Database Gold - Findings from the 2016 Breach Level Index" (Gemalto, 2016), 8.

47 Verizon, "2017 DBIR," 3.

48 Kaspersky Lab, "Measuring Financial Impact of IT Security on Business - IT Security Risks Report 2016," 11.

49 Verizon, "2017 DBIR," 3.

50 Ponemon Institute, "2017 Cost of Data Breach Study" (Ponemon Institute, June 19, 2017), 14, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&.

51 Gemalto, "2016 Mining for Database Gold - Findings from the 2016 Breach Level Index," 6.

52 Ponemon Institute, "2016 Cost of Cyber Crime Study & the Risk of Business Innovation," 12.

data and application layers.[53] Nevertheless, the average cost of a data breach is considered to be decreasing, as well as the overall number of data breaches. The average size of a data breach (number of records stolen or lost) has however been on the rise.[54] [55] A speculative explanation for this trend could be related to the centralization of data through cloud computing. Although such outsourcing of data storage to third-party data centres reduces the number of potential entry points, it increases the impact once a breach has been successful.

The above-mentioned trend varies significantly by country and economic sector. **Figure 4** shows the cost of a data breach per country investigated by Ponemon in 2017. This study aims to provide a global analysis and regional trends of such costs by focusing on the selected 11 countries and two regional samples.[56] The EU Member States included in the Ponemon study – namely Germany, France, Italy and the UK – all experienced a decline in the costs compared to a four-year average, whereas many other non-European countries experienced significant increases.

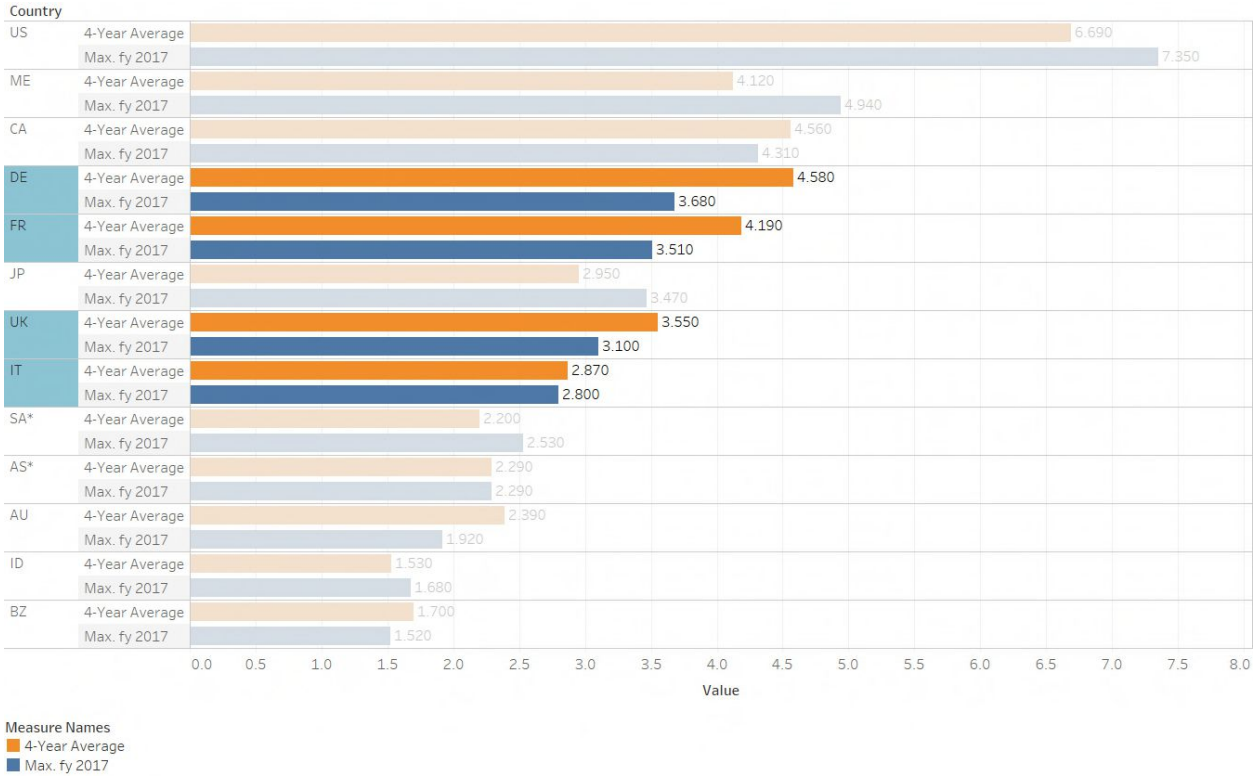


*Figure 4: The average cost of a data breach compared to the four-year average measured in US$ (millions) (*historical data are not available for all years)*[57]

53 Ponemon Institute, 8,14.

54 Ponemon Institute, "2017 Cost of Data Breach Study," 1.

55 Gemalto, "2016 Mining for Database Gold - Findings from the 2016 Breach Level Index," 12.

56 The United States, Germany, Canada, France, the United Kingdom, Italy, Japan, Australia, the Middle East, Brazil, India, South Africa and ASEAN (Association of Southeast Asian Nations).

57 Ponemon Institute, "2017 Cost of Data Breach Study," 10.

As far as economic sectors are concerned, results of the Ponemon survey indicate that some industries are experiencing higher costs than others. **Figure 5** presents an overview of the cost of a data breach by industry in 2017, when compared to a four-year average. As is shown, the healthcare, financial and services sectors recorded the highest costs of a data breach in 2017. While the overall costs of data breaches are on the decline, costs incurred in these sectors have, in fact, increased. The technology and retail sectors equally faced increasing costs.[58]

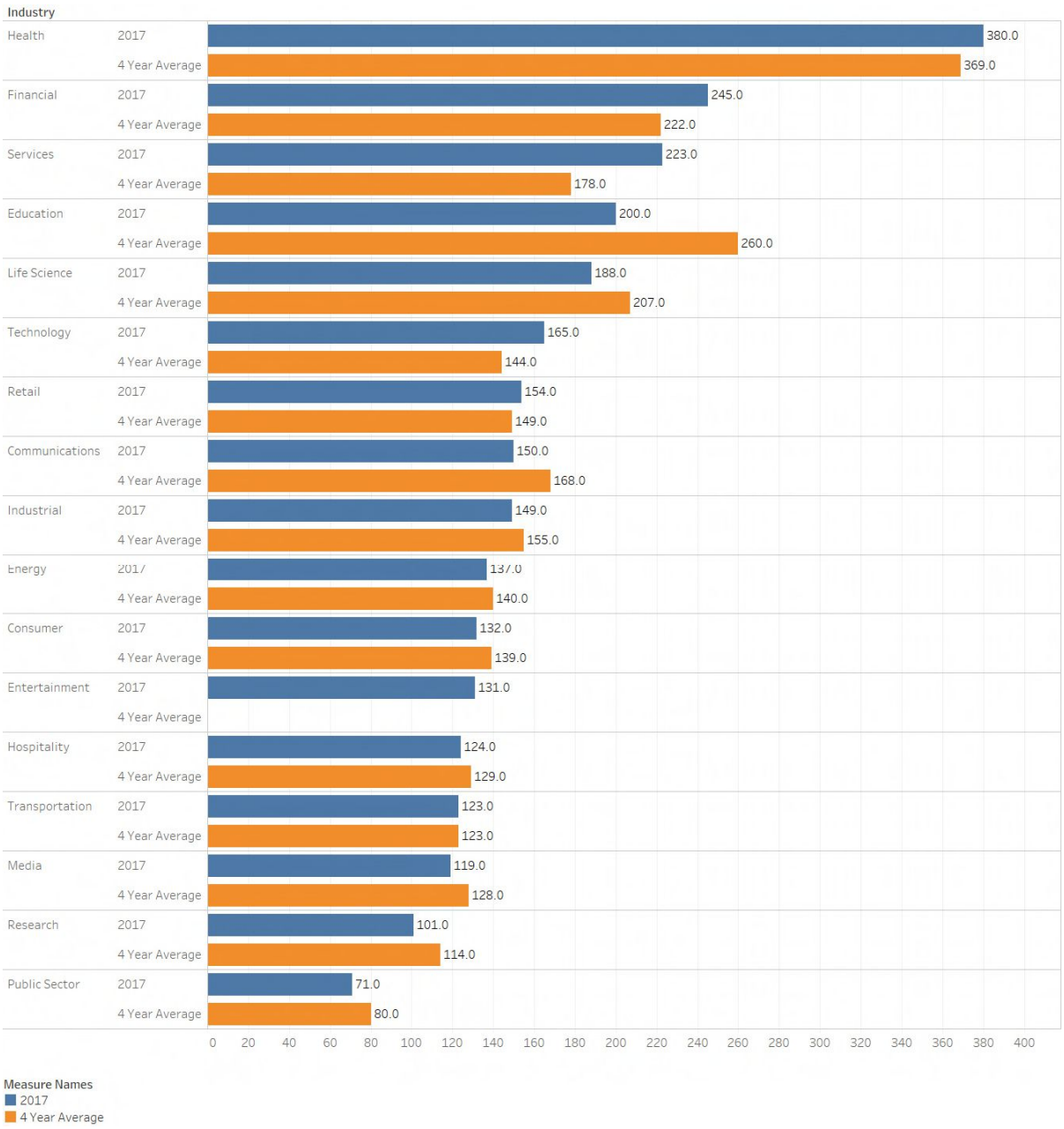


Figure 5: Cost of a data breach by industry in 2017[59]

58 Ponemon Institute, 5,13.

59 Ponemon Institute, "2017 Cost of Data Breach Study."

Not only are the aforementioned sectors – finance, healthcare, services, technology and retail – facing increasing costs, they have also experienced the highest frequency of data breaches. Figure 6 combines data provided by Gemalto, Symantec and Verizon, published in 2017. Although each of the reports provides different figures per individual sector, several sectors rank high in all three reports. Taken together, the aggregate graph shows that finance, healthcare, retail, business services, and information technology can be considered to be most frequently hit by data breaches.

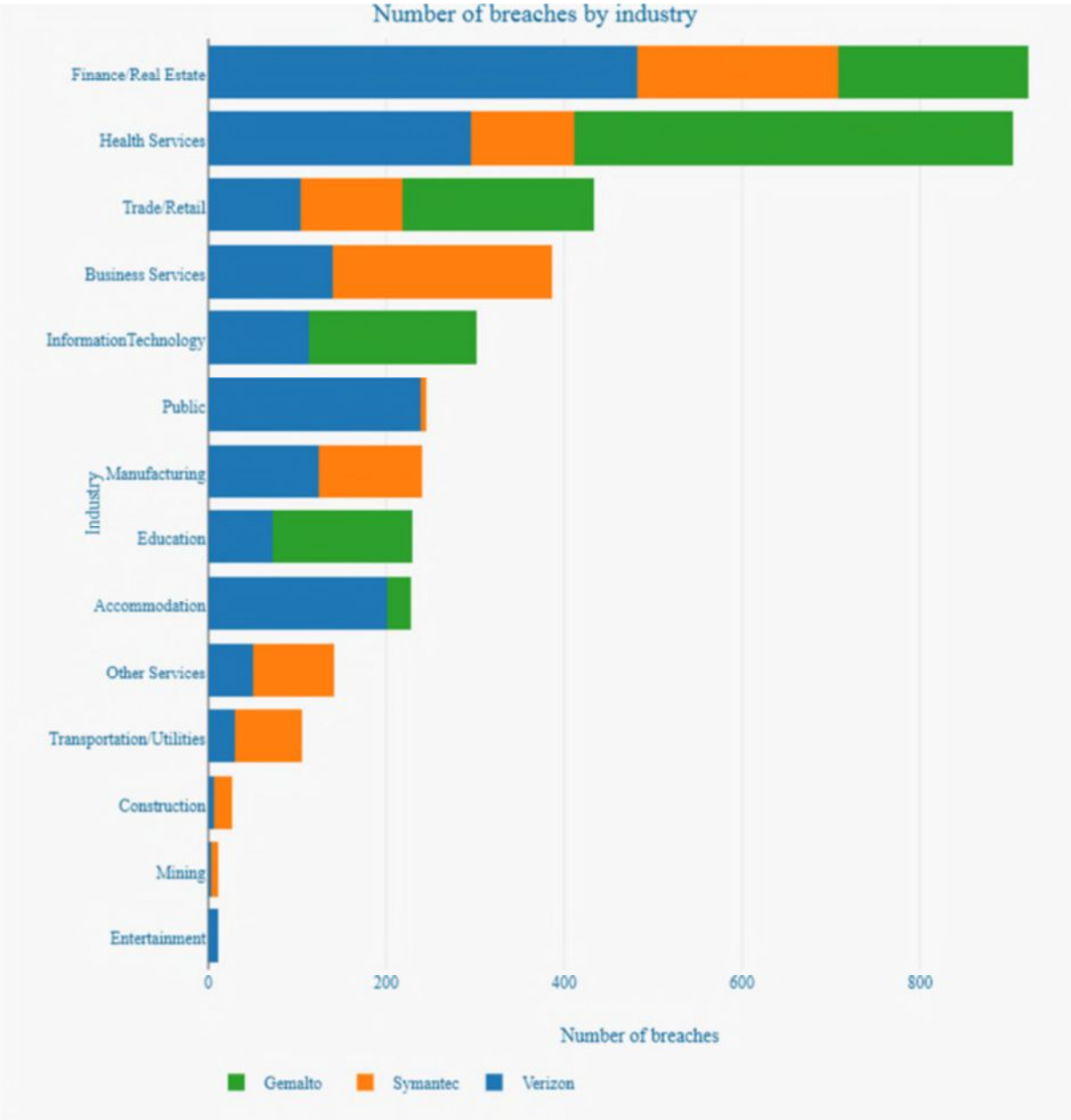


Figure 6: Number of data breaches by industry recorded in 2016 according to Verizon, Symantec and Gemalto

3.1.3.1 The healthcare sector: a sitting duck?

Sensitive personal information – like financial or health records – remains the key focus of cyber attacks. As put forward by PwC, "identity has been at the heart of almost every breach in the past two years".[60] Relative to financial services, energy sector and telecommunications that have long been targeted by cyber attacks and have developed sophisticated defense mechanisms, the healthcare sector lags in terms of its awareness and preparedness for cyber incidents. In the absence of actual penalties for noncompliance, cybersecurity continues to take second place after medical purpose, even though a cyber incident could result in severe injury or death.[61] The exposure of the healthcare sector deserves closer attention.

In recent years, cyber criminals have turned their attention toward the healthcare sector as the target of their illicit activities. According to IBM, the rate of cyber attacks on the healthcare sector climbed to the highest level of all industries studied.[62] According to FireEye, healthcare constitutes a target of as much as 88% of ransomware attacks.[63] Within the first six months of 2017 alone in the United States, a reported 151 healthcare industry breaches have seen more than 1.9 million health records compromised, topped off by the infamous WannaCry ransomware attack that hit UK's National Health Service (NHS) and spilled into other industries.[64] As a direct result of the ransomware, 6,912 appointments – including operations – were cancelled, as many as 19,000 appointments were affected, ambulances and individuals were diverted from emergency departments, and trusts and GPs experienced delays in information, such as test results.[65]

The recent occurrence of cyberattacks is not altogether unsurprising given the trends in the healthcare sector. The push to digitize the sector on the whole, accompanied by the emergence of Electronic Health Records (EHRs) and cross-border eHealth services, have created ample opportunities for criminals to seize upon.[66] While such developments allow easier access to health records for both patients and providers, they centralize personal information and make it a prime target for criminal activity. This situation is compounded with the general lack of awareness, experience and preventative measures in place within the sector. Healthcare organizations, such as hospitals, often lack the infrastructure to identify and track threats as well as the ability to analyze threat data and convert it into actionable information. In addition, the continued use of legacy systems and the lack of access to proper security training indicate that many healthcare organizations have yet to cross the

60 PwC, "The Global State of Information Security® Survey 2017."

61 David Nickelson, "Medical Systems Hacks Are Scary, but Medical Device Hacks Could Be Even Worse," Harvard Business Review, May 15, 2017, https://hbr.org/2017/05/medical-systems-hacks-are-scary-but-medical-device-hacks-could-be-even-worse.

62 Ryan Hewlett, "Cyber Crime against the Healthcare Sector" (Kennedys Insurance, January 2017).

63 "FireEye - Marsh & McLennan Cyber Risk Report 2017 - Cyber Threats: A Perfect Storm About to Hit Europe?" (Milpitas, CA, USA: FireEye, Inc., 2017), 12.

64 Joe Ross, "Cybersecurity Trends: A Look at the First Half of 2017," Huffington Post (blog), July 31, 2017, https://www.huffingtonpost.com/entry/cyber-security-trends-a-look-at-the-first-half-of_us_597f48a2e4b09982b7376650.

65 "NHS Trusts 'at Fault' over Cyber-Attack," BBC News, October 27, 2017, sec. Technology, http://www.bbc.com/news/technology-41753022.

66 RCA security, "Cyber Crime and the Healthcare Industry" (RCA Security, LLC, 2013).

"cybersecurity digital divide".[67] In addition to the lack of time and resources, the rapid spread of the WannaCry malware was blamed on NHS' failure to upgrade old computer systems at a local level, despite previous alerts from NHS Digital, the Department of Health and the Cabinet Office.[68] An assessment of 88 out of 236 trusts by NHS Digital found that none passed the required cyber-security standards before the attack.[69] Apart from operating a vulnerable older software, there was also a lack of planning for such an event. Although the Department of Health had developed a plan, it was not properly communicated or tested in NHS trusts.[70]

In comparison to other industries, healthcare companies tend to hold a vast amount of personal information, from financial to medical.[71] Medical records are increasingly viewed as 'data gold mines'.[72] Their value can be partly attributed to their static nature. In the face of a breach, medical data cannot be cancelled or re-written and the information contained in a medical record has a broad utility, allowing the hacker to commit multiple types of fraud or identity theft.[73] As such, ransomware is viewed as weapon of choice for malicious actors, often forcing hospitals to pay the ransom demanded in order to regain control of stolen data. A strong case showing the debilitating nature of ransomware attacks on the healthcare industry is illustrated in the recent infamous WannaCry attack that impacted the NHS as well as numerous industries in at least 150 countries. In the aftermath of the attack that forced staff to revert to pen and paper, as well as to postpone of multiple surgeries and procedures, it was found that roughly 50 NHS Trusts were impacted. This attack highlighted the lack of accountability and preparedness on the side of healthcare providers, but also the destructive power that a cyber attack can harness.[74] The ransom amounts were relatively small, varying between $300 to $600[75], although the damage and threat of these attacks is best illustrated by the threat to life itself. A paralyzed hospital, or healthcare system, cannot give patients the care they may desperately need, possibly resulting in loss of life.

---

67 Emery Csulak et al., "Report on Improving Cybersecurity in the Health Care Industry" (Health Care Industry Cybersecurity Task Force, June 2017), 14.

68 "NHS Trusts 'at Fault' over Cyber-Attack."

69 "NHS Trusts 'at Fault' over Cyber-Attack."

70 "NHS Trusts 'at Fault' over Cyber-Attack."

71 RCA security, "Cyber Crime and the Healthcare Industry."

72 The value of stolen medical information can vary depending on whether it is being sold individually, as part of a larger package of personal information dubbed 'fullz'# by vendors, and the country of origin of the victim. If sold individually, the value of records of a US citizen can be as low as $1US, with 'fullz' records of US citizens starting at $5US. Very few European records are available on the various dark web online marketplaces, although a report by TrendLabs highlights that UK-based health insurance ID numbers, along with additional information such as full name and address, are being sold for roughly US$3.34 per record. See: Mayra Rosario Fuentes, "Cybercrime and Other Threats Faced by the Healthcare Industry" (TrendLabs, 2017).

73 RCA security, "Cyber Crime and the Healthcare Industry."

74 Chris Graham, "NHS Cyber Attack: Everything You Need to Know about 'biggest Ransomware' Offensive in History," The Telegraph, May 13, 2017, http://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/.

75 Graham.

In addition to the threat to hospitals, the cybersecurity of medical devices is also of great concern for the healthcare sector. The exponential growth in types of medical devices, many of them 'smart devices', augments the risk that they may fall victim to attack, exposing sensitive data and control of the device itself.[76] Research has shown that healthcare cybersecurity continues to focus on the protection of patient health records, whilst ignoring the threat of a compromised medical device that may potentially cause harm to patients themselves.[77] The scope of a cyberattack against the healthcare sector thus widens beyond hospitals, encapsulating related providers and even manufacturers of medical devices.

The trend of cyberattacks levied against the healthcare industry may not subside anytime soon, with some experts believing that ransomware attacks on healthcare organizations will quadruple by 2020 globally.[78] Compounded with the finding that healthcare security executives appear to have less of an understanding regarding cyber threats to their organizations relative to other industries,[79] the vulnerability of healthcare is of great concern for providers, patients, stakeholders and policymakers alike.

3.2 Affected Companies by Size

While all businesses of all sizes are vulnerable to targeted attacks, the past years have witnessed the rise of threat levels for SMEs. According to Symantec, the period 2010-2015 recorded a steady increase in the spear-phishing attacks targeting businesses with less than 250 employees, while share of large and medium sized companies has decreased, globally.[80] This trend is expected to continue in the near future.

The cost of cybercrime also varies by organizational size. Smaller organizations tend to experience a higher proportion of cybercrime costs resulting from web-based attacks, malware, phishing, social engineering attacks and stolen devices. Larger organizations, in contrast, experience a higher proportion of costs relating to malicious insiders, malicious code and denial of services.[81] While big enterprises incur the highest costs in nominal terms, the situation in Germany and the UK shows that the financial impact of cyberattacks is disproportionately high for the smallest enterprises.[82] In the case of Germany, for example, the average cost of a cybersecurity incident for the smallest enterprises is almost half the average for the largest organisations, which are at least ten times larger in size (see

76 Richard Piggin, "Cybersecurity of Medical Devices" (BSI Group, 2017).

77 Piggin.

78 "Healthcare Cybersecurity and Ransomware Report 2017," Cybersecurity Ventures (blog), March 31, 2017, https://cybersecurityventures.com/healthcare-cybersecurity-report-2017/.

79 Cisco, "Healthcare Security: Improving Network Defenses While Serving Patients" (Amsterdam: Cisco, 2016).

80 Symantec, "Attackers Target Both Large and Small Businesses," accessed November 16, 2017, https://www.symantec.com/content/dam/symantec/docs/infographics/istr-attackers-strike-large-business-en.pdf.

81 Ponemon Institute and Accenture, "2017 Cost of Cyber Crime Study & the Risk of Business Innovation," October 2016, 21.

82 Hiscox, "The Hiscox Cyber Readiness Report 2017" (London, United Kingdom: Hiscox Group, 2017), 5.

Table 3). It can be argued that in relative terms, small enterprises are paying the highest price for operating online.

Country	Smaller companies	Larger companies
Germany	54%	65%
UK	48%	59%
US	60%	72%

Table 2: Companies reporting one or more attacks in the last 12 months[83]

Country	99 or fewer employees	250 or fewer employees	250 or more employees	1,000 or more employees
Germany	€21,829	€27,776	€36,837	€45,347
UK	£25,736	£29,127	£53,543	£62,712
US	$35,967	$41,334	$81,322	$102,314

Table 3: Average estimated cost of an organisation's largest cyber incident in last 12 months[84]

3.2.1 Importance of European SMEs

European SMEs play a crucial role in society as well as in the European cybersecurity ecosystem. Digital technologies are appearing and changing at a rapid pace and only agile and flexible enterprises can offer cutting-edge solutions to social issues such as sustainable food and energy provision, sustainable use of raw materials or healthcare.[85] Start-ups and scale-ups deserve special attention. They are a source of innovation within the economy, they create new activity and challenge the established order to modernise.[86] Innovation is a costly endeavor, and intellectual property and patents have high competitive value. Companies cannot reap the benefits of their innovations if such information is stolen. Without adequate security measures in place, R&D investments can be seen as less attractive which can halt the growth and innovation potential of numerous SMEs and start-ups.[87]

83 Hiscox, "The Hiscox Cyber Readiness Report 2017."

84 Hiscox.

85 Netherlands Ministry of Economic Affairs, "Digital Agenda for the Netherlands Innovation, Trust, Acceleration" (The Hague, Netherlands: Netherlands Ministry of Economic Affairs, July 1, 2016), 5, https://www.government.nl/documents/reports/2017/04/11/digital-agenda-for-the-netherlands-innovation-trust-acceleration.

86 Netherlands Ministry of Economic Affairs, 30.

87 Ponemon Institute and Accenture, "2017 Cost of Cyber Crime Study & the Risk of Business Innovation," 15–19.

The above mentioned trends are particularly worrying in light of the fact that SMEs make up 99,8% of European enterprises, yet they are ill-prepared for cyber attacks.[88] Although the average performance in terms of awareness and preparedness is low, SMEs in northern Europe perform marginally better than those in southern Europe.[89] If the actual awareness already exists, the threat posed by cybercrime is often underestimated by SME management. As a consequence, small enterprises lack sufficient IT support to be up to speed on security issues in light of potential cyber threats. Because threat levels have historically been lower for smaller companies, most SMEs show lower than average maturity levels. Large enterprises, in contrast, can easily acquire the knowledge they need, and are thus better prepared and equipped to deal with cyber attacks.[90]

SMEs struggle with cybersecurity not only due to a lack of awareness but also because they perceive cybersecurity as a costly endeavour. Most EU cybersecurity start-ups and SMEs face funding problems in raising the necessary resources to adopt adequate security measures. Lack of funding also prevents them from acquiring external support to help with cyber-related matters.[91] In proportion to their size and income, the investments required to obtain reasonable levels of cybersecurity can be as much as double compared to investments of larger organizations.[92] From an operational point of view, taking advantage of the funding offered at EU level requires the ability to handle the administrative burden related to applying and subsequent reporting.[93] As a result, many small companies are unable to grasp completely the scope and risks of cybercrime, and are only able to protect themselves against truly existential threats by means of relatively basic controls.[94] A combination of valuable information and low security standards – low risk and high pay-off – makes SMEs a vulnerable target for cybercrime and cyber espionage.

Uptake of cyber insurance is also significantly lower in the case of small companies. Although some SMEs consider cyber insurance options, they often regard premiums to be high. In addition, cyber insurance will not cover some of the prevalent risks, such as losing IP or market share. As such, SMEs may consider cybersecurity investments as inefficient – i.e. costing more than reducing risk.[95] The increasing sophistication of attackers will further exacerbate this problem over time.

This uneven distribution of risks makes the digital economy a potentially hostile environment for SMEs, increasing entry costs and creating unfair competition with large and multinational enterprises.

88 “European Cybersecurity Strategy: Fostering the SME Ecosystem” (European Digital SME Alliance, July 31, 2017), 1.

89 Interview with Mr. Fabio Guasconi, Digital SME Alliance, 30 October 2017.

90 Hiscox, “The Hiscox Cyber Readiness Report 2017,” 5.

91 Interview with Mr. Fabio Guasconi, Digital SME Alliance, 30 October 2017.

92 Deloitte, “Dealing Efficiently with Cybercrime - Cyber Value at Risk in The Netherlands 2017,” 17, accessed October 16, 2017.

93 “European Cybersecurity Strategy: Fostering the SME Ecosystem.”

94 Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), “Cybersecuritybeeld Nederland CSBN 2017” (The Hague, Netherlands: Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), June 2017), 70; Deloitte, “Dealing Efficiently with Cybercrime - Cyber Value at Risk in The Netherlands 2017,” 17.

95 Deloitte, “Dealing Efficiently with Cybercrime - Cyber Value at Risk in The Netherlands 2017,” 17.

It is therefore necessary that governmental policies are in place that protect the digital market by stimulating SME cybersecurity, cyber skills and information exchange.

3.3 Economic costs

Whether we are talking about cybercrime, cyber incidents, or cyber breaches, it is a very demanding task to determine their overall impact on the economy. A similar conclusion was drawn by ENISA:

> *"The measurement of the real impact of incidents in terms of the costs needed for full recovery proved to be quite a challenging task. Determining cost values that are as close as possible to reality is a key to determining the real economic impact of incidents on EU's economy. [...] We have also noticed the lack of a unified and standardised approach in developing such studies, often driven by business factors rather than actual interests of stakeholders or realistic needs."*[96]

Many private sector estimates present staggering numbers. A 2015 study by Grant Thornton estimated that cyberattacks caused a $62,3 billion loss of revenues for the private sector in the EU.[97] The 2017 Hiscox Cyber Readiness Report estimated that cybercrime cost the world economy around $450 billion in 2016 alone.[98] According to Juniper Research, cybercrime costs to businesses will reach $2 trillion in 2019.[99] Another report by Cybersecurity Ventures estimates that cybercrime costs will rise from $3 trillion in 2015 to $6 trillion in 2021.[100] Lloyd's has estimated the potential economic impact of a scenario in which a cloud service provider is taken down, leading to a loss of $53 billion – roughly the equivalent of economic damage caused by hurricane Sandy in 2012.[101] The spread of these outcomes underscores the absence of a structured standard to measure such costs. In addition, one has to be wary of the tendency observed in the private sector to inflate cyber threats due to commercial or economic interests. Due to a lack of methodological coherence, agreed definitions and

96 Dan Tofan, Theodoros Nikolakopoulos, and Eleni Darra, "ENISA The Cost of Incidents Affecting CIIs: Systematic Review of Studies Concerning the Economic Impact of Cyber-Security Incidents on Critical Information Infrastructures (CII)" (Heraklion, Greece: European Union Agency For Network and Information Security, August 2016), 5; Tom Spring, "EU Struggles to Determine Growing Cost of Cyberattacks," Threatpost | The first stop for security news, August 12, 2016, https://threatpost.com/eu-struggles-to-determine-growing-cost-of-cyberattacks/119870/.

97 GrantThornton, "Cyber Attacks Cost Global Business over $300bn a Year," Grant Thornton International Ltd. Home, September 22, 2015, https://www.grantthornton.global/en/insights/articles/cyber-attacks-cost-global-business-over-$300bn-a-year/.

98 Luke Graham, "Cybercrime Costs the Global Economy $450 Billion: CEO," www.cnbc.com, February 7, 2017, https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html.

99 Juniper Research Ltd, "Cybercrime Will Cost Businesses Over $2 Trillion by 2019," www.juniperresearch.com, May 12, 2015, https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion.

100 Steve Morgan and Cybersecurity Ventures, "Hackerpocalypse Cybercrime Report," Cybersecurity Ventures (blog), August 12, 2016, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

101 Lloyd's of London, "Extreme Cyber-Attack Could Cost as Much as Superstorm Sandy," www.lloyds.com, July 17, 2017, https://www.lloyds.com/news-and-insight/press-centre/press-releases/2017/07/cyber-attack-report.

indicators to measure the costs, it is hard to present a clear-cut overview of economic costs of cybersecurity incidents across the EU.

The lack of national and EU-specific reports constitutes another issue in assessing the economic cost of cybercrime throughout Europe. Much of the research and reporting is conducted on a global scale. Even if it were possible to draw a general picture of the costs of cybersecurity incidents based on such findings, their applicability in the EU context would remain disputable. The level of ICT development, as well as the frequency of incidents, are likely to vary significantly between Europe and other regions.

In an attempt to estimate the global cost of cybercrime, McAfee and the *Centre for Strategic and International Studies* (CSIS) published a joint report in 2014 which highlighted some of the important difficulties in providing such an estimate.[102] In the first place, the lack of a coherent definition of 'cybercrime' constitutes a problem in that it leads to diverging methodologies across different reports. For example, it leads to ambiguity as to what should be included in cost measurements. Although not all cyber incidents are caused by criminal or malicious intent, they can all inflict significant harm to a company. Moreover, it is also unclear whether only direct costs – emergency response, data loss, containment etc. – should be included, or if indirect costs, such as reputational damage, should be covered as well.

3.3.1 Cost categorization

To measure the cost of cybercrime systematically, Anderson et al. distinguish between four types of costs related to cybercrime: criminal revenue, direct losses, indirect losses and protection (or defense-related) expenses.[103] *Direct losses* are defined as "the monetary equivalent of losses, damage, or other suffering felt by the victim as a consequence of a cybercrime".[104] These include, inter alia, financial losses due to money extracted from victims, costs of direct response and recovery, and denial of access with the potential to disrupt business processes. *Direct losses* are generally small, almost minimal, and do not cause severe harm to the victims of cybercrime. *Indirect losses* are defined as "the monetary equivalent of the losses and opportunity costs imposed on society by the fact that a certain cybercrime is carried out".[105] These include factors such as confidence loss in cyber transactions by individuals and corporations, reputational damage suffered by corporations and the expansion of the underground economy. *Defence costs* refer to "the monetary equivalent of prevention efforts",[106] and include both direct and indirect defence costs, as well as opportunity costs

102 McAfee and Center for Strategic and International Studies, "Net Losses: Estimating the Global Cost of Cybercrime Economic Impact of Cybercrime II" (Santa Clara, CA, USA: McAfee & Center for Strategic and International Studies, June 2014), 4.

103 Ross Anderson et al., "Measuring the Cost of Cybercrime" (11th Workshop on the Economics of Information Security, Berlin, Germany, June 26, 2012), http://www.econinfosec.org/archive/weis2012/presentation/Moore_presentation_WEIS2012.pdf.

104 Anderson et al., 5.

105 Anderson et al., 5.

106 Anderson et al., 6.

caused by the prevention measures.[107] In comparative terms, indirect losses tend to be much larger than direct costs and expenses for protection measures.

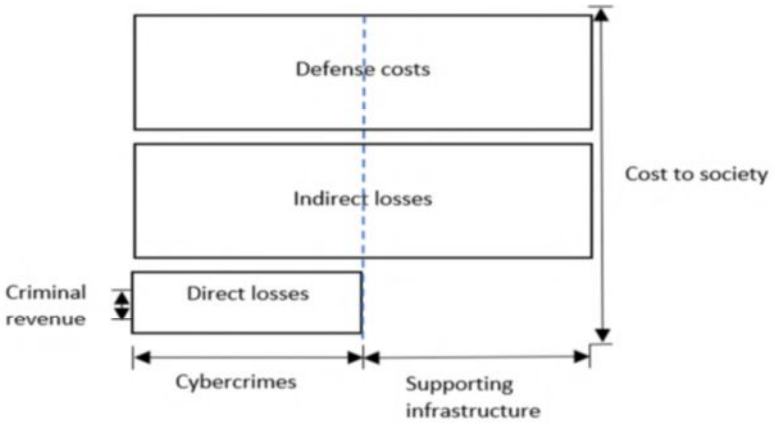


Figure 7: Framework for analysing the cost of cybercrime (Anderson et al.)

A similar categorization, distinguishing between direct, indirect and opportunity costs, is suggested by Ponemon Institute and Accenture. *Direct costs* refer to amounts directly spent to accomplish a given activity. *Indirect costs* refer to non-cash expenses such as the amount of effort, time, and other organizational resources spent. *Opportunity costs* result from lost business opportunities as a consequence of reputation loss following the incident.[108] Ponemon Institute and Accenture make an additional distinction between *internal costs*, which pertain to dealing with the cybercrime, and *external costs*, which relate to the consequences of a cyber attack.[109] As **Figure 8** demonstrates, internal costs start with the detection of the incident and end with the final or ex-post response to the incident, which involves dealing with business disruption and lost business opportunities. External costs include the loss of information assets, business disruption, equipment damage and revenue loss.

107 Igor Bernik, "Cybercrime: The Cost of Investments into Protection," Journal of Criminal Justice and Security, no. 2 (n.d.): 105–16.

108 Ponemon Institute and Accenture, "2017 Cost of Cyber Crime Study & the Risk of Business Innovation," 46.

109 Ponemon Institute and Accenture, 45.

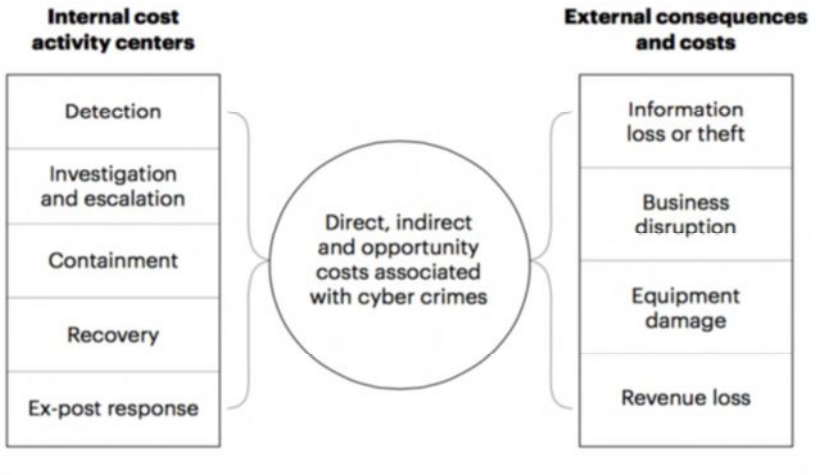


Figure 8: Ponemon Institute and Accenture cost framework for cybercrime.[110]

Because of its conceptual applicability, this study relies on the framework provided by Anderson et al. Not all cash expenses are direct costs per se (i.e. preparation costs); cyber attacks may inflict direct non-monetary costs such as business disruption. Although the distinction provided by Ponemon and Accenture between direct, indirect and opportunity costs is not adopted in this study, there is a synergy between the two. Both internal and external costs and the subsequent categories presented by Ponemon and Accenture would fall within Anderson et al.'s definition of direct costs, or 'a consequence of cybercrime'.

3.3.2 Direct costs

Direct costs of cybercrime may be considered at multiple levels. At the end-user level, a survey across six European Member States – namely Germany, Estonia, Italy, the Netherlands, Poland and the United Kingdom – estimated the direct costs of cybercrime per individual over a time period of five years to fall between €14,17 and €49,88 – a significant part of which comes from the monetary value of the time lost recovering from a cyber incident.[111] A recent Eurobarometer survey has shown that only a minority of respondents from across the EU have had an actual experience dealing with cybercrime.[112]

In contrast to the end-user level, encounters with cybercrime are considered to be the norm at the industry level. The 2016 Ponemon Cost of Cybercrime Report found that 99% of respondents from businesses worldwide have encountered malware or other sorts of cybercrime.[113] Moreover, in 2017, Ponemon and Accenture found that the most significant external cost of a cyber attack is information

110 Ponemon Institute and Accenture, 46.

111 Riek Markus et al., "Estimating the Costs of Consumer-Facing Cybercrime: A Tailored Instrument and Representative Data for Six EU Countries." (TU Delft, 2016), 24.

112 European Commission, "European Attitudes Toward Cybersecurity," 2017, 66, http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/79734.

113 Ponemon Institute, "2016 Cost of Cyber Crime Study & the Risk of Business Innovation," 8.

loss (43%), followed by business disruption (33%), revenue loss (21%), and equipment damages (3%).[114] Regarding internal costs, most resources are allocated towards threat detection (35%), threat containment (21%), and data recovery (20%), followed by investigation (11%), incident management (8%), and ex-post response (5%).[115]

Although there is a scarcity of EU-wide reports on the direct costs of cybercrime, several country-level estimates provide a useful indication in this regard. In the UK, total annual costs of cybercrime suffered by UK companies are estimated to equal £29.1 billion (€33.2 billion)[116] – about 1.1% of the country's GDP in 2016.[117] The German Federal Crime Office has estimated the total cost of cybercrime to its economy in 2016 at €22.4 billion[118], which constituted 0.76% of GDP.[119] In the Netherlands, a study by Deloitte estimated the total annual costs of cybercrime to the Dutch economy stands at €10 billion (equalling 1,5% of GDP). However, 75% of the costs represented a 'loss of opportunity', making the actual direct losses a quarter of the overall sum, or €2.5 billion[120] (0.32% of GDP).[121]

The numbers presented above are primarily based on private sector reporting and only cover north-western Europe. Neutral reporting on direct costs with a wider geographical focus in Europe is currently absent.

3.3.3 Indirect costs

Anderson et al. estimate indirect losses to be much larger than direct costs and expenses for protection measures, but remark that they are very difficult to quantify.[122] Trust is a key component of the digital economy and perceptions of risk have a negative effect on technology acceptance and use of online services.[123] According to McAfee, the cost of reputational damage caused by cyber attacks has been

114 Ponemon Institute and Accenture, "2017 Cost of Cyber Crime Study & the Risk of Business Innovation."

115 Ponemon Institute, "2017 Cost of Cyber Crime Study & the Risk of Business Innovation," 13.

116 Deloitte, "Dealing Efficiently with Cybercrime - Cyber Value at Risk in The Netherlands 2017," 11.

117 "United Kingdom (UK) GDP - Gross Domestic Product 2016," countryeconomy.com, accessed November 14, 2017, https://countryeconomy.com/gdp/uk?year=2016.

118 Andrea Shalal, "Germany Sees Rise in Cybercrime, but Reporting Rates Still Low," Reuters, May 3, 2017, https://www.reuters.com/article/us-germany-cybercrime-crime/germany-sees-rise-in-cybercrime-but-reporting-rates-still-low-idUSKBN17Z26S.

119 World Bank, "GDP (Current US$), Germany | Data," accessed November 14, 2017, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=DE.

120 Deloitte, "Dealing Efficiently with Cybercrime - Cyber Value at Risk in The Netherlands 2017," 11.

121 World Bank, "Netherlands | Data," accessed November 14, 2017, https://data.worldbank.org/country/netherlands.

122 Anderson et al., "Measuring the Cost of Cybercrime," 8.

123 Markus Riek, Rainer Bohme, and Tyler Moore, "Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance," 2015; United Nations Interregional Crime and Justice Research Institute (UNICRI), "Cybercrime: Risks for the Economy and Enterprises at the EU and Italian Level," 2014, 54.

increasing.[124] Kaspersky Lab estimates that reputational damage to a company can be as much as 7.5 times higher than the associated direct costs of a cyber attack.[125] A Eurobarometer survey has found that two-thirds of respondents from across the EU are concerned about falling victim to bank card or online banking fraud.[126] However, estimating the indirect economic impact on the basis of public opinion surveys has proven difficult. There is a lack of up-to-date and reliable estimates at the European level and beyond. Non-partisan research into this topic is needed.

3.3.4 Defense costs

Defense costs at the end-user level are estimated to total between €41.93 and €331.91 per individual over a time period of five years.[127] The wide spread of the estimate highlights the unevenness of cybersecurity spending across the EU, with users in Estonia (€41.93) and Poland (€96.58) spending disproportionately less than those in the Netherlands (€263.86) and Germany (€331.91).[128]

At the industry level, it is estimated that businesses cross Western European spent $19.5bn on cybersecurity tools and services in 2016, with the banking industry leading as the largest spender.[129] Breaking down the allocation of funds within corporate security budgets according to six IT security layers, a study conducted by the Ponemon Institute in 2016 found that spending is unevenly allocated and predominantly focused on the network (29%), application (21%) and data (21%) layers, with the human (12%), physical (10%) and host layers (7%) lagging behind.[130] On the whole, the value of the European cybersecurity market was estimated at $22bn in 2016 and is expected to grow 8% p.a. due to increasing spending on services.[131]

With regard to the public sector, HCSS in-house research found that many countries do not openly share (parts of) their cybersecurity budgets, which makes it difficult to provide a complete overview of the allocation of public funds. Where data was available, we found that only a small portion of the

124 McAfee and Center for Strategic and International Studies, "Net Losses: Estimating the Global Cost of Cybercrime Economic Impact of Cybercrime II," 17.

125 Kaspersky Lab, "A True Cost of Cyberattacks," February 16, 2016, https://www.kaspersky.com/blog/cost-cyberattack-enterprise/5195/.

126 European Commission, "European Attitudes Toward Cybersecurity," 64.

127 Markus et al., "Estimating the Costs of Consumer-Facing Cybercrime: A Tailored Instrument and Representative Data for Six EU Countries.," 24.

128 Markus et al., "Estimating the Costs of Consumer-Facing Cybercrime: A Tailored Instrument and Representative Data for Six EU Countries."

129 IDC, "Worldwide Revenue for Security Technology Forecast to Surpass $100 Billion in 2020, According to the New IDC Worldwide Semiannual Security Spending Guide," www.idc.com, October 12, 2016, http://www.idc.com/getdoc.jsp?containerId=prUS41851116; Jonathan Vanian, "Here's How Much Businesses Worldwide Will Spend on Cybersecurity by 2020," Fortune, October 12, 2016, http://fortune.com/2016/10/12/cybersecurity-global-spending/.

130 Ponemon Institute, "2016 Cost of Cyber Crime Study & the Risk of Business Innovation," 14.

131 PwC, "Cybersecurity: European Emerging Market Leaders" (PwC UK, January 2017), 4.

overall GDP is generally dedicated to cybersecurity spending.[132] Nevertheless, some EU Member States have been boosting their cyber defence spending. The UK is set to invest a total of £1.9 billion over the next five years on cybersecurity, while the German Military launched a new Cyber and Information Space Command in April 2017.[133] On the whole, costs associated with cyber defense are rising in both the public and private sector, while data about the extent to which the end-users are affected by these changes remain insufficient.

132 Michel Rademaker et al., "Dutch Investments in ICT and Cybersecurity - Putting It in Perspective," Security (The Hague, Netherlands: The Hague Centre for Strategic Studies, March 8, 2017), 21.

133 HM Government, "National Cybersecurity Strategy 2016-2021," 10, accessed November 14, 2017; Nina Werkhauser, "German Army Launches New Cyber Command | Germany | DW | 01.04.2017," DW.COM, April 1, 2017http://www.dw.com/en/german-army-launches-new-cyber-command/a-38246517.

4. The state of awareness and resilience across Europe

The second part of the findings section offers an overview of the current state of cyber resilience at the European, national and corporate level. It first provides an overall assessment of digitization of economy and society across Europe and then looks at different indicators of cyber awareness. These include existing security measures against cybercrime, national cyber strategies and policies, cybersecurity education offered across Europe, the level of public investment in cybersecurity in comparison to the level of digitization, as well as the availability of the right skills and workforce capable of supporting an organization's cybersecurity needs.

4.1 Digitization of businesses across Europe

The level of digitization of the private sector is uneven across the EU, creating a disparate architecture where varying levels of digital development cause incompatibility of policies and business practices. Several studies have been conducted, two of which are used in this study to illustrate different levels of business digitization across the EU.

The 2015 *World Economic Forum Executive Opinion Survey* ranks countries based on their level of competitiveness on a scale of 1-7. Three indicators are used in the *Networked Readiness Index* that are also useful in this context: firm-level technology absorption, business-to-business ICT usage, and business-to-consumer ICT usage. Executives were asked to what extent businesses in their country used the latest technologies, to what extent businesses used ICTs for transactions with other businesses, and to what extent businesses used the Internet to sell goods and services to consumers. **Figure 9** provides an overview of the EU-28 ranked according to the aforementioned indicators. The graph indicates a geographic trend: businesses in the North-Western Europe tend to score highest, while those from Southern and Eastern European countries generally lag behind.

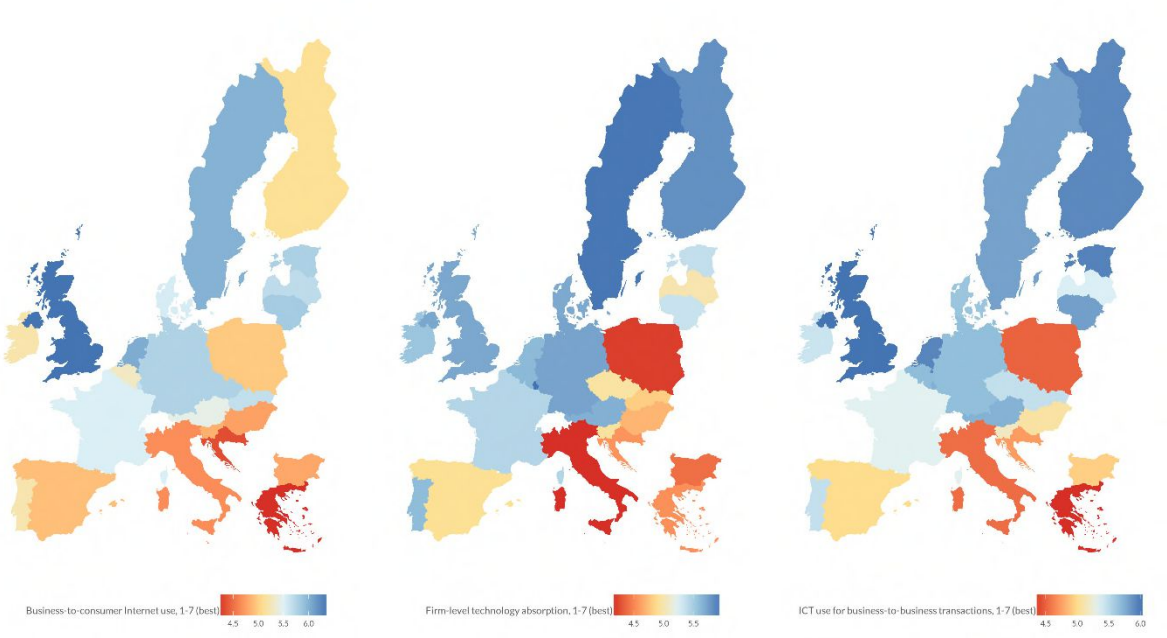


Figure 9: Business Usage of ICT (Measures: Business-to-consumer internet use; Firm-level technology absorbs ion; ICT use for business to business transactions) [134]

The European Commission developed the Digital Economy and Society Index (DESI), which assesses digital maturity of EU Member States in areas such as public policy, connectivity, digital skills and education. One dimension of DESI focuses on the level of integration of digital technology in the private sector (see **Figure 10**). This dimension consists of two elements, namely digitization of business processes and eCommerce. Although some distinctions are evident when DESI rankings are compared with the WEF ones (see Figure 9) – namely the level of digitization in Ireland and the United Kingdom – DESI nevertheless presents a similar trend, where North-Western Europe leads in terms of digital maturity and integration of digital technology in the private sector.

134 World Economic Forum, "Networked Readiness Index," Global Information Technology Report 2016, 2016, http://wef.ch/29cCKbU.

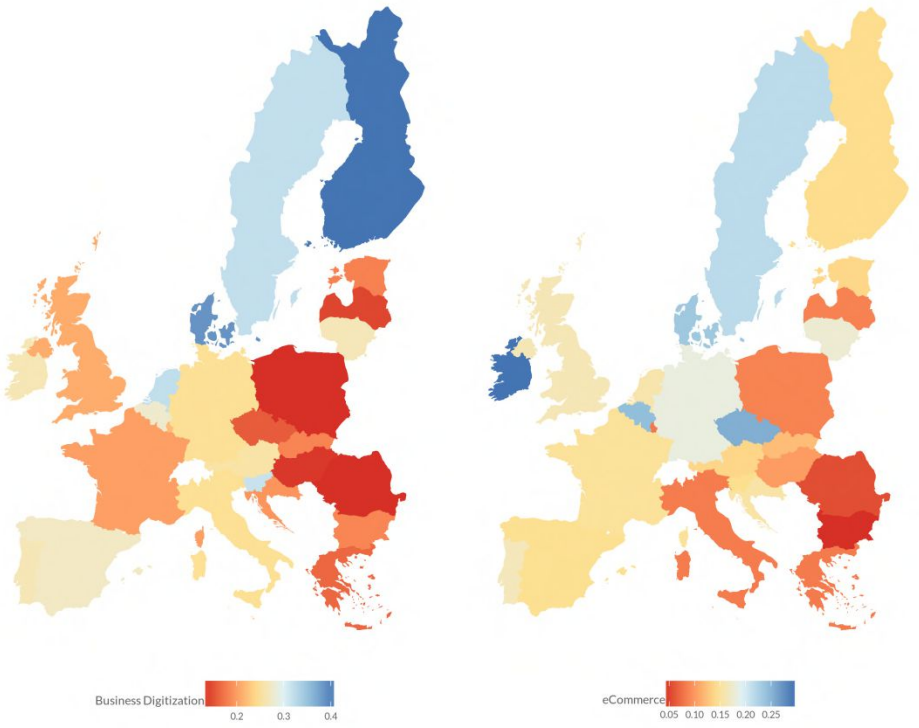


Figure 10: Integration of Digital Technology (Measures: Business digitization; eCommerce)[135]

4.2 Current state of cyber resilience at the national level

4.2.1 Cybersecurity in the EU policy context

Within cyberspace, governments can provide a secure business climate by safeguarding a high-quality and secure digital infrastructure and by ensuring privacy protection of citizens and businesses alike. In the EU context, cybersecurity policy constitutes a 'shared area of competence' between Member States and the EU,[136] which implies that when the EU decides to regulate, EU law takes primacy over any adopted national law. As such, a significant proportion of digital legislation and policies related to cybersecurity originate at the EU level.[137]

135 European Commission, "Digital Economy and Society Index — Digital Scoreboard - Data & Indicators," Digital Single Market - Digital Economy & Society, 2017, http://digital-agenda-data.eu/charts/desi-components#chart={"indicator":"DESI_4_IDT","breakdown-group":"DESI_4_IDT","unit-measure":"pc_DESI_4_IDT","time-period":"2017"}.

136 The New Europe of Security, June 2017, https://www.swp-berlin.org/fileadmin/contents/products/comments/2017C20_bdk.pdf

137 Netherlands Ministry of Economic Affairs, "Digital Agenda for the Netherlands Innovation, Trust, Acceleration," 9.

On the whole, key European strategies and legislation have – up until now – primarily tackled the protection of personal data, security of operation of large scale and publically accessible information networks, and protection of operation of key infrastructures (of vital importance). The importance of cybersecurity in industrial settings has only been recognized marginally, and deserves increased attention.[138]

With the aim to better protect Europeans online, in 2013 the European Commission launched the **EU Cybersecurity Strategy**, which currently defines cybersecurity policy framework within the EU. The strategy sets forth five key priorities, namely to 1) increase cyber resilience; 2) drastically reduce cybercrime; 3) develop EU cyber defence policy and capabilities; 4) develop the industrial and technological resources for cybersecurity; 5) establish an international cyberspace policy for the EU and promote core EU values.[139] The cybersecurity strategy was complemented by the **European Agenda on Security** 2015-2020, which set the fight against cybercrime as one of its three priorities.

The 2015 **Digital Single Market Strategy** constitutes another important initiative in this regard. It aims to reinforce cooperation across borders, and between all sectors and actors active in cybersecurity, as well as to help develop innovative and secure technologies, products and services throughout the EU. As part of this strategy, the first European public-private partnership on cybersecurity was launched between the Commission and the European Cybersecurity Organization (ECSO) – an industry-led association, which comprises over 200 stakeholders, including SMEs and start-ups, large cybersecurity companies, universities, research centers, end-users, operators, clusters and associations as well as public authorities.[140] The goal of this partnership is to help overcome fragmentation of the European cybersecurity market by means of innovation, trust building between Member States and industrial actors, and the alignment of the demand and supply for cybersecurity products and solutions. Under its research and innovation program Horizon 2020, the EU committed to invest up to €450 million in the partnership until it expires in 2020. Cybersecurity market players, represented by ECSO, are expected to invest three times that amount.[141]

Cyber attacks know no borders, which is why improved standardisation and related certification play an important role in guaranteeing the cybersecurity of both networks and devices. The Communication on **ICT standardisation** for the Digital Single Market constitutes an important milestone with regards to cybersecurity in industrial settings.[142] It aims to set ICT standards in five

138 "Digitizing Industry (4.0) and Cybersecurity" (European Parliament, November 2017).

139 European Commission, "EU Cybersecurity Initiatives - Working towards a More Secure Online Environment," January 2017, 2, http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf.

140 European Commission, 3.

141 European Commission, "COMMISSION STAFF WORKING DOCUMENT ASSESSMENT OF THE EU 2013 CYBERSECURITY STRATEGY," September 13, 2017, 17, http://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF.

142 European Commission, "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: ICT Standardisation Priorities for the Digital Single Market," April 19, 2016.

priority areas – namely 5G communications, IoT, cybersecurity, cloud computing, and big data technologies – which are deemed essential to the Digital Single Market. Areas such as eHealth, smart energy, intelligent transport systems and connected and automated vehicles (including trains, advanced manufacturing, smart homes and cities, and smart farming) are all expected to benefit considerably from the proposed prioritization of standards.[143]

Delivering on the above-listed strategies, in July 2016 the Commission put forward a Communication on strengthening Europe's cyber resilience systems and fostering a competitive and innovative cybersecurity industry, which announced the launch of a public-private partnership on cybersecurity and additional market-oriented policy measures to boost industrial capabilities in Europe.[144]

The European Directive on Security of Network and Information Systems (the **NIS Directive**), adopted by the European Parliament in July 2016, constitutes the first EU-wide legislation on cybersecurity that provides legal measures to boost the overall level of cybersecurity across the EU.[145] These legal measures aim to reinforce trust and confidence among Member States, and ensure an efficient cross-border cooperation and information exchange.[146] When the Directive comes into full effect in 2018, it will place further demands on both governments and selected businesses to raise the baseline of their cybersecurity capabilities. Among other provisions, it will require all Member States to have a cybersecurity strategy, a national competent authority, and national cybersecurity incident response teams in place.[147] With regards to its impact on the private sector, the NIS Directive will require those companies that have been identified by Member States as 'operators of essential services' (namely energy, transport, banking, financial market infrastructures, healthcare, water and digital infrastructure) to take appropriate security measures and notify serious security incidents to the relevant national authority. Key Digital Service Providers (namely online search engines, cloud computing services and online marketplaces) will also have to comply with the security and notification requirements.[148] As such, the implementation of the NIS Directive is expected to lead to an overall increase in cybersecurity across those sectors that are considered vital for the economy and

143 European Commission.

144 European Commission, "COMMUNICATION FROM THE COMMISSION - Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry," July 5, 2016, https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-410-EN-F1-1.PDF.

145 "Global Cybersecurity Index 2017: Europe" (International Telecommunication Union (ITU), 2017), 5, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/EUR_GCIv2_report.pdf.

146 European Political Strategy Centre, European Commission, "Building an Effective European Cyber Shield," ec.europa.eu, May 8, 2017, 6, /epsc/publications/strategic-notes/building-effective-european-cyber-shield_en.

147 "FireEye - Marsh & McLennan Cyber Risk Report 2017 - Cyber Threats: A Perfect Storm About to Hit Europe?," 17.

148 European Commission, "COMMISSION STAFF WORKING DOCUMENT ASSESSMENT OF THE EU 2013 CYBERSECURITY STRATEGY."

European Parliament and Council of the European Union, "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," July 19, 2016, 27, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN.

the society. At the same time, the flexible implementation allowed for by the Directive – i.e. the fact that each Member State is responsible for identifying the sectors it deems essential – may lead to inconsistencies across the EU, as well as possible misallocation of resources.[149]

In addition, a new data-protection regulation has been agreed that will further harmonise data privacy legislation across Europe. While the NIS Directive imposes notification requirements around security incidents, the General Data Protection Regulation (GDPR) focuses on personal data breaches. When the GDPR takes full effect in 2018, companies will be required to report incidents involving the loss of personal data to national data protection authorities and – where the threat of harm is substantial – to affected individuals.[150] Non-compliance with the GDPR's requirements will result in fines as high as 4% of global revenues for the preceding fiscal year.

The proposal for a revised **ePrivacy Regulation** is intended to complement the GDPR. Whereas the GDPR focuses on the general protection of personal data (in paper-based as well as electronic form), the ePrivacy regulation is intended to protect a person's right to a private life, including confidentiality, and focuses on data processed by means of electronic communications. Fines for violations will be as high as under the GDPR, and can go up to €20 million.[151] On the one hand, critics contend that complying with both the GDPR and the ePrivacy regulation will be difficult and costly. On the other hand, one set of rules for all companies processing data in the EU – wherever they are based – will create a level playing field, increase consumer confidence, and improve the business climate in the long run.[152]

In line with the EU's efforts to ensure a high level of data protection for its citizens, in 2016 the European Court of Justice (ECJ) set a new precedent for EU Member States on any **data retention procedures**, stating that access to such data must be restricted to the purpose of preventing and detecting serious crime. This invalidated the 2006 Data Retention Directive, which required providers of publicly available telecommunication services to store the communications data of EU citizens for up to two years.[153] Another landmark ruling worth mentioning is the so-called **'right to be forgotten'**, which requires search engines that gather personal information for profit (such as Google, for example) to remove links to private information upon demand, provided the information is no longer

149 Danielle Kriz, "Passage of EU NIS Directive Is a Milestone, but next Steps Matter Even More," Palo Alto Networks (blog), July 6, 2016.

150 "FireEye - Marsh & McLennan Cyber Risk Report 2017 - Cyber Threats: A Perfect Storm About to Hit Europe?," 15.

151 Julia Apostle, "The Uber Data Breach Has Implications for Us All," Financial Times (FT), November 27, 2017, https://www.ft.com/content/e2bf6caa-d2cb-11e7-a303-9060cb1e5f44;

"Data Protection - Better Rules for Small Businesses," European Commission, n.d., http://ec.europa.eu/justice/smedataprotect/index_en.htm.

152 "Data Protection - Better Rules for Small Businesses."

153 Tzanou, Maria. The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance. London: Bloomsbury Publishing Plc, n.d.

relevant.[154] The ECJ also played a role in the suspension of the EU-US Safe Harbour Agreement, which concerned **personal data transfers outside the EU**.[155]

Cybersecurity is addressed by several EU networks/organizations. Notable institutions that take part in the overall provision of cybersecurity include the EU Network and Information Security Agency (ENISA), Europol's European Cyber Crime Centre (EC3), EU Computer Emergency Response Team (CERT-EU), the EU Hybrid Fusion cell within the EU Intelligence and Situation Centre (EU INTCEN), the European External Action Service (EEAS), the European Defence Agency (EDA), and Eurojust. It is worth mentioning that the European Commission, in cooperation with the EEAS, ENISA, and Member States is looking into developing a platform for education and training in the area of cybersecurity to provide the necessary tools in order to prevent or deal with cybersecurity incidents.[156] The platform is expected to be put in place by 2018.

In September 2017, the European Commission adopted a **new cybersecurity regulatory package**. This reform aims to build on the measures put in place by the cybersecurity strategy, and its main pillar, the NIS Directive. The proposal sets out a wide range of concrete measures, such as building a stronger EU Cybersecurity Agency on the structures of the existing European Union Agency for Network and Information Security (ENISA). The new agency's role would be to help Member States, EU institutions and businesses alike deal with cyber attacks.[157] The Agency would be entrusted to support businesses in key areas including the implementation of the NIS Directive and the cybersecurity certification framework.[158]

Another measure proposed in the package is the creation of an **EU-wide cybersecurity certification scheme** for ICT products, services and processes. This initiative is intended to increase the security of digital products and services, improve cross-border trade, and reduce market fragmentation within the EU. This framework would apply to critical and high-risk applications in essential services (and specific sectors), such as healthcare, transport, energy, banking, financial market infrastructure, drinking water or digital infrastructure.[159] A joint Commission-industry initiative will also be launched to define a 'duty of care' principle for reducing software and product vulnerabilities, and to promote a 'security by design' approach for producers of connected devices.[160] Although the design of

154 Maria Tzanou, The Fundamental Right to Data Protection: Normative Value in the Context of Counter- Terrorism Surveillance (London: Bloomsbury Publishing Plc, n.d.), 60.

155 Shara Monteleone and Laura Puccio, "From Safe Harbour to Privacy Shield: Advances and Shortcomings of the New EU-US Data Transfer Rules" (European Parliamentary Research Service (EPRS), January 2017).

156 European Commission, "COMMUNICATION FROM THE COMMISSION - Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry."

157 "Reform of Cybersecurity in Europe," General Secretariat of the Council of the European Union, August 1, 2018, http://www.consilium.europa.eu/en/policies/cyber-security.

158 "Digitizing Industry (4.0) and Cybersecurity," 9.

159 "Reform of Cybersecurity in Europe." General Secretariat of the Council of the European Union, August 1, 2018. http://www.consilium.europa.eu/en/policies/cyber-security.

160 "Reform of Cybersecurity in Europe."

ICT products that incorporate security principles from the very beginning would contribute to a much higher resilience of a digitized industry, the *voluntary* nature of the envisaged certification puts a question mark on the extent to which certification will support the needs of Europe's industry.[161]

The package also revises the implementation of the aforementioned NIS Directive. Although it continues to apply to large-scale cybersecurity incidents affecting Member States and key strategic sectors, the target sectors have now been broadened to include public administration, the postal sector, food sector, chemical and nuclear industry, environmental sector, and civil protection, should Member States wish to include them.[162]

Additional initiatives proposed by the European Commission include a **Blueprint** on how to respond to large-scale cyber attacks, the establishment of a **European Cybersecurity Research and Competence Centre** joined by a network of similar centres at member state level, a more effective criminal law response to cybercrime through a new directive to fight fraud and counterfeiting of non-cash payments, and the **enhancement of international cooperation**.[163] Under the aforementioned Blueprint, the EU will have a well-rehearsed plan in place in the event of a large-scale cross-border cyber incident or a crisis which requires swift communication and coordination between the Member States and EU institutions.[164]

Even though the new cybersecurity package constitutes a positive development towards the creation of a unified strategy against cyber-related threats, it does not fully eliminate fragmentation between individual Member States. Internal divisions with regards to cybersecurity amongst Member States continue to pose a limitation on the Strategy's effectiveness. For example, it remains unclear whether the new strategy will actually result in enhanced information sharing between individual Member States. Sharing of cybersecurity information remains a sensitive issue, given the existence of considerable constraints to the free flow of data and the relative lack of willingness on behalf of Member States to comply with such a scheme.[165] A greater willingness to cooperate, share information and exchange best practices at the EU level is still needed.

4.2.2 International Activities

At the international level, the Commission and the EEAS ensure, together with the Member States, coordinated international action in the field of cybersecurity.[166] The EU Global Strategy and the Joint

161 "Digitizing Industry (4.0) and Cybersecurity," 11.

162 "Digitizing Industry (4.0) and Cybersecurity," 9.

163 "Reform of Cybersecurity in Europe."

164 European Commission, "JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU," September 13, 2017, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017JC0450.

165 Bendetta Di Matteo, "New EU Cyber Strategy Leaves Key Security Gaps," Global Risks Insight, October 15, 2017, https://globalriskinsights.com/2017/10/new-eu-cyber-strategy-leaves-key-security-gaps/.

166 European Commission, "EU Cybersecurity Initiatives - Working towards a More Secure Online Environment."

Communication entitled "A Strategic Approach to Resilience in the EU's External Action" noted that the EU would continue to work internationally on cybersecurity promotion and cooperation building.[167] In June 2017, the development of a framework for a joint EU diplomatic response to malicious cyber activities – the so-called **Cyber Diplomacy Toolbox** (CDT) – was endorsed. Once approved, the CDT will provide a way of coordinating a response to malicious cyber activities directed against EU Member States in cyberspace, including the possible imposition of sanctions.[168]

In addition, the EEAS, the Commission and Member States engage in policy dialogue with a variety of international partners such as the Council of Europe (CoE), Organisation for Cooperation and Development (OECD), Organization for Security and Co-operation in Europe (OSCE), the North Atlantic Treaty Organization (NATO) and the United Nations (UN).[169] Direct dialogue and a measure of cooperation in the realm of cyber policies has also been established with key strategic partners such as Brazil, China, India, Japan, the Republic of Korea and the United States. With the financial sector bearing the brunt of cyber attacks, the Commission has endorsed the work of the G7 Cyber Expert Group to address the "increase in sophistication, frequency and persistence of cyber threats in the financial sector" and to develop a set of non-binding fundamental components of effective cybersecurity assessment by October 2017.[170]

The Commission also supports capacity building in third countries and envisages new cyber capacity building efforts to assist third countries in addressing cyber threats. The aim is to improve third countries' preparedness, increase their technical capabilities, establish effective legal frameworks to address issues pertaining to cybersecurity and cybercrime, while at the same time enhancing their capacity for effective international cooperation in these areas.[171]

4.2.3 National initiatives

To date, all 28 Member States have put complete cybersecurity strategies in place, with Greece being the most recent and the last state to adopt a national strategy.[172] Although all Member States have a cybersecurity strategy, the levels of maturity of adequate incident response capabilities among them

167 European Commission, "JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - A Strategic Approach to Resilience in the EU's External Action," June 7, 2017, 15.

168 Katriina Härmä and Tomáš Minárik, "European Union Equipping Itself against Cyber Attacks with the Help of Cyber Diplomacy Toolbox," The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), September 18, 2017, https://ccdcoe.org/european-union-equipping-itself-against-cyber-attacks-help-cyber-diplomacy-toolbox.html.

169 European Commission, "EU Cybersecurity Initiatives - Working towards a More Secure Online Environment," 7.

170 G7 2017, "COMMUNIQUÉ G7 Finance Ministers and Central Banks' Governors Meeting Bari, Italy, May 12-13, 2017," May 13, 2017.

171European Commission, "EU Cybersecurity Initiatives - Working towards a More Secure Online Environment."

172 ENISA, "ENISA National Cybersecurity Strategies (NCSSs) Map," Topic, European Union Agency for Network and Information Security, accessed September 20, 2017, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map.

varies significantly.[173] The NIS Directive requires all Member States to have a national/governmental incident response team, also known as a CERT, in place. CERTs help governments protect the critical information infrastructure and play a key role in coordinating incident management with the relevant stakeholders at the national level. They also bear responsibility for cooperation with the national and governmental teams in other countries.[174] **Figure 11** shows that all Member States have at least one public CERT. However, there are large differences in the amount of CERTs beyond that, in particular the number of private CERTs. An in-house team of a particular company, serving a certain customer-base or serving a particular industry would constitute a private CERT. Such forms of service and cooperation may significantly increase efficiency and capacity for incident response. According to ENISA, the diversity of such capabilities across the EU constitutes a key obstacle to achieving a cross-border cooperation that is needed to achieve a powerful incident response.[175]

173 ENISA, "CSIRTs in Europe — ENISA," Topic, European Union Agency for Network and Information Security, accessed September 20, 2017, https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities?tab=details.

174 ENISA, "Definition of National/Governmental CERTs - Baseline Capabilities — ENISA," Page, European Union Agency for Network and Information Security, accessed September 20, 2017, https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/baseline-capabilities.

175 ENISA.

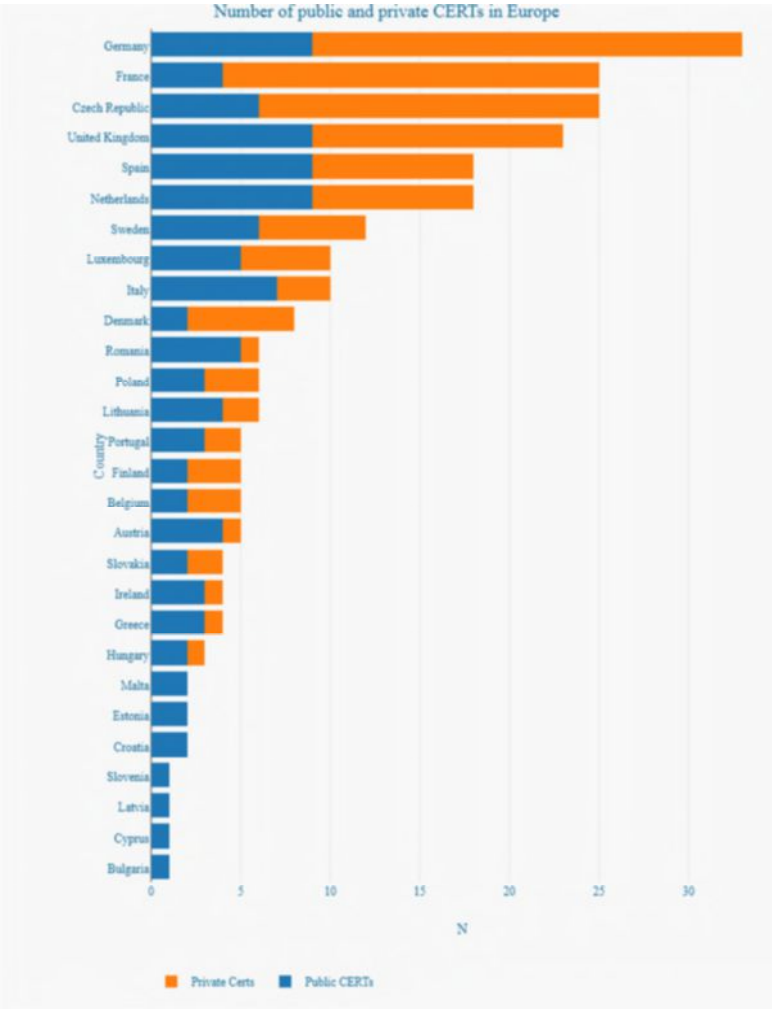


Figure 11: Number of CERTs per EU member state (public and private)[176]

With regard to public investment, cybersecurity is still not adequately enshrined in public policies. According to ENISA, many states will tolerate malicious activity as long as it remains within 'acceptable' levels, which are defined as affecting less than 2% of national GDP, which is currently the case in Europe. Germany is the only EU Member State that seemingly nears this 2% 'tolerance threshold'.[177] However, measuring the exact impact of cybercrime has proven to be difficult. Some countries may maintain different standards of measurement than others, potentially leading to discrepancies in what is considered tolerable.

Educational programs provide another venue through which governments can raise the awareness of cybersecurity issues and enlarge the pool of graduate students tailored to meet the needs of the cybersecurity market. As **Figure 12** shows, the distribution of cybersecurity education programs throughout Europe is uneven. With a total of 526 programs, the majority of them are located in only a

176 ENISA, "CSIRTs by Country - Interactive Map — ENISA," European Union Agency for Network and Information Security, accessed September 20, 2017, https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map.

177 Tofan, Nikolakopoulos, and Darra, "ENISA The Cost of Incidents Affecting CIIs: Systematic Review of Studies Concerning the Economic Impact of Cyber-Security Incidents on Critical Information Infrastructures (CII)," 5.

handful of countries, led by Germany, UK and the Czech Republic. Lithuania and Slovakia are the only Member States without cyber-related courses or certification programmes.

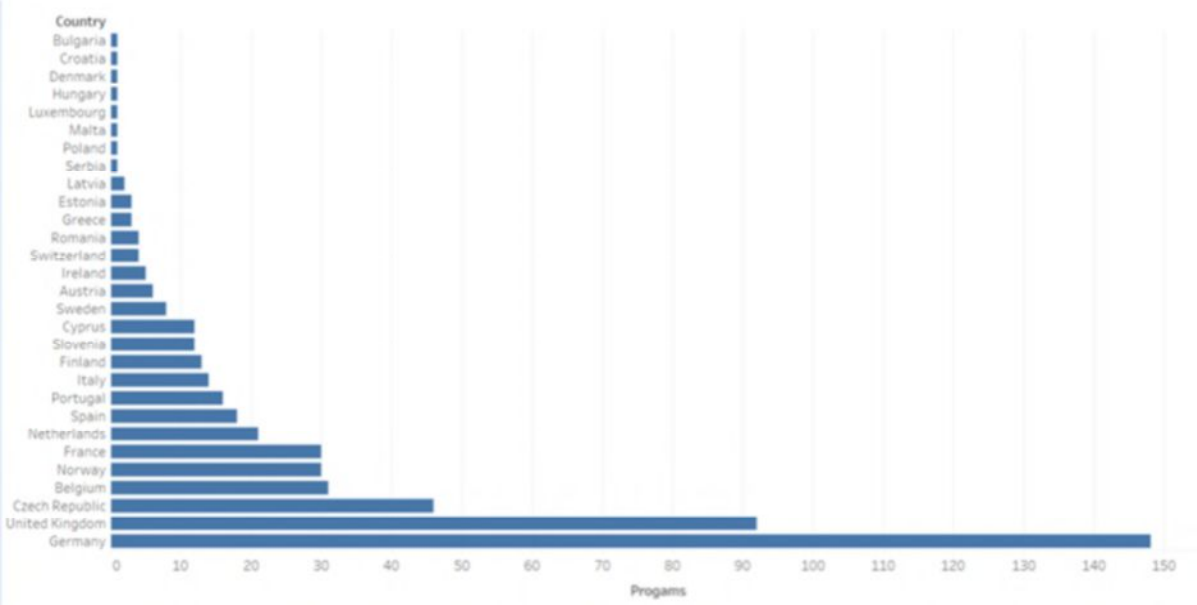


Figure 12: Available courses and certification programmes linked to Network and Information Security in EU Member States[178]

In 2015, Claire Vishik (Intel) and Maritta Heisel (University Duisburg-Essen) gathered data from 19 countries on cybersecurity education for ENISA, in order to compare approaches taken by different Member States with regard to available cybersecurity curriculum.[179] As **Figure 13** shows, cybersecurity is mostly taught at a graduate level – led by Germany and UK – while undergraduate programs remain very scarce across the EU.

178 "Education Map - ENISA," European Union Agency for Network and Information Security (ENISA), 2017, https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/universities.

179 Vishink & Heisel (2015) quoted in: Rademaker et al., "Dutch Investments in ICT and Cybersecurity - Putting It in Perspective," 35–37.

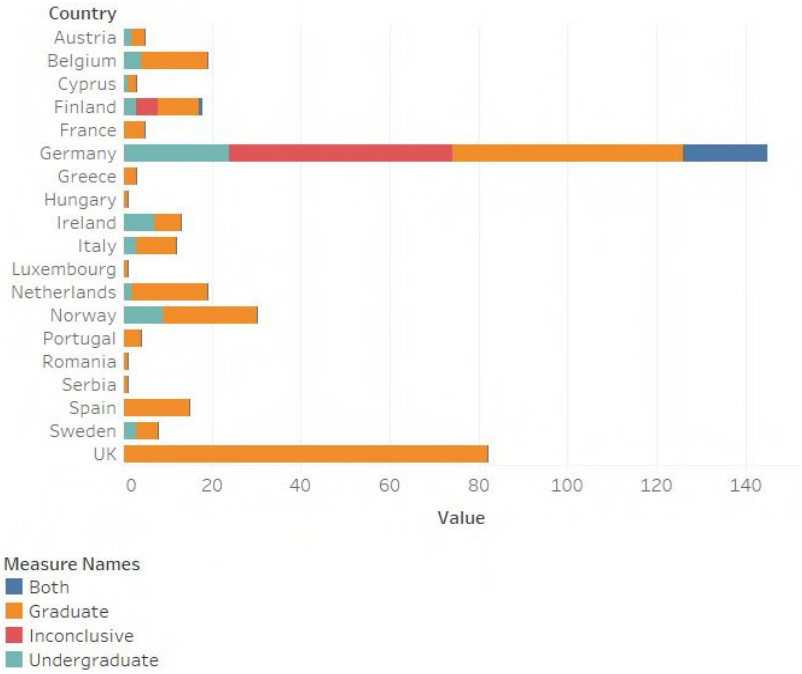


Figure 13: Numbers of graduate and undergraduate cybersecurity courses per country (last updated in August 2015)[180]

Moreover, their findings show that most cybersecurity courses are offered in the discipline of computer science (see **Figure 14**). It is evident that cybersecurity remains underrepresented in other non-technical educational programs. This is of particular relevance given the fact that governments and businesses alike have been calling for an interdisciplinary approach to cybersecurity as it is no longer regarded as a purely technical matter, but one that transcends into other domains, such as defense, politics, economics and law.[181]

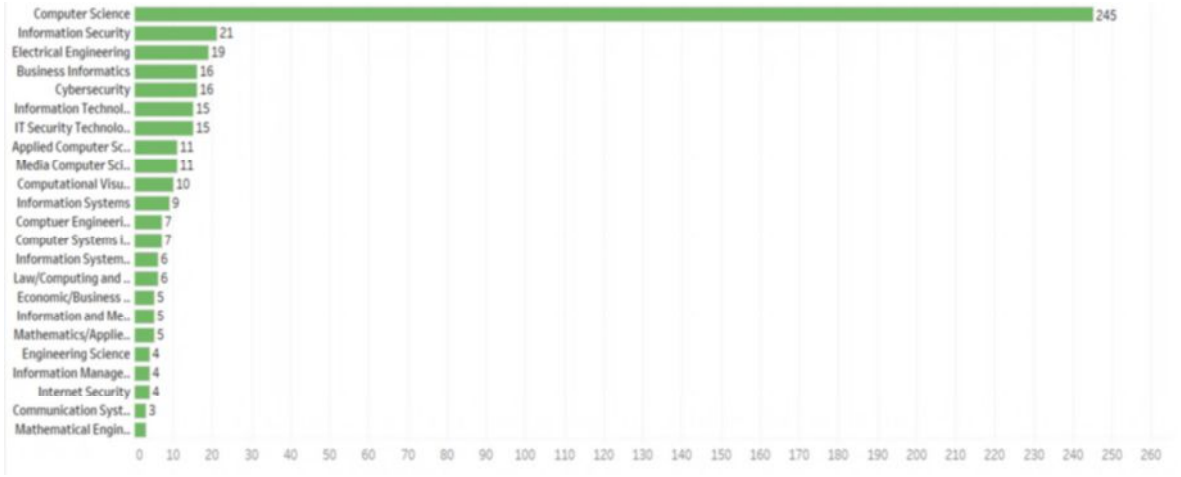


Figure 14: Number of disciplines in which most courses are offered (last updated in August 2015)[182]

180 Rademaker et al., 36.

181 Rademaker et al., 35.

182 Rademaker et al., 36.

4.3 EU Member States Comparison

Despite the European Commission stepping up its efforts, there is still a visible gap between countries in terms of knowledge, awareness and capacity to deploy strategies, programs and capabilities in the field of cybersecurity.[183] Although Europe, overall, performs well in terms of cybersecurity-related commitments when compared to other regions, these commitments are often unequally distributed with countries performing well in some areas, and less so in others.

In order to assess the cybersecurity performance of a given country or region, various indices and rankings have been developed over recent years. Indices provide interesting and potentially useful information on the progress of countries on the cybersecurity front. Indices and rankings worth mentioning include:

1. International Telecommunication Union (ITU) Global Cybersecurity Index, 2017
2. The National Cybersecurity Index (NCSI), 2017
3. Melissa Hathaway (Potomac Institute), Cyber Readiness Index 1.0 (2013) and 2.0 (2017)
4. Economist Intelligence Unit & Booz-Allen Hamilton, Cyber Power Index, 2017
5. World Economic Forum, Network Readiness Index (WEF-NRI), 2017
6. Kaspersky Cybersecurity Index, 2017
7. BSA EU Cybersecurity Dashboard, 2015

Because of differences in methodologies, approaches and geographic coverage which obstruct a comprehensive comparison of different indices and their resulting outcomes we founded our analysis on the results of the ITU's Global Cybersecurity Index (GCI), which was the only recently updated index covering the entire European region. A brief description of the limitations we encountered is provided in the Annex.

The ITU, the United Nations specialized agency for information and communication technologies, together with Member States, has established the Global Cybersecurity Index (GCI) in order to provide a more accurate picture of the cybersecurity situation globally, and to measure the commitment displayed by each contributing member state individually. The EU Member States are classified according to five key pillars comprised of various indicators, with a weighted average of all indicators for a specific pillar representing its specific score. The five pillars are legal, technical, organizational, capacity building and cooperation, with twenty five individual indicators. Using these pillars, a final score was computed for each Member State – scores upon which the bulk of our analysis is based.

183 "Global Cybersecurity Index 2017: Europe," 5.

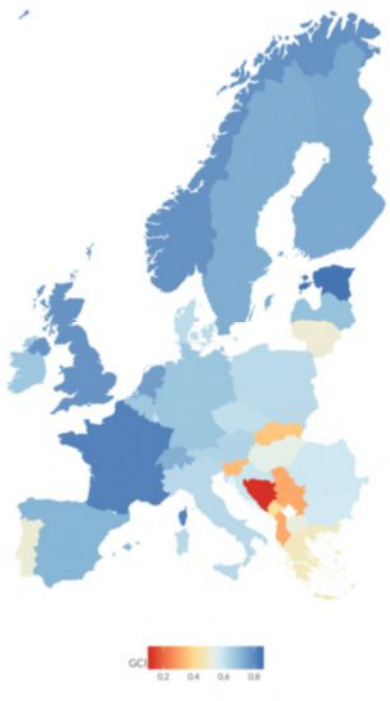


Figure 15: The map of national cybersecurity commitments in the EU (including Norway, Switzerland and the Balkans).[184]

When the level of commitment to cybersecurity on a public (government) level is observed throughout the EU, a fairly heterogeneous and fractured landscape emerges. Regional leaders, such as Estonia, France, Norway and the United Kingdom serve as models from which less cyber mature states, such as Portugal, Lithuania, Greece, Slovakia and Slovenia can learn.

Leading EU Member States	Estonia, France, Norway*, UK, Netherlands, Finland, Sweden, Switzerland*, Spain, Latvia, Germany, Ireland, Belgium, Austria, Italy, Poland, Denmark, Czech Republic, Luxemburg
Maturing EU Member States	Croatia, Romania, Bulgaria, Hungary, Portugal, Lithuania, Greece, Iceland, Slovakia, Slovenia.

Table 4: EU Member States classification according to their GCI score.[185]

Over the past 10 years, **Estonia** has not only become a European leader, but also a global heavyweight in cybersecurity.[186] The country has taken great lengths to stay ahead of potential cyber threats and its preparedness to handle cyber assaults has considerably increased since the 2007 cyber attack. Estonia's cybersecurity is sustained by high-functioning e-government infrastructure, a central system for monitoring, reporting and resolving incidents, and a mandatory security baseline for all

184 "Global Cybersecurity Index 2017: Europe," 12.

185 "Global Cybersecurity Index 2017: Europe," 12.

186 In 2017, Estonia led European rankings, and was also among the top ten most committed countries globally, according to GCI.

government authorities. Since 2013, Estonia has legislation in place that mandates vital service providers to assess, manage and report ICT incidents.[187] Estonia systematically raises public cybersecurity awareness and competence by means of training and education in both the technical and non-technical aspects of cyber defence. Most importantly, there is a shared understanding that cybersecurity can only be ensured through cooperation and that a joint contribution is required from the government, industry and citizens alike.[188] The country also hosts the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), which focuses on research, development, training and education in cyber defence and, as such, contributes to NATO's growing cyber capability.[189] Over the past 10 years, Estonia has not only become a European leader, but a world leader in cyber commitment.[190]

According to the ITU rankings, **France** occupies the second place among EU Member States in terms of cyber commitment. Earning first place in both the technical and capacity building pillars, it serves as another model that less prepared Member States can emulate. France sees cyberspace as a frontier that must be secure in order to allow for economic growth. The established French authority on matters relating to cyberspace, the National Agency for the Security of Information Systems (ANSSI) has published measures specific to various sectors, allowing France to set a benchmark in managing cybersecurity[191]. Although France focuses strongly on issues of national security and defence, it has shown willingness and understanding when it comes to adapting to the cybersecurity environment by adopting its first national cybersecurity strategy in 2011, and following up in 2015 with a second, revised national cybersecurity strategy in response to increasing volume of cyber attacks.[192] The national strategy contains recommendations for closer cooperation with the private sector. Since the late 1990's, the Gendarmerie (a military force charged with civilian police duties) has been combating cybercrime through the use of several institutions such as the Center for the Fight against Digital Crime (C3N), the National Center of Child Pornography Images (CNAIP) and specialized cybercrime training programs run by the National Center for Police Training.[193]

Norway ranks third regionally and occupies the first place in the legal pillar. The country has enacted specific legislation and regulation related to cybersecurity through various instruments such as the Electronic Commerce Act, the Personal Data Act, and the Freedom of Information Act, among others.[194] Aside from laws dealing with cybersecurity, Norway has taken a keen interest in understanding its cybersecurity culture in order to pinpoint weaknesses that may facilitate the

187 BSA, "BSA Country: Estonia" (BSA, 2015), http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_estonia.pdf.

188 "How Estonia Became a Global Heavyweight in Cybersecurity," e-Estonia, June 2017, https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/.

189 "CCDCOE," CCDCOE, accessed January 12, 2018, https://www.ccdcoe.org.

190 "How Estonia Became a Global Heavyweight in Cybersecurity."

191 BSA, "BSA Country: France" (BSA, 2015), http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_france.pdf.

192 Melissa Hathaway et al., "France Cyber Readiness At A Glance" (Arlington, VA: Potomac Institute, 2016), http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_france.pdf.

193 Hathaway et al.

194 "Global Cybersecurity Index 2017: Europe," 25.

compromise of its cyber landscape. Part of its assessment include understanding the degree to which citizens would accept monitoring of their online activities and understanding trust levels between various actors in the Norwegian cyberspace.

In 2016, the UK's National Crime Agency (NCA) reported that cybercrime had surpassed all other forms of crime in the UK, reiterating the need for cyber defensive capabilities. As the fourth strongest European state in terms of cyber commitment, the United Kingdom plans to almost double its investment in cybersecurity (up to a maximum of $2.35billion over the next five years) significantly boosting its already strong commitment to cyberspace.[195] In addition to increased spending, the UK actively supports development programs targeted towards grooming the next generation of cyber professionals through training courses. The UK government has also issued reports seeking to provide guidance for teachers to better integrate cybersecurity into their curricula.[196]

When a breakdown of the five pillars is observed in greater detail (see ANNEX 2), it becomes apparent that several EU Member States consistently rank below the European average. **Slovakia** and **Slovenia** are the most consistent underperformers, both ranking below the European average in each pillar defining a country's cybersecurity commitment. Neither of the two possesses any form of law enforcement training in the realm of cybersecurity, while Slovakia appears to be the weakest in terms of cybersecurity regulations, with an exceptionally low score of 0.095 out of 1. Slovenia is the 4th weakest Member State when cyber-criminal legislation is concerned, which indicates a lack of institutional frameworks intended to handle cyber-criminal infractions. Sectoral CERTs and public-private partnerships for cybersecurity are also absent in Slovenia. Although the absence of sectoral CERTs alone does not indicate weakness (Estonia does not have sectoral CERTs either), this factor in conjunction with other vulnerabilities should be a cause for concern. Moreover, both Slovenia and Slovakia lack certification frameworks for professionals in the cyber industry. Most concerning, however, is the absence of any form of a homegrown cybersecurity industry in both countries, as indicated by the score of zero allocated to both by the ITU. Aside from possible government protection, businesses in both countries under study are expected to deal with cyber infractions without any third-party help (excluding the possibility of outsourcing cybersecurity to firms outside of the country), forcing them to face threats head on using their own cyber defensive capabilities. These may vary to extreme degrees depending on the enterprise itself.

Despite the aforementioned weaknesses, it is important to note that Europe, relative to the rest of the world, shows very strong levels of commitment towards cybersecurity. Estonia and France not only topped the European rankings, but were also among the top ten most committed countries globally in 2017. The weaker states – Slovenia and Slovakia among others not mentioned – must be fortified as they could pose a significant vulnerability within Europe. Ideally, these weaknesses would be

195 Ponemon Institute, "The Cyber Resilient Organisation in the United Kingdom: Learning to Thrive against Threats," January 2016, http://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/TheCyberResilientEnterpriseUKFINAL.pdf?submissionGuid=0d7b9d75-06ee-49df-a641-a726c26d2b73.

196 Hathaway et al., "France Cyber Readiness At A Glance."http://www.potomacinstitute.org/images/CRI/CRI_France_Profile_PIPS.pdf

addressed before weaker states endure an attack similar to the one encountered by Estonia in 2007. It is important for EU Member States to approach cybersecurity in a proactive way.

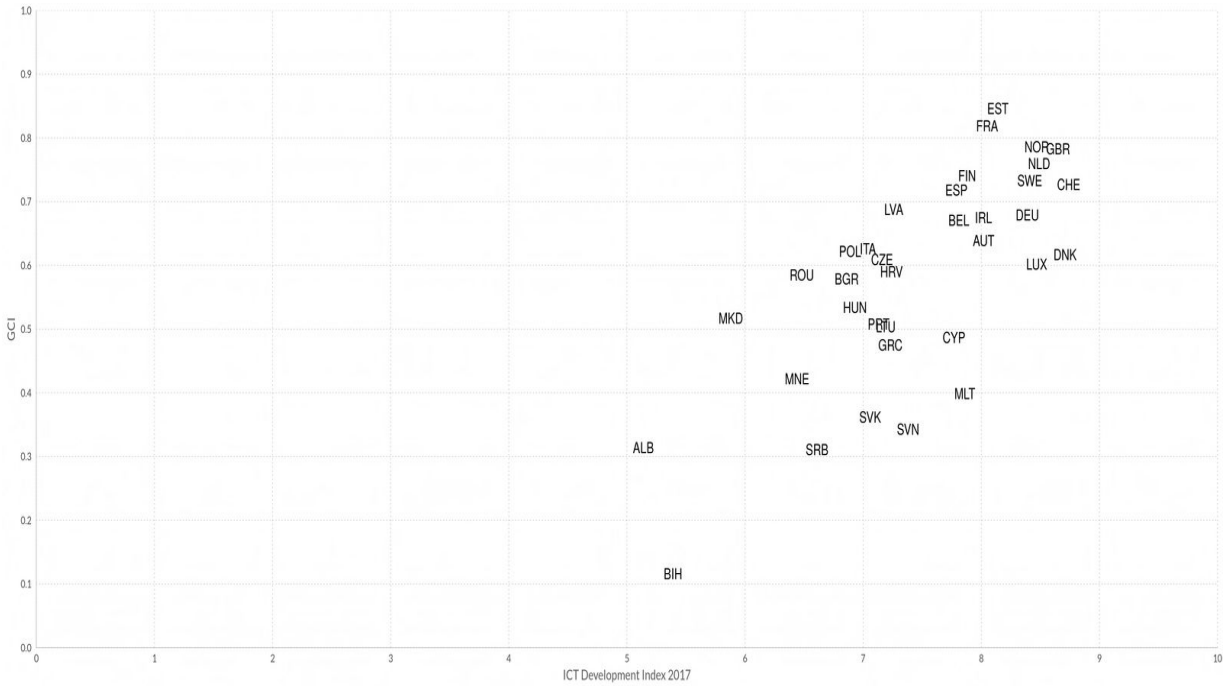


Figure 16: Comparison of the GCI and and IDI across the EU (including Norway, Switzerland and the Balkan states).[197]

Figure 16 explores the relationship between a country's overall ICT development status and the level of cybersecurity commitment, represented by the IDI (ICT Development Index 2017) and the GCI (Global Cybersecurity Index 2017), respectively.[198] The vast majority of EU Member States which score high in terms of ICT development also invest in cybersecurity with a similar level of commitment. This linear/close relationship is also confirmed by ITU, which states: "given Europe's high level of IT development, it is not surprising that the region overall is doing well in all five pillars of the GCI, despite a few countries in the region with low marks."[199] At the same time, it can be inferred that the average GCI score is slightly weaker than the corresponding IDI score, although there are some countries that show a larger gap between the two indicators. It is interesting to note that Romania and Bulgaria, which experience lower levels of ICT development than Greece, Slovakia or Slovenia, for example, show higher cybersecurity commitment. As has been aforementioned (Section 3.1.1.2; Figure 3), Romania and Bulgaria find themselves above the global average in terms of encountered malware, which has most likely triggered the interest of both the public and private sector in increasing cybersecurity commitment. EU MS need to harmonize their cybersecurity practices to ensure a safe and appropriate use of ICTs as enablers for economic development.

197"Global Cybersecurity Index 2017: Europe," 21.

198 Comparison of the GCI with the ITU ICT for Development Index (IDI). The ICT Development Index (IDI) is used to monitor and compare developments in information and communication technology between countries and over time.

199 GCI 2017: Europe, p. 23.

4.4 Current state of cyber resilience of businesses

Cybersecurity is no longer a concern of governments only. Today, the private sector needs to respond, protect and design strategies toward capacity building and awareness. One way to judge the cybersecurity preparedness of an individual enterprise is to see whether it has a formally defined ICT security policy[200] in place, i.e. measures, controls and procedures applied by enterprises in order to ensure integrity, confidentiality and availability of their data and ICT systems. A 2015 Eurostat survey shows that the share of enterprises having a formally defined ICT security policy largely depends on a company's size. While 72% of large enterprises (250 or more persons employed) had such a policy in place, this percentage drops to 51% for medium enterprises (50-249 persons employed), and further to 27% for small enterprises (10 to 49 persons employed).[201] It is interesting to note that the share of large enterprises with a formally defined ICT security policy is almost three times the share of small ones. In comparison to 2010, cybersecurity preparedness of individual enterprises increased across all company sizes. Although the financial sector formed part of the Eurostat survey in 2010, it was not included in 2015, which complicates cross-sector comparison between 2010 and 2015.

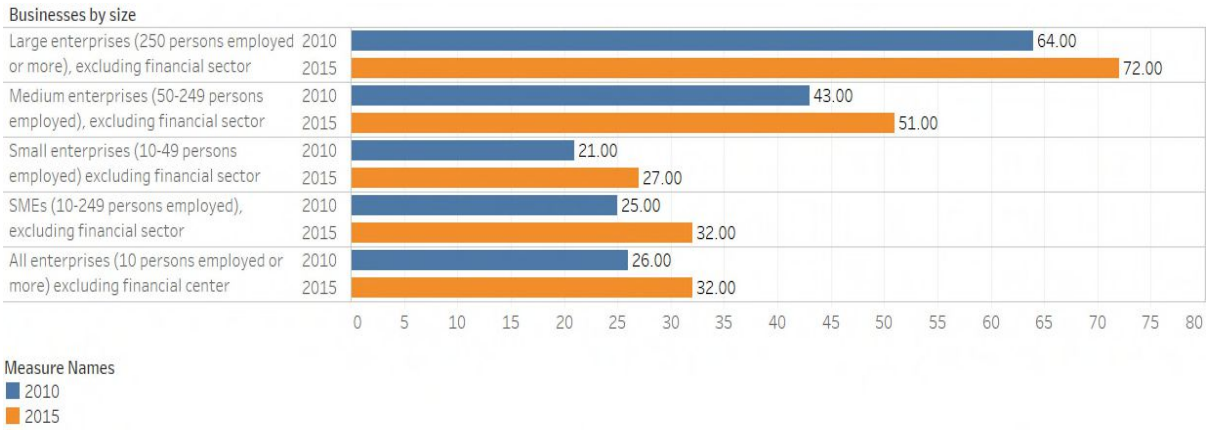


Figure 17: Percentage of EU companies having a formally defined ICT security policy by company size[202]

The share of enterprises having a formally defined ICT security policy in place also varies considerably between individual Member States. Across the EU, 32% of companies had a formally defined ICT security policy (see **Figure 18**). This represents an increase of 6% when compared to the situation recorded in 2010. In 2015, the highest percentages were recorded in Sweden and Portugal, where over 45% of all enterprises had a formally defined ICT security policy in place. Countries that made significant progress between 2010 and 2015 include Bulgaria, Romania, Slovenia, Croatia and Portugal. It is interesting to note that some countries that score low on level of business digitalisation – Italy or Croatia, for example – score high in terms of having a formally defined ICT security policy in place.

200 Eurostat uses the term "ICT security" which will be used interchangeably with cybersecurity in this chapter.

201 Eurostat, "ICT Security in Enterprises," Eurostat - Statistics Explained, December 2015, http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises.

202 Eurostat: ICT security in enterprises, comparison of Eurostat survey results in 2010 and 2015.

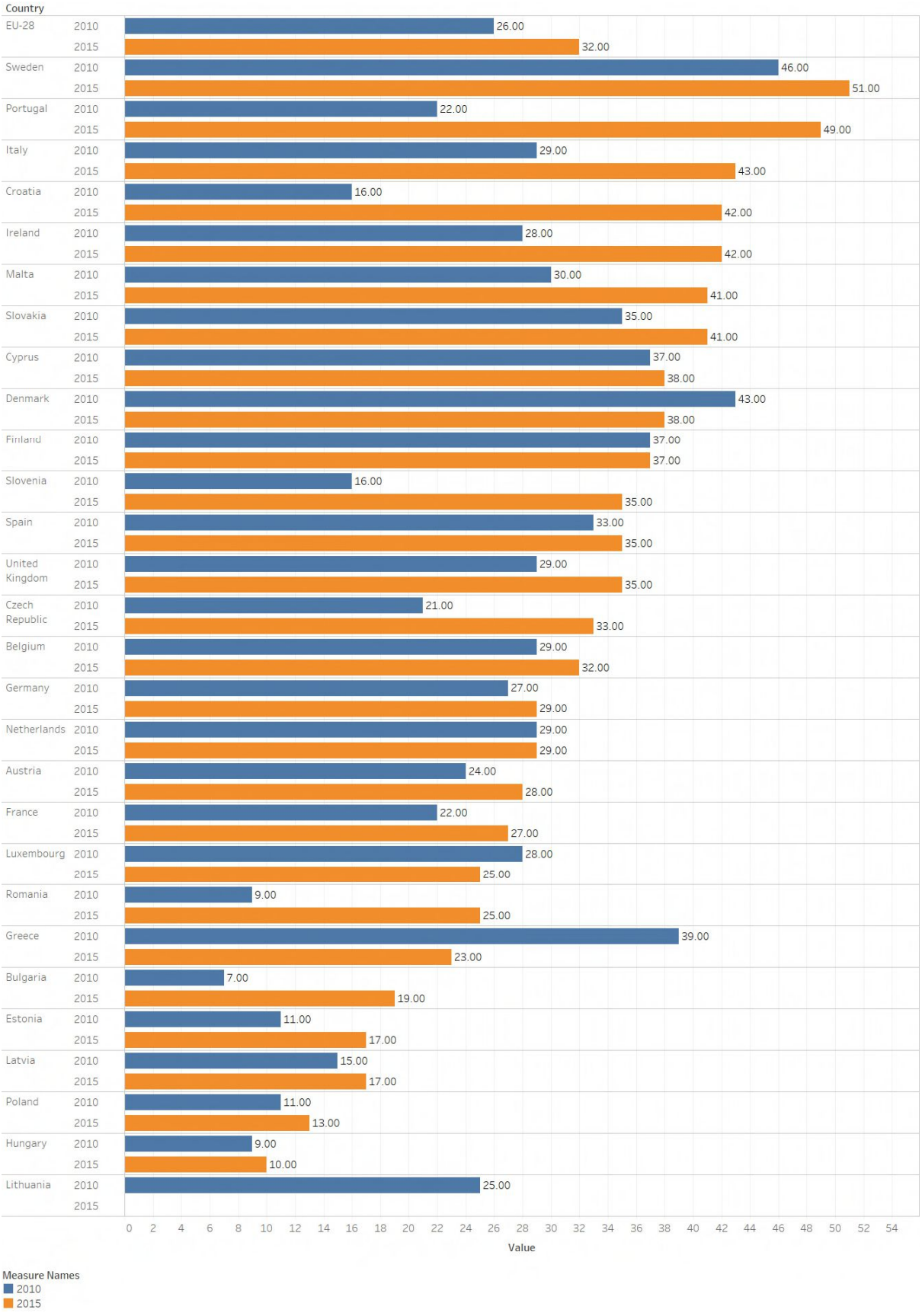


Figure 18: Percentage of EU companies having a formally defined ICT security policy by member state

In terms of sectoral awareness, all economic sectors have made some progress in the period between 2010 and 2015 (see **Figure 19**). Some sectors that face high threat levels – such as administration and services, and retail trade – continue to lag behind. The same goes for less technically sophisticated sectors, such as construction and transportation, where the percentage of companies with a formal cybersecurity policy is substantially lower. Although the financial sector, which is most concerned by the threat of a cyber attack globally,[203] formed part of the Eurostat survey in 2010, it was not included in 2015, which complicates cross-sector comparison of the awareness of financial institutions between 2010 and 2015.

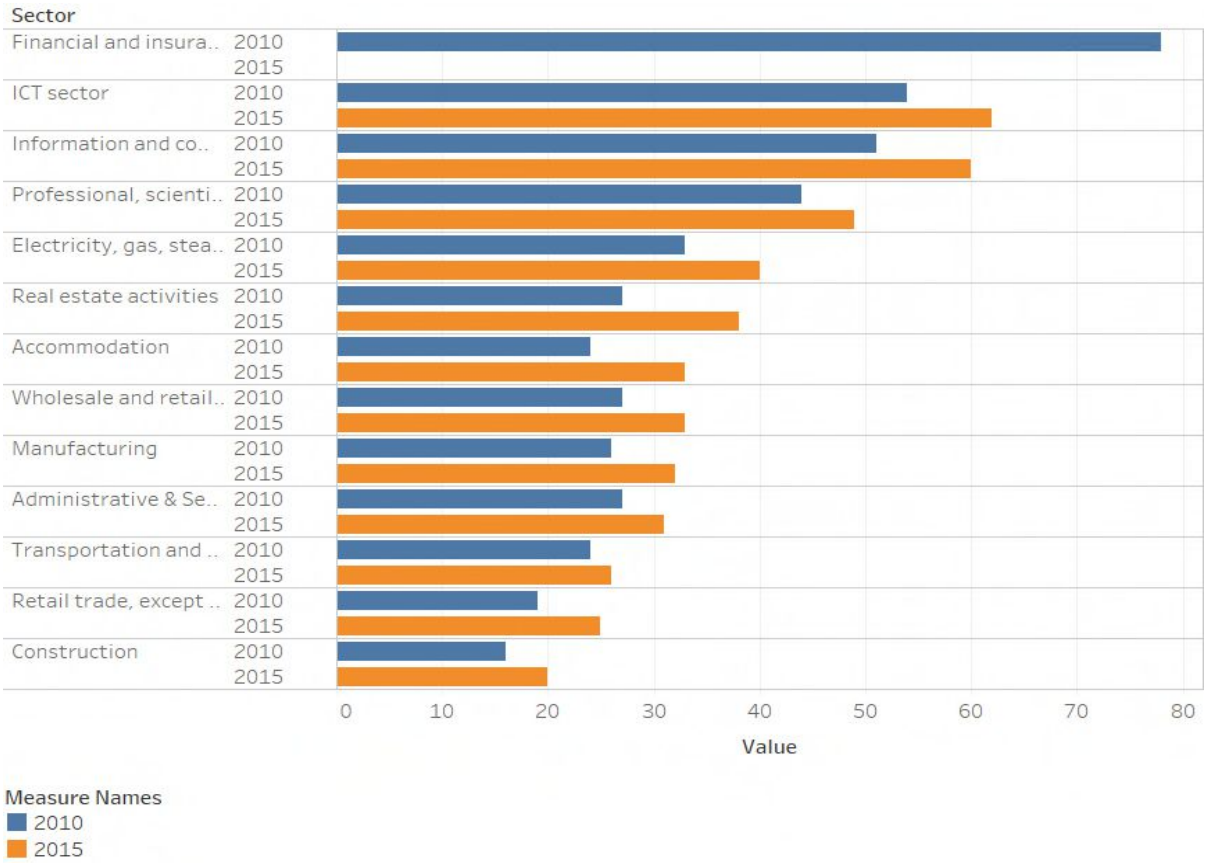


Figure 19: Percentage of EU companies having a formally defined ICT security policy by economic sector

ICT security policy translates into various approaches that enterprises adopt. One group of efforts aims to protect systems and data by internal security procedures such as offsite data backup and strong password authentication. Other efforts are targeted towards improving the awareness and skills of employees, such as mandatory trainings on security policies.[204] The Ponemon *Cost of Cybercrime Study* (2016) identifies three best practices as most effective in reducing the costs of cybercrime: integration of security operations with enterprise risk management activities; sharing of threat intelligence and/or collaborating with industry partners/competitors on security issues; and advanced

203 GrantThornton, "Cyber Attacks Cost Global Business over $300bn a Year."

204 See Eurostat survey results for 2010: Eurostat, Konstantinos Giannakouris, and Maria Smihily, "ICT Security in Enterprises, 2010," Industry, trade and services (Eurostat, July 2011).

procedures for backup and recovery operations.[205] According to the findings of the same study, formal cybersecurity strategies – including those related to the GDPR implementation – have a positive but limited effect, which means they are merely policy on paper until they are actually put in practice.[206]

4.4.1 The scale of cybersecurity expenditure

The scale of a company's cybersecurity expenditure provides a good gauge for measuring the real perception of cyber threats and demand for IT security solutions. Unfortunately, this data is not easily accessible and credible estimates are close to impossible to find. Most often, estimates of cybersecurity spending reside within market research firms, which treat them as confidential and proprietary business information. When such data is publically available, it is often inconsistent due to the absence of a shared definition of 'cybersecurity' by corporations across the EU. In addition, the methodologies used to estimate the size of the cybersecurity market differ as well. As a consequence, estimates of cybersecurity spending and the scope of the cybersecurity market differ widely.[207] Several sources show a continuous increase in spending on cybersecurity. Gartner and PwC estimated the European cybersecurity market to be worth $22 billion in 2016, and expected it to grow at the rate of 8.3% per annum to 2018.[208] *The Darkening Web* offers an estimate of private-sector cybersecurity spending in Europe to be at around €27 billion (estimated US$33 billion), which is considerably lower in comparison to the US market, which was estimated to be around $75 billion in 2015 (these numbers include sales to the government).[209]

A survey conducted by the WEF and McKinsey points out that cybersecurity spending and enterprise maturity do not necessarily correlate. While some companies spend little on IT security and spend it poorly, others punch above their weight by spending little and doing a better job at risk management. A third group of companies spend vigorously and have a good return on their investment in terms of capabilities that have been developed. The last group is populated by companies that spend a great deal without much risk management sophistication.[210]

4.5 Skills gap

Another way to judge the cybersecurity preparedness is to study the number of cybersecurity professionals who work on securing businesses, government agencies and organizations of all sizes. According to the 2017 PREDICT Report of the European Commission's Joint Research Centre, ICT

205 Ponemon Institute, "2016 Cost of Cyber Crime Study & the Risk of Business Innovation," 21.

206 Ponemon Institute, 21.

207 This assessment is based on the findings of: Maarten Gehem et al., "Assessing Cybersecurity - A Meta-Analysis of Threats, Trends, and Responses to Cyber Attacks," Security (The Hague, Netherlands: The Hague Centre for Strategic Studies, April 16, 2015), 65.

208 PwC, "Cybersecurity: European Emerging Market Leaders," 4.

209 Klimburg, Alexander, The Darkening Web: The War for Cyberspace (New York: Penguin Press, 2017).

210 "Risk and Responsibility in a Hyperconnected World," Insight Report (Geneva, Switzerland: World Economic Forum (WEF), January 2014), 15.

sector employment in the EU exceeded 5.6 million people in 2014.[211] The study utilized a definition of the ICT sector based on the NACE-Rev.2 classification of economic activities in the European Community.[212] Although NACE-Rev.2 includes numerous categories related to security provision, cybersecurity is not featured as a separate classification and is subsumed within generic IT categories. Similarly, "e-Skills in Europe", a study conducted by Empirica which is based on the international ISCO-08 descriptions of occupations, estimated the total ICT workforce in Europe to be at 7.5 million in 2014.[213] 48% of these ICT practitioners were working in the ICT industry sector. As in the case of NACE-Rev.2, cybersecurity is not differentiated within ISCO-08 codes which makes it difficult to determine the actual size of the cyber-security workforce within the EU. An effort towards the addition of a cybersecurity specific identifier within these systems may produce more reliable statistics than the ones that are currently available.

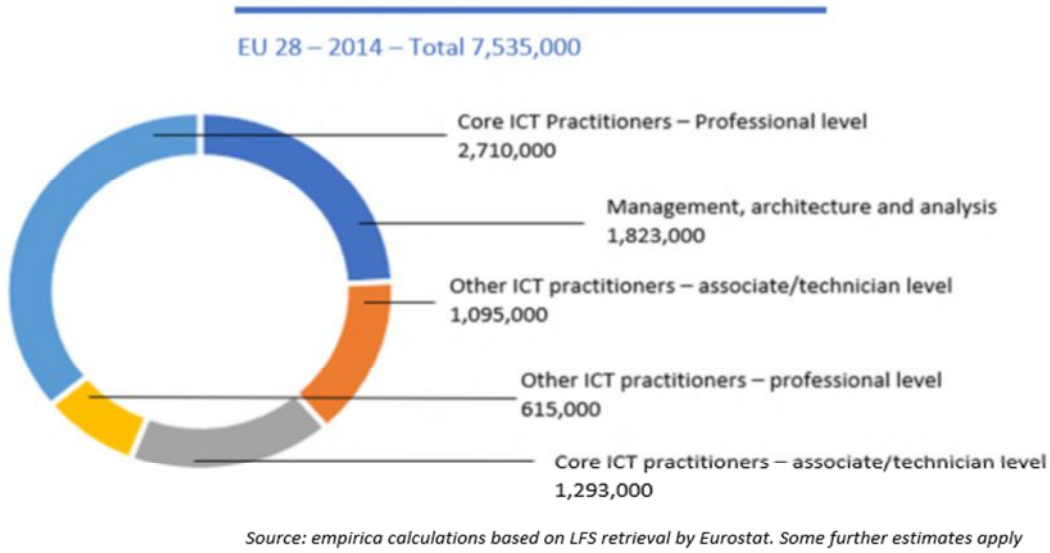


Figure 20: ICT professional workforce in Europe in 2014, by ISCO-08 skills clusters[214]

Such classification would also help in accurately assessing supply and demand for cybersecurity professionals. In Europe, the demand for ICT practitioners is growing at a rate of around 4% a year.[215] Open vacancy data, available from different sources for several countries, reveals a "severe excess demand" for "core ICT jobs", such as software and application developers, web and multimedia experts, database designers and administrators, system administrators and network and operations

211 M Mas et al., "The 2017 PREDICT Key Facts Report" (Joint Resarch Centre, 2017), 7.

212 E. Bengales et al., "The 2017 PREDICT Dataset Methodology" (Joint Resarch Centre, 2017), 10.

213 Tobias Husing, Werner B. Korte, and Eriona Dashja, "Trends and Forecasts for the European ICT Professional and Digital Leadership Labour Markets (2015-2020)" Empirica, November 2015), 8.

214 Husing, Korte, and Dashja, 7.

215 DIGITALEUROPE, "Facts and Figures," digitaleurope.org, accessed October 16, 2017, http://www.digitaleurope.org/Our-Work/Projects/Past-projects/eSkills-for-Jobs/Facts-and-Figures.

practitioners.[216] This demand carries over into the field of cybersecurity. As the 2017 *Global Information Security Workforce Study* underscores, "nearly 40% of European firms are looking to grow their cybersecurity teams by at least 15% over the next 12 months".[217] Concurrently, the available supply of ICT personnel has been declining. The number of computer science graduates peaked in 2006 and has recorded a steady decline ever since.[218]

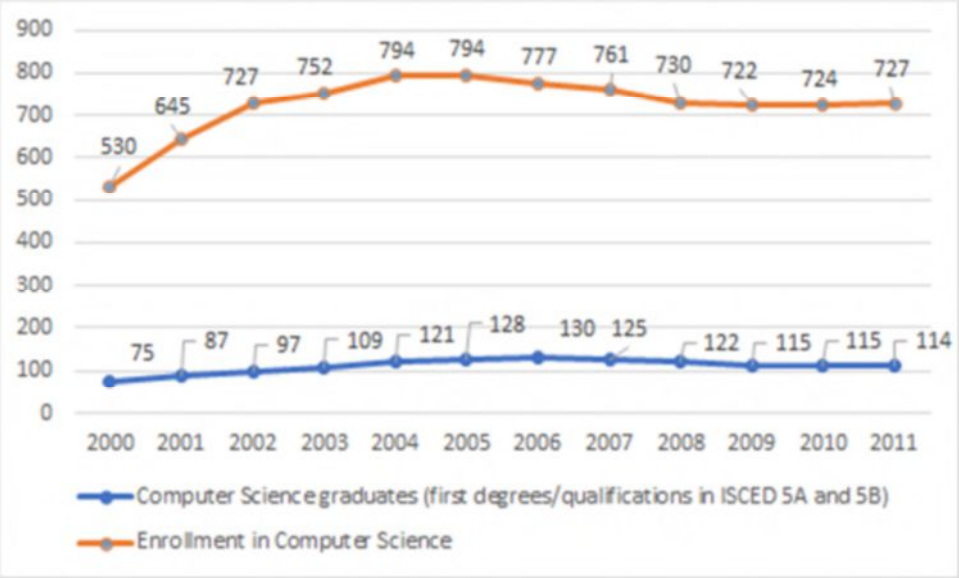


Figure 21: Enrolment in and graduates from computer science studies in Europe (EU-28), in thousands[219]

As a consequence, the demand has already outstripped the supply by a wide margin, with the gap reaching 755,000 potential vacancies by 2020 (see **Figure 22**).[220] This shortage is caused by the lack of relevant e-skills and includes all categories of ICT employees. Despite the lack of cybersecurity specific studies, the aforementioned 2017 GISW Study estimates that Europe may face a gap of 350,000 cybersecurity professionals by 2022: "*The combination of virtually non-existent unemployment, a shortage of workers, the expectation of high salaries, and high staff turnover that only increases among younger generations creates both a disincentive to invest in training and*

216 Husing, Korte, and Dashja, "Trends and Forecasts for the European ICT Professional and Digital Leadership Labour Markets (2015-2020)," 13.

217 Stuart O'Brien, "Demand for Cybersecurity Professionals on the Rise – Total...," Total Security Summit (blog), June 12, 2017, https://totalsecuritysummit.co.uk/demand-for-cyber-security-professionals-on-the-rise/.

218 Husing, Korte, and Dashja, "Trends and Forecasts for the European ICT Professional and Digital Leadership Labour Markets (2015-2020)."

219 Eurostat, some imputations and assumptions apply.

220 Husing, Korte, and Dashja, "Trends and Forecasts for the European ICT Professional and Digital Leadership Labour Markets (2015-2020)," 23.

development and a conundrum for prospective employers of how to hire and retain talent in such an environment."[221]

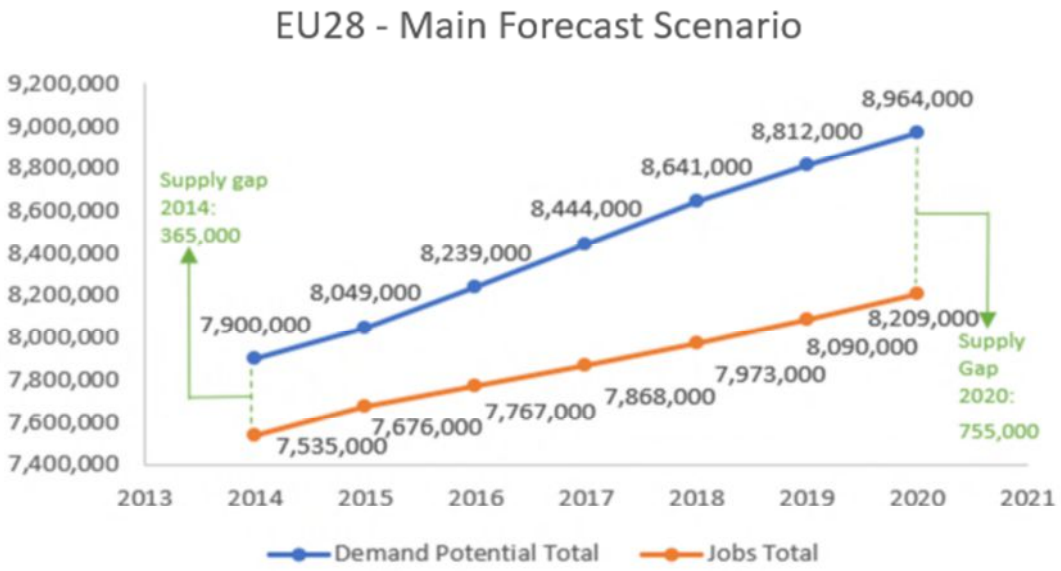


Figure 22: Main forecast scenario: ICT Professional Jobs and Demand in Europe (EU-27) 2014-2020.[222]

In addition to ICT professionals working in the private sector, more attention ought to be paid to the shortage of cyber experts in academia and civil society, who are responsible for educational activities. The severely uneven distribution of cyber-related programs throughout Europe serves as an indication of the lack of cyber experts in the academic field in the vast majority of European countries. The same applies to the civil society arena, where more work needs to be done in order to get more experts into the field to provide support and deterrence against cyber threats.

4.6 Comparison of public and private commitments

We approached the task of comparing public and private commitment towards cybersecurity by using two different rankings discussed in this report. The GCI (2017) was used as a proxy to measure public commitment, though a comparable index detailing private sector commitment has yet to become available. As such, an indicator presented by Eurostat that quantifies the percentage of private firms with ICT security policies in place was used as a proxy to analyze cybersecurity preparedness of the private sector. While this is not ideal, as the GCI is comprised of 25 indicators compared to Eurostat's 1, until a more comprehensive analysis and indices are published regarding the private sector, we will continue to use the Eurostat indicator. This imbalance may reflect on the accuracy of our results.

221 PwC, "The Global State of Information Security® Survey 2017"; Jay Jay, "Europe May Face Cyber-Security Skills Gap of 350,000 Workers by 2022," TEISS, June 6, 2017, https://teiss.co.uk/news/europe-may-face-cyber-security-skills-gap-350000-workers-2022/.

222 Husing, Korte, and Dashja, "Trends and Forecasts for the European ICT Professional and Digital Leadership Labour Markets (2015-2020)," 23.

Public sector ranking (GCI 2017)		Private Sector ranking (Eurostat 2015)
1	Estonia	Sweden
2	France	Portugal
3	United Kingdom	Italy
4	Netherlands	Ireland
5	Finland	Croatia
6	Sweden	Malta
7	Spain	Slovakia
8	Latvia	Denmark
9	Germany	Cyprus
10	Ireland	Finland
11	Belgium	United Kingdom
12	Austria	Spain
13	Italy	Slovenia
14	Poland	Czech Republic
15	Denmark	Belgium
16	Czech Republic	Netherlands
17	Luxembourg	Germany
18	Croatia	Austria
19	Romania	France
20	Bulgaria	Luxembourg
21	Hungary	Romania
22	Portugal	Lithuania
23	Lithuania	Greece
24	Cyprus	Estonia
25	Greece	Bulgaria
26	Malta	Latvia
27	Slovakia	Poland
28	Slovenia	Hungary

Table 5: Comparison of country rankings provided by the GCI (2017) and Eurostat (2015).

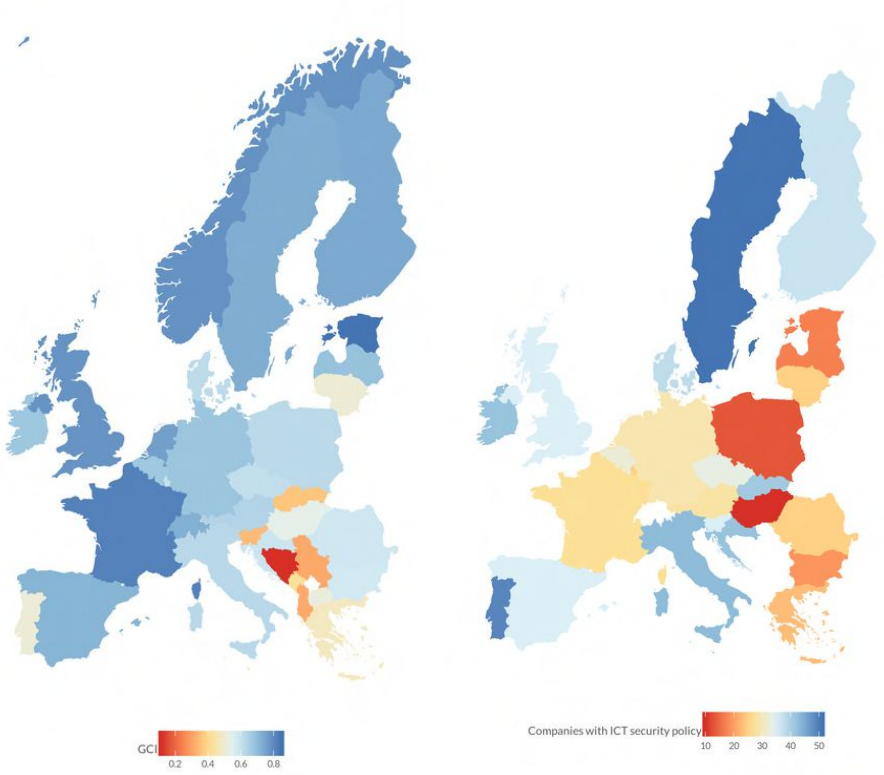


Figure 23: Comparison of public and private commitment to cybersecurity on the basis of the rankings provided by the GCI (2017) and Eurostat (2015).

Figure 23 reveals possible discrepancies within EU Member States relating to private and public sector attitudes towards cybersecurity. When comparing the GCI scores of Member States with their private sector's preparedness as reported by Eurostat, several key findings can be ascertained. There seems to be an inverse relationship between state-level preparedness and private-level preparedness. Estonia and France, both occupying ranks 1 and 2 respectively in the GCI score, rank only 24th and 19th respectively in terms of private sector preparedness. While it is difficult to identify exact causes of such differing rankings, it could be that private enterprises feel adequately protected by government initiatives and regulations relating to cybersecurity, which could have resulted in the lack of incentives to develop their own protection mechanisms.

Member States that perform poorly relative to other European states in the public-sector rankings perform strongly when the private sector is analysed. Slovakia and Slovenia, two countries that lag behind in the public sphere, achieved ranks 7 and 13 respectively in private sector preparedness. Due to a lack of public oversight, it is possible that private firms of all sizes in both Slovakia and Slovenia feel the need to fortify their cyber protocols and preparedness and be in a position where they are able to face attacks themselves. Two other examples of Member States that score low in the public sector ranking yet score high in the private sector rating are Portugal and Croatia achieving rank 2 and 5 in the private sector, and rank 22 and 18 in the public sector, respectively. Both governments and industry stakeholders should actively participate in future efforts to enhance their cybersecurity.

5. Bottlenecks in public and private policies

Corporate Europe faces challenges in implementing cybersecurity practices both from an external, public policy perspective, and from an internal, company perspective. From the external perspective, the challenges comprise the adequacy – or lack thereof – of current legal and regulatory frameworks, educational programs, financial and facilitating instruments, as well as the level of cyber threat intelligence sharing that may all affect the private sector's ability to effectively tackle the bottlenecks described. From an individual company perspective, the challenges relate to the general level of awareness, appropriate training and availability of skilled personnel, the availability of necessary funding and equipment, organizational design, technological vulnerabilities, and lack of trust to share information.

5.1 External/public policy perspective

5.1.1 Fragmented regulatory environment

Cybersecurity is a challenge shared by all EU Member States. A collective ability to address vulnerabilities, risks and threats – particularly to critical information infrastructures – is viewed as crucial for providing high levels of cybersecurity across Europe.[223] The EU continues to face heterogeneity of security and privacy regulations across Member States, which presents a hurdle to effective cross-border collaboration. This is compounded by the fact that each EU Member State has a different level of cybersecurity maturity. Divergence of approaches towards cybersecurity is evidenced by the limited number of Member States participating in the European Government CERT group.[224] This slow development of cybersecurity regulatory frameworks is struggling to keep pace with the evolution of the digital realm. It is imperative that future regulatory changes are equal across all Member States so as to avoid businesses being subject to different levels of security.

5.1.2 Lack of financial support

The European Commission has recognized that SMEs, among other actors, find it challenging to address even the most basic cybersecurity threats. It has therefore earmarked €22 million from Horizon 2020, Europe's largest R&D programme, towards a project that could help overcome these shortcomings.[225] The Commission has also launched the first European public-private partnership on cybersecurity, a €450 million investment (also under the Horizon 2020 programme), with the aim to build cybersecurity solutions for sectors such as energy, health, transport and finance. The initiative hopes to trigger as much as €1.8 billion in private sector investment.[226] At the national level, the UK government has an active program in place that supports the development of cybersecurity start-ups.

223 "Connecting Europe Facilities — Cybersecurity Digital Service Infrastructure," Digital Single Market, April 2, 2016, https://ec.europa.eu/digital-single-market/en/news/connecting-europe-facilities-cybersecurity-digital-service-infrastructure.

224 European Political Strategy Centre, European Commission, "Building an Effective European Cyber Shield."

225 "SoSo: Cybersecurity for SMEs, Local Public Administration and Individuals | Ideal-Ist," August 25, 2016, https://www.ideal-ist.eu/ps-es-101370; European Commission, "A Guide to ICT-Related Activities in WP2016-17," July 25, 2016.

226 European Commission, "EU Cybersecurity Initiatives - Working towards a More Secure Online Environment."

To this end, the government dedicated £4 million for a competition that will help SMEs develop ideas for countering cyber threats.[227] For victims of cybercrime and fraud, it established the Economic Crime Victim Care Unit (ECVCU) which offers support and advice.[228] Similar initiatives exist throughout Europe, but a noticeable trait of these programs is that the investments do not scale favourably with the rising costs of cybercrime, and, on the whole, do not meet the needs of the private sector.

5.1.3 Absence of national educational programs

Educational programs form the foundation of a stable influx of specialists for the cybersecurity market. ENISA research on cybersecurity education found two significant bottlenecks that limit workforce availability.[229] First, cybersecurity is mostly taught at a graduate level, while undergraduate programs remain very scarce across the EU. Second, most cybersecurity courses are offered in the discipline of computer science. As a result, cybersecurity remains underrepresented in other non-technical educational programs. The rising demand for managerial and interdisciplinary cybersecurity positions, coupled with the lack of specific courses tailored for those positions is creating a job gap within the EU that the private sector will find increasingly challenging to fill.

5.1.4 Discrepancies in threat intelligence sharing policies

Cyber threat intelligence sharing is often discussed and encouraged but rarely enforced and put into practice. ENISA distinguishes between three types of approaches to share information on cybersecurity incidents that have been observed in Europe: 1) traditional regulation; 2) alternative forms of regulation, such as self- and co-regulation; and 3) the remaining approaches enabling information sharing, such as education and information schemes.[230] Regulatory and non-regulatory approaches vary from one member state to another, and are each associated with different challenges. Numerous information sharing initiatives coexist but are often limited in scope and reach. For example, initiatives such as the EU-level Distributed Energy Security Knowledge (energy sector) and UK's Transport Sector Information Exchange (transportation) focus only on intra-sector information sharing, while other initiatives such as the Belgian Cybersecurity Coalition and the Austrian Trust Circle reflect cross-sector collaboration, albeit limited to the national level.[231] In light of this organizational complexity, ENISA recommends that EU and national policy makers leverage existing regulatory initiatives as opposed to enacting new ones.[232]

227Ashford Warwick, "New Government Plan to Support Cybersecurity Startups," ComputerWeekly.com, January 27, 2016, http://www.computerweekly.com/news/4500271901/New-government-plan-to-support-cyber-security-startups.

228 "Economic Crime Victim Care Unit (ECVCU)," Text, Action Fraud, October 13, 2016, https://www.actionfraud.police.uk/support-and-prevention-economic-crime-victim-care-unit.

229 Vishink & Heisel (2015) quoted in: Rademaker et al., "Dutch Investments in ICT and Cybersecurity - Putting It in Perspective," 35–37.

230 ENISA, "Cybersecurity Information Sharing: An Overview of Regulatory and Non-Regulatory Approaches," December 2015, 6.

231 ENISA, 23.

232 ENISA, 7.

5.1.5 Vulnerability disclosure debate

'Vulnerability disclosure' refers to the process of information sharing of software and system vulnerabilities so that they can be fixed or at least mitigated.[233] Particularly critical are 'zero-day vulnerabilities' – software vulnerabilities for which no patch or fix is yet available.[234] Taking into account that the average period of time before the vulnerability is discovered is 6.9 years, there is a strong incentive for governments to keep them hidden, whether for offensive or defensive purposes. This knowledge is of critical importance for private companies that may be using software from affected providers. The importance of introducing a coordinated vulnerability disclosure (CVD) process in Europe is already a topic of discussion in policy circles but EU Member States have taken only small steps toward the implementation of this process in practice. The 2016 CVD Initiative launched in Amsterdam is a step in the right direction, but it is currently limited in size and consists primarily of Dutch companies.[235]

5.1.6 GDPR-related bottlenecks

The upcoming General Data Protection Regulation (GDPR) could significantly impact the cybersecurity of the private sector. First, complying with the GDPR is viewed as a costly endeavor. According to Accenture's estimates, complying with all rules and regulations can add up to a once-off investment of €5 million, and an additional million per annum on 'maintenance'.[236] Although the costs for SMEs will not be as high as for large enterprises, they can reach as much as €1 million.[237] In addition to financial strain, global research commissioned by Veritas Technologies found that many organizations do not have proper technology to address the regulations (32%), nor do they feel confident that their organization is able to accurately identify and locate relevant data (39%).[238] This is compounded by a general lack of awareness with 42% of respondents stating that they do not have a way to determine which data should be saved.[239] As a result, 86% of organizations are concerned that non-compliance and subsequent penalties incorporated into the GDPR could have a major negative impact on their business, and could result in layoffs, reputational damage and loss of customers.[240]

233 CEPS, "Software Vulnerabilities Disclosure: The European Landscape," Centre for European Policy Studies, July 31, 2017, https://www.ceps.eu/publications/software-vulnerabilities-disclosure-european-landscape.

234 Andy Bogart and Lillian Ablon, "Zero Days, Thousands of Nights The Life and Times of Zero-Day Vulnerabilities and Their Exploits" (RAND Corporation, n.d.), 9.

235 Global Forum on Cyber Expertise, "Coordinated Vulnerability Disclosure - Initiative," www.thegfce.com, September 16, 2015, https://www.thegfce.com/initiatives/r/responsible-disclosure-initiative-ethical-hacking.

236 Inge Abraham, "How General Data Protection Regulation Can Unlock Value," Accenture Insights, February 24, 2017, https://www.accenture-insights.nl/en-us/articles/gdpr-general-data-protection-regulation-opportunities.

237 Abraham.

238 Veritas, "2017 VERITAS GDPR REPORT," 2017.

239 Veritas.

240 Veritas, 2.

5.1.7 Lack of trust between the public and the private sector

Lack of trust to share information constitutes a bottleneck both from an external, public policy perspective, and from internal, company perspective (addressed later in this report). Governments throughout Europe remain hesitant to work with ICT enterprises, fearing that businesses will pursue their own commercial interests, party preferences, lobbying activities, or put pressure on governments in the areas where their interests do not align.[241] Businesses, in turn, are hesitant to share information with the government because of its police and oversight functions, as well as for fear of punishment.[242] Fear of adverse media coverage constitutes yet another reason why companies are wary of exposing sensitive information to the public.

5.2 Internal/company perspective

5.2.1 General lack of awareness

Despite the complexity and scale of the cyber threat landscape, organizations' knowledge and awareness of cybersecurity issues remains limited. As the former director of Cisco Systems John Chambers stated, "there are two types of companies: those that have been hacked and those who don't know they have been hacked".[243] A survey conducted by Marsh revealed that as much as 69% of European companies have either no or only basic understanding of their exposure to cyber risks. Moreover, 60% of companies had never estimated the potential financial losses from a major cyber attack.[244] In addition, a recent Eurobarometer survey revealed that 51% of European citizens do not feel well informed about the risks of cybercrime activity.[245] The human factor can pose a significant risk within an organisation, as the majority of breaches are caused by negligence or human error – both intentional and unintentional.

5.2.2 Lack of skills and training

In addition to the lack of awareness, cyber education is another aspect that is often overlooked. Digital competencies are key to ward off cyber attacks. A lack of expertise will always hamper the ability of computer users to protect themselves. Securing well-qualified employees is thus regarded as a necessity for a company's survival. The European private sector currently faces shortages of digital skills: the available supply of highly-skilled ICT personnel is declining, and the gap is predicted to reach 755,000 potential vacancies by 2020.[246] While multinational enterprises can cope with scarcity of skilled personnel by relocating operations or attracting professionals from another country, this is

241 Interview with Mr. Arie van Bellen (ECP), 24 October 2017.

242 Interview with Mr. Arie van Bellen (ECP), 24 October 2017.

243 Kerravala, "John Chambers' 10 Most Memorable Quotes as Cisco CEO."

244 Marsh, "Continental European Cyber Risk Survey: 2016 Report," October 2016, 7.

245 European Commission, "Special Eurobarometer 464a Europeans' Attitudes towards Cybersecurity," September 2017.

246 Husing, Korte, and Dashja, "Trends and Forecasts for the European ICT Professional and Digital Leadership Labour Markets (2015-2020)," 23.

not possible for SMEs.[247] In addition to ICT professionals, there is also a shortage of cyber experts in academia and civil society, who would be responsible for educational and training activities. Where training is available, its focus and level differs across borders. Hiring and retaining skilled ICT professionals, sensitizing private users, and offering basic training to employees and public officials alike would yield positive results. Cyber education should begin at the grade-school level and expand into life-long learning provided by enterprises.

5.2.3 Inadequate cybersecurity spending

The availability of the necessary funding and equipment constitutes another challenge in implementing cybersecurity practices. In spite of potential losses, companies are not earmarking sufficient budgets for cyber protection. This is directly associated with the lack of cyber-security awareness among board members, who are responsible for the resource allocation decisions. Although European cybersecurity budgets have been on the rise, recording $22 billion in 2016,[248] lack of investment and of available funding is of particular concern for SMEs. SMEs generally lack awareness of available funds and subsidies, and avoid complex bureaucratic procedures for obtaining them.[249] Many small and midsized companies are linked to larger companies through their supply chains. To make the system as a whole more secure, it is not sufficient that only large companies spend more on their cybersecurity. The real issue that needs to be addressed first is the limited recognition of the *need* to invest in cybersecurity.

5.2.4 Corporate under-reporting

Lack of information sharing and incident reporting represents a major obstacle towards understanding and tackling cyber threats. Cyber attacks often inflict financial repercussions and reputational damage, which is why companies show reluctance to share information about the number of attacks and the extent of losses incurred. This is particularly true for those enterprises whose business models are built around trust in the protection of private data. Other forms of corporate under-reporting include unwillingness of IT management teams to inform senior management; lawyers discouraging their clients from reporting; or the lack of knowledge about who to turn to in the event of an attack.[250] To date, very few European companies have publicly acknowledged a cyber threat. This is partly due to the fact that, in contrast to the US, there is currently no provision at the EU level requiring companies to disclose cyberattacks. The entry into force of both the NIS Directive and the GDPR as of May 2018

247 "10 Ideas for the Future of Europe's Digital Economy - 'SMEs as the Engines of Digital Change'" (European Digital SME Alliance, March 11, 2016).

248 According to a survey conducted by PwC, the European cybersecurity market of products and services protecting companies from cyber breaches was worth $22 billion in 2016, and is expected to grow at 8% p.a. To 2018. See: PwC, "Cybersecurity: European Emerging Market Leaders," 4.

249 Interview with Mr. Fabio Guasconi, Digital SME Alliance, 30 October 2017.

250 European Political Strategy Centre, European Commission, "Building an Effective European Cyber Shield," 4.

will mandate that the breaches are disclosed and, by extension, increase public awareness of data breaches.[251]

5.2.5 Lack of awareness about the implications of the GDPR

According to the results of Symantec's State of European Data Privacy Survey, published in October 2016, a large number of companies remain unaware of the new regulation and its implications, and are underprepared for its implementation. By the end of 2016, 96% of the surveyed companies lacked comprehension of the GDPR.[252] Only 22% of businesses considered compliance a top priority in the period leading to GDPR's entry into force. The Symantec survey also revealed a lack of confidence in meeting the May 2018 deadline: of those surveyed, 91% of companies expressed concerns about their *ability* to become compliant, while nearly a quarter (23%) confirmed their organization will not meet the requirements in time, or only partly.[253] A more recent survey conducted in June 2017 found that only 2% of surveyed European organizations feel "fully prepared" for GDPR.[254] Top concerns of EU respondents were that the steps to comply with GDPR are not clear (37%), lack of awareness among management regarding the impact of the new regulation (37%), the potential of fines (29%) and the subsequent increase in complexity of the IT market (27%).[255] Even though companies in some countries appear to be more aware of the upcoming regulation than elsewhere, interviews conducted for the purpose of this study revealed that increased awareness does not always translate into action. Although hiring privacy consultants could help companies comply with GDPR, SMEs often lack financial resources for these services.[256]

5.2.6 Lack of detection capabilities

Unawareness of breaches due to inadequate detection capabilities is often the cause of corporate under-reporting. While many types of breaches take weeks or months to detect, a fair number may never be detected at all.[257] SMEs, in particular, have low levels of cyber protection. Lacking financial instruments, a large portion of SMEs are only able to fend off truly existential threats by means of relatively basic controls.[258] In the face of budget constraints, both large and small companies have to prioritize between investing in detection mechanisms and response capabilities.

5.2.7 Technological vulnerability

251 European Political Strategy Centre, European Commission, 4.

252 Symantec, "Businesses Underprepared for GDPR | Symantec."

253 Symantec.

254 Spiceworks Inc, "Many Companies Unprepared for GDPR Compliance Deadline in 2018," June 27, 2017, https://community.spiceworks.com/research/gdpr-impact-on-it.

255 Spiceworks Inc.

256 Interview notes.

257 European Political Strategy Centre, European Commission, "Building an Effective European Cyber Shield," 4.

258 Deloitte, "Dealing Efficiently with Cybercrime - Cyber Value at Risk in The Netherlands 2017."

Businesses across Europe are reliant on externally-developed technologies (software, hardware, and services). Most software and hardware is built outside the EU. The largest global suppliers and companies managing data flows originate in the US, while China's role in this domain is rapidly increasing. The European cyber industry remains fragmented and highly dispersed: as many as 600 small European companies provide support to public authorities and critical infrastructure in Europe.[259] In the absence of home-grown technologies, EU risks becoming excessively dependent on ICT produced outside its borders, as well as on security solutions developed elsewhere.[260] A certain degree of industrial autonomy in critical hardware, software and services is required to protect Europe's strategic interests. Complexity of IT processes and application of patches constitute other barriers to effective cybersecurity. Software updates are difficult for many. A typical SME in Europe relies on outdated legacy systems.[261] In the event it runs all year round, installing security updates would require stopping production, what can inflict additional costs.

5.2.8 Lack of incident response plans

The capacity of a company to respond to a cyber incident is contingent on two factors. The first is the existence of a formulated incident response plan (IRP). The second is regular updating and testing of such a plan. According to Pierre Audoin Consultants, nearly 40% of EU companies have no IRP in place and of those that do only 30% test and update them regularly (at a rate of more than once a month).[262] A Ponemon Institute study looking into cyber preparedness in Germany found that 79% of businesses reported they have either ad-hoc or no cyber-incident response plans.[263] In the UK Ponemon discovered that 43% of surveyed companies did not have an incident response plan, while 20% had informal or "ad hoc" ones. All in all, only 18% reported having a well-defined plan that is applied consistently throughout their entire enterprise.[264] Having such a dedicated incident response/crisis management plan has proven to have a positive effect when mitigating the operational, financial and reputational impact of a cyber attack.

5.2.9 Average detection times

The financial impact of cyber attacks increases with time. More rapid detection of data breaches is thus a key factor in minimizing not only data loss but also financial costs to businesses.[265] FireEye found that the time lag between cyber intrusions and their detection is estimated to be as much as

259 European Political Strategy Centre, European Commission, "Building an Effective European Cyber Shield," 5.

260 2013 Cybersecurity Strategy, quoted in: European Political Strategy Centre, European Commission, 5.

261 Europol-Enisa Conference Takeaways, 18-19 October 2017, The Hague, The Netherlands.

262 "Independent Study Reveals Incident Response Perception Gap Among EU Companies," IBM Resilient, June 1, 2015, https://www.resilientsystems.com/news-and-events/incident-response-press-releases/gap-among-eu-companies/.

263 "New Ponemon Institute Study Reveals Nearly 80 Percent of German Organizations Aren't Prepared for a Cybersecurity Incident," IBM Resilient, February 3, 2016, https://www.resilientsystems.com/news-and-events/incident-response-press-releases/new-ponemon-institute-study-reveals-nearly-80-percent-german-organizations-arent-prepared-cyber-security-incident/.

264 Ponemon Institute, "The Cyber Resilient Organisation in the United Kingdom: Learning to Thrive against Threats," January 2016, 8.

265 Kaspersky Lab, "Measuring Financial Impact of IT Security on Business - IT Security Risks Report 2016."

three times longer in the EU than elsewhere in the world. The EU's mean 'dwell time' – or the time between a compromise and its detection – is 469 days (approximately 15 months), in comparison to a global average of 146 days.[266] Dwell times of this length allow outside intruders the opportunity to develop multiple entry and exit doors, and can result in repeated breaches.[267]

5.2.10 Lack of trust to share information

Lack of trust is regarded as the number one inhibitor of cross-sector and cross-border collaboration. Intense competition and mistrust of company rivals often prevents information exchange and cooperation among different stakeholders.[268] In the face of mounting cyber threats, businesses are concerned that news of cyber intrusions could give their rivals a competitive advantage.[269] Currently, information sharing is often done informally, on an ad-hoc basis.[270] Naturally this makes it harder to coordinate an effective response to cyber incidents and hampers information exchanges both within and across borders. In contrast with large enterprises, SMEs often lack sufficient levels of information security to share threat intelligence information altogether. Often times, they merely react to events, without properly managing the threat intelligence information. A minimum level of information security management maturity must be reached before threat intelligence sharing activities can be pursued.[271]

5.2.11 Organisational design

In most cases, cyber risk continues to be regarded as a technical issue, rather than a business one. As a consequence, cybersecurity strategies remain confined to IT departments, with little involvement of senior management. According to the 2016 Marsh Continental European Cyber Risk Survey, this is the case in as many as 68% of surveyed companies across Europe.[272] Although they are well disposed to implement cybersecurity strategies, IT departments are not in a position to determine elements critical to business continuity or the potential financial and operational impacts a cyber incident could have.[273] Smaller companies, especially micro-enterprises, tend to have an informal organisational structure in place. Due to limited resources – both financial and human – they exhibit little specialization of roles and functions, and an 'everyone-does-everything' mindset.[274] Centering

266 "FireEye - Marsh & McLennan Cyber Risk Report 2017 - Cyber Threats: A Perfect Storm About to Hit Europe?," 10.

267 "FireEye - Marsh & McLennan Cyber Risk Report 2017 - Cyber Threats: A Perfect Storm About to Hit Europe?," 10.

268 George V. Hulme, "Tackling Cybersecurity Threat Information Sharing Challenges," CSO Online, January 17, 2017, https://www.csoonline.com/article/3157540/security/tackling-cybersecurity-threat-information-sharing-challenges.html.

269 Drjim, "When It Comes To Cyber Threats, CIOs Don't Like To Share," The Accidental Successful CIO, November 11, 2015, http://theaccidentalsuccessfulcio.com/security-2/when-it-comes-to-cyber-threats-cios-dont-like-to-share.

270 Nick Ismail, "Sharing Cyber Threat Intelligence Is Necessary to Combat Data Theft," Information Age (blog), August 16, 2017, http://www.information-age.com/sharing-cyber-threat-intelligence-necessary-combat-data-theft-123467953/.

271 Interview with Mr. Fabio Guasconi, Digital SME Alliance, 30 October 2017.

272 Marsh, "Continental European Cyber Risk Survey: 2016 Report," 5.

273 Marsh, 5.

274 "European Cybersecurity Strategy: Fostering the SME Ecosystem."

multiple functions in one single person, most often the company owner, can result in lower cyber preparedness levels. The average age of directors is also of relevance, as older board members generally find new technologies intimidating and may prefer to channel ICT-related issues towards IT departments.[275]

5.2.12 Cyber interdependence

According to the WEF, the rising cyber interdependence of infrastructure networks constitutes one of the world's top risk drivers.[276] Europe has a long-standing history of interdependence among countries' critical infrastructures, the vast majority of which are privately owned and maintained. Since 2000, 501 of 1749 incidents of critical infrastructure failure were caused by infrastructure failures in other sectors. 76 of those 501 incidents resulted from a second cascade, what means that the failure in one service triggered a failure into a second service, which triggered a failure in a third.[277] A cyber incident can cascade and have a cross-industry and cross-border impact on critical infrastructure, what requires greater regional and inter-industry coordination on cyber defense and crisis management on critical infrastructure.

275 Interview with Mr. Arie van Bellen (ECP), 24 October 2017.

276 The 2017 WEF Global Risks Report, quoted in: PwC, "Strengthening Digital Society against Cyber Shocks," 2017.

277 Luiijf et al. as quoted in: Philip Chertoff, "Good Neighbours Make Good Security: Coordinating EU Critical Infrastructure Protection Against Cyber Threats" (GLOBSEC Policy Institute, August 28, 2017), 6.

6. Good practices and lessons learned

Numerous good practices to improve cybersecurity of businesses across the EU have been put in place. These include public-private partnerships, educational and training activities (both public and private), challenges, competitions, hackathons and prizes, cyber insurance uptake, and the formation of cyber communities as a form of collective cyber defense. These provide good examples for corporate Europe to follow. Nevertheless, it has been observed that good practices often come after a company suffers damages, rather than being proactive in nature.

6.1 Public-private partnerships

It has been widely agreed that dealing with a cyber attack effectively requires speed and agility, which necessitates a deeper level of integration between parties affected. A very powerful tool that has the ability to combat a wide variety of threats can be found with the coming together of both private and public actors. This tool extends particularly into the cyber world, especially within the context of market-oriented economies where the private sector is the harbinger of innovation. The existence and strength of public-private partnerships (PPPs) is vital when resisting a cyberattack.

The intersection between public and private actors is made more important due to characteristics within the cyber industry. The private sector controls much of the critical infrastructure that is vulnerable to cyber threats, and as a result, many private entities have developed their own cybersecurity programs and have intimate knowledge regarding the cybersecurity landscape. In addition, private entities are very capable in mustering more cyber expertise, and more rapidly, compared to their public counterparts. This is even more accentuated the smaller the target country is. The public sphere has large resources and can facilitate the transfer of information from other states, and maintains the responsibility as the principal security provider against top-level threats, especially if these emanate from nation states.[278]

Throughout the world, public-private partnerships exist in varying forms, with varying degrees of integration between both actors. Provan and Kenis (2008) briefly outline three basic theoretical models of network governance that can be transposed into the cyber sphere. The first model emphasizes ‘shared governance’ by the network members themselves, and is characterized by the equality of members and high levels of trust within the networks. The second model, termed as a lead-organization model uses a more centralized and hierarchical approach. Finally, the third model, the network administrative organization, involves a separate and external entity to specifically govern the network’s activities. While these three models are theoretical ideal types, they serve well to frame the varying forms of PPPs in the cyber sphere.[279]

278 Sergei Boeke, “National Cyber Crisis Management: Different European Approaches,” Governance, September 2017, 1–16.

279 Keith G. Provan and Kenis Patrick, “Modes of Network Governance: Structure, Management, and Effectiveness,” Journal of Public Administration Research and Theory, August 2, 2007, 229–52, https://doi.org/10.1093/jopart/mum015.

In a very broad sense, the cybersecurity PPP practices of certain European countries can be aligned with the three models described above. As will be explored in more detail later on in the text, the Dutch execution of a PPP is closest to the participant-governed model as exemplified by the closeness and trust between institutions and the private sector, along with the fact that private participation is entirely voluntary. Estonia and the Czech Republic rather use coordinating authorities to set standards and enforce them accordingly. Within both these countries, participation by the private sector is ensured rather than voluntarily provided. Thus, Estonia and the Czech Republic rely on a more hierarchical format and thus their execution of PPPs is more closely aligned with the network administrative organization model. Finally, the Danish model implies a strong lead agency model due to the central monitoring task and regulatory role of the Danish authorities.

Regardless of the form of a PPP, the benefits of a strong public and private partnership to tackle cyber threats cannot be understated. Cooperation between private and public agencies can draw from strengths that each player possesses which are often complementary.[280] Public and private partnerships can also help foster trust between the two sides, an element that is vital when responding to cyber threats, whether they are internal or external.

6.1.1 The Case of the Netherlands

The Netherlands provides a strong case of voluntary involvement of the private sector when dealing with cyber threats. Dutch public-private partnerships revolve around the National Response Network (NRN) that links both private and public organizations on a voluntary basis. The NRN facilitates cooperation in times of crises, and is meant to act akin to a 'bucket brigade' that channels aid to where it is needed. This voluntarily based network model facilitates information sharing between both spheres, leading to the creation of 14 different Information Sharing and Analysis Centers (ISACs), each centering around a specific sector, such as energy or finance. The National Cybersecurity Centre (under the Ministry of Justice and Security) functions as a secretariat in this hub-and-spoke model, coordinating the 14 ISACs for different sectors.[281]

The separation from the intelligence communities and the ISACs helps foster information sharing and trust between the public and private sectors, though it should be noted that companies nonetheless sometimes chose to meet without government officials present. Information sharing within individual members of the private sector, as well as information sharing between the private and public sectors is fairly streamlined, though sharing within the public sphere is still hampered by a fragmented institutional landscape.

Another key element of the Dutch PPP strategy is the widespread use of the Coordinated Vulnerability Disclosure (CVD) Manifesto, which is a public-private initiative with over 30

280 Boeke, "National Cyber Crisis Management: Different European Approaches."

281 Netherlands National Cybersecurity Centre, "ISAC's," National Cybersecurity Centre - Ministry of Justice and Security, accessed September 20, 2017, https://www.ncsc.nl/english/Cooperation/isacs.html.

participating enterprises[282]. Participants to the Manifesto declare to implement a series of measures that allows ethical hackers to disclose IT system vulnerabilities in a legal and responsible way. The Manifesto is accommodated by the Global Forum on Cyber Expertise, whose secretariat is publically funded.

The National Cybersecurity Center (NCSC), established in 2012 as the result of the first national cybersecurity strategy, acts as a central node, allowing it to facilitate cooperation, but not directly impose it. The Dutch have also made great efforts to decentralize the ability to make sense of a crisis through the use of IT expertise. Though this has the potential to develop a sense of uncertainty concerning a concrete decision making process during crises, it has led to the idea that all relevant public and private actors are entitled to 'a seat at the table', with responsibilities becoming more and more clear as a cyber crisis unfolds[283].

6.2 Training and education

Various educational activities, both public and private, have been put in place across the EU to increase the supply of highly qualified ICT professionals, including cybersecurity specialist and data experts.

6.2.1 Public Educational Activities

European cybersecurity month (ECSM) provides a good example of an effective EU-wide educational initiative aimed at improving cybersecurity across the EU. Each October, the European Union Agency for Network and Information Security (ENISA), the European Commission DG CONNECT and Partners cooperate to deploy an awareness campaign that promotes cybersecurity among organizations and individual citizens alike. Through education and sharing of good practices, the campaign highlights the simple steps that can be taken to protect data, whether financial, personal and/or professional.[284]

In 2015 and 2016, the eSkills for Jobs campaign took place, organized by the European Commission.[285] The campaign was later replaced by the Digital Skills and Job Coalition, which brings together Member States, corporations, non-profit organizations, social partners and educational providers in order to tackle the lack of digital skills in Europe.[286] Once an organization, business or government body becomes a member of the coalition and endorses its Charter, it is encouraged to

282 Boeke, "National Cyber Crisis Management: Different European Approaches."

283 Boeke.

284 "What Is ECSM? — ECSM," Cybersecuritymonth.eu, accessed November 3, 2017, https://cybersecuritymonth.eu/about-ecsm/whats-ecsm.

285 "More ICT Campaigns — ECSM," Cybersecuritymonth.eu, accessed November 3, 2017, https://cybersecuritymonth.eu/about-ecsm/more-ict-campaigns.

286 European Commission, "The Digital Skills and Jobs Coalition," Digital Single Market, accessed November 3, 2017, https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition.

make a concrete commitment to carry out actions ('pledges') that would contribute to reducing the digital skills gap in Europe. The 'pledge' should address the shortage of digital skills within one of the four target groups: the citizenry in general, the labor force, ICT professionals and educators.[287] A special emphasis is placed on stimulating interest in digital skills among women and girls.[288] The goals of the coalition are to train one million young unemployed people for digital jobs by 2020, to support SMEs, modernize education and training for digital skills and to support other digital skill initiatives.[289]

Europe Code Week is exemplary of the initiatives supported by the European Commission as part of its Digital Single Market strategy. It aims to expand knowledge of programming among all age groups by stimulating bottom-up engagement.[290] This is done by providing toolkits, presentations and resources in local languages that volunteers, or 'Code Week Ambassadors', (schools, teachers, libraries, code clubs, businesses and others) can use to organize a coding event that is subsequently promoted on the Code Week website. With close to one million participants across fifty countries, EU Code Week is a cost-effective way of improving digital literacy.[291]

At the international level, the U.S. National Cybersecurity Alliance (NCSA) driven STOP. THINK. CONNECT.™ campaign was developed to help all Internet users keep their personal information, data, communications, and transactions more secure and safer online.[292] Created by a coalition of government, industry and nonprofit organizations, STOP. THINK. CONNECT allows organizations to register as partners and gain access to a library of educational materials on cyber hygiene, account and password security, common cybercrime techniques and other basic internet security-related knowledge.

At the Member State level, ENISA's up to date database of courses and certification programmes linked to Network and Information Security lists a total of 528 courses across 29 countries (most EU Member States, Switzerland, Norway and Serbia).[293] The figure includes both undergraduate and graduate courses, the overwhelming majority (521) of which are traditional university courses, with a few (7) offered online. The United Kingdom has the second largest number of courses on offer (92) and it has implemented a solution to filter out and promote the best among them. This is done through certification by the National Cybersecurity Centre (NCSC), which forms part of the UK's intelligence

287 European Commission, "Pledges for Action," Digital Single Market, accessed November 3, 2017, https://ec.europa.eu/digital-single-market/en/pledges-action.

288 European Commission.

289 European Commission.

290 "Europe Code Week 2017 - Europe Code Week," codeweek.eu, accessed November 3, 2017, http://codeweek.eu/.

291 "Europe Code Week 2017 - Resources and Guides," codeweek.eu, accessed November 3, 2017, http://codeweek.eu/resources/; "Europe Code Week 2017 - About EU Code Week," codeweek.eu, accessed November 3, 2017, http://codeweek.eu/about/.

292 "More ICT Campaigns — ECSM."

293 "Education Map - ENISA."

establishment. As of October 2017, it has certified 25 graduate and 2 undergraduate degrees.[294] The NCSC has also set up the 'Cybersecurity Body of Knowledge' project, which aims to codify the knowledge underpinning the profession, giving structure to core topics and reference texts.[295] Recognizing that the heavy reliance on certifications and qualifications cannot help fill the widening cybersecurity job gap, the UK government has started the 'HMG Cyber Schools Programme' intended to train secondary school level students the basics in "digital forensics, defending web attacks, programming and cryptography".[296] This is indicative of an overall trend within the UK, in which public initiatives are striving to foster interest in cybersecurity from an early age in order to stimulate growth of the cyber workforce.

6.2.2 Private Educational Activities

By means of certifications, courses, on-the-job trainings and consultancy services, the private sector plays an important role in educating cybersecurity specialists. Deloitte, one of the 'Big Four' accounting firms, offers a good example of cyber-consultancy and training services provided by the private sector. The company's EMEA Cyber Academy provides technical cybersecurity courses and (non-technical) awareness training, while its Cybersecurity Learning program offers a variety of ISACA certified Management and Hacking courses.[297] Most of the organizations providing certifications for cybersecurity professionals (ICS2, EC Council, CompTIA etc.) are based in the United States.[298]

Given the fact that the majority of attacks occur as a result of negligence, employee training for cyber hygiene and awareness also plays an important part in shoring up an organization's cyber defence.[299] As there is no standard approach to cyber hygiene across Europe, the programs currently in place such as the "Belgian Cybersecurity Guide" and the "Cyber Essentials" of the UK government are usually derived from the National Cybersecurity Strategies of individual Member States.[300] "Cyber Essentials" define a number of technical controls and requirements an organization needs to meet in order to be considered 'secure'. Upon implementation of these requirements a certification body

294 National Cybersecurity Centre, "NCSC-Certified Degrees - NCSC Site," NCSC.gov.uk, September 8, 2017, https://www.ncsc.gov.uk/information/ncsc-certified-degrees.

295 Cybok, "The Cybersecurity Body Of Knowledge," cybok.org, accessed November 3, 2017, https://www.cybok.org/.

296 Matt Burgess, "UK Gov Wants Teens to Practice Cybersecurity in Their Spare Time," WIRED UK, June 26, 2017, http://www.wired.co.uk/article/cyber-skills-uk-cybersecurity-skills-shortage.

297 ISACA is one of a number of international bodies providing certifications for cybersecurity professionals.Deloitte, "Deloitte EMEA Cyber Academy Cyber Training, Education and Awarenesss," 2017.

298 "7 Top Security Certifications You Should Have in 2017," InfoSec Resources, October 13, 2017, http://resources.infosecinstitute.com/7-top-security-certifications-you-should-have/.

299 "Cybersecurity Boost for UK Firms - GOV.UK," gov.uk, January 16, 2015, https://www.gov.uk/government/news/cyber-security-boost-for-uk-firms.

300 ENISA, "Review of Cyber Hygiene Practices" (Heraklion, Greece: European Union Agency For Network and Information Security, December 2016), 7.

assesses compliance and a "Cyber Essentials" certificate is awarded.[301] There are two levels of certification: the "regular", in which an organization self-assesses its systems and this assessment is independently verified, and a "plus" certification in which the organization's systems are independently tested.[302] However, a recent ENISA study found that these programs suffer from low levels of adherence: "cyber hygiene [...] is generally quite low priority for most businesses unless there is a pressing, external, need to comply (such as) business to business contract terms and governmental regulations". [303]

The majority of successful educational/training initiatives currently take place at the associational level. In 2016, the European SME Alliance, which represents around 20,000 small and medium sized IT companies across the EU, launched the #DigitalSME4skills campaign. The aim of the campaign is to enhance digital skills of the workforce and to offer highly skilled professionals to all industry sectors.[304] The campaign will engage hundreds of digital SMEs, which will offer work experience schemes (such as internships, traineeships and apprenticeships) to those who sign up for the program. The type of acquired skills will depend on the participant's profile, as well as on the company's specialization. It is estimated that by 2019, the program will address as many as 5000 people. The number of impacted people could be even higher: positive publicity for companies engaged in the program is expected to trigger a network effect and create a peer-to-peer pressure on other companies.[305] The campaign is proving successful, particularly when cost/effectiveness ratio is considered.[306] In addition to enhancing workforce digital skills, Digital SME Alliance is partnering with education providers and other GDPR experts in order to offer its members trainings and advice on GDPR compliance.[307]

DigiDuck, a special edition of the Donald Duck magazine presented during the 2015 Global Conference on CyberSpace, constitutes another example of a successful initiative to enhance cybersecurity awareness among children, professionals and the general public. The booklet, distributed in over 300,000 copies, provides hints and tips on the safe use of the Internet and social media. It also gives a brief overview of examples of collaborative efforts that can make people safe online.[308] DigiDuck was considered as a successful initiative introducing ICT and programming to children at a young age. This initiative was a result of a collaborative effort itself. It came about as a joint initiative of the Dutch Electronic Commerce Platform (ECP), Ministry of Economy, Ministry of Justice and Security and Sanoma Media.

301HM Government, "Cyber Essentials - OFFICIAL SITE," cyberaware.gov.uk, 2016, https://www.cyberaware.gov.uk/cyberessentials/faq.html.

302 HM Government.

303 ENISA, "Review of Cyber Hygiene Practices," 5.

304 European Commission, "Pledge for the Digital Skills and Jobs Coalition," Digital Single Market, accessed November 3, 2017, https://ec.europa.eu/digital-single-market/en/pledge-for-digital-skills-jobs-coalition.

305 European Commission.

306 Interview with Mr. Fabio Guasconi, 30 October 2017.

307 Interview with Mr. Fabio Guasconi, 30 October 2017.

308 "DigiDuck – Safer Online | GCCS 2015," gccs2015.com, accessed November 3, 2017, https://www.gccs2015.com/nl/node/556.

6.3 Challenges, competitions, hackathons and prizes

Hosting cybersecurity challenges and competitions is a strategy that has been embraced by both the private and the public sector. This approach can yield significant benefits. Firstly, on a national level, it helps to increase the pool of ICT talent, stimulate interest in cybersecurity and combat the shortage of e-skills. Secondly, it provides the cybersecurity industry an advertising platform and a means to come into contact with potential future employees. Over time, these events have evolved to take a variety of forms, namely hackathons, competitions and conferences, with a significant amount of crossover between them.[309]

Cybersecurity competitions are specifically designed events that simulate the challenges of a working cybersecurity environment. Their aim is to help contestants network, share experiences and sharpen their skills. Cybersecurity competitions have been developed on both national and pan-European levels. The Cybersecurity Challenge UK provides a good example of the structure national competitions can take.[310] It offers an online platform (CyPhinx), in which prospective competitors can participate in specially designed cybersecurity challenges. At times, these challenges are used as qualifiers for 'face-to-face' competitions which can be both individual and group-based, and lead to the next 'Masterclass' stage of competition. The 'Masterclass Final' constitutes the highest competition level, simulating the demands of a typical cybersecurity working environment. In addition to these competitions there are also 'Cyber Games', a set of regional school competitions for 12-16 year olds, and 'Capture the Flags', which can be either 'Jeopardy' or 'Attack-defence' style.[311] Sponsors of these contests range from public institutions, state-controlled companies, major American and European defense companies, IT enterprises and educational institutions.[312]

The pan-European level is exemplified by the European Cybersecurity Challenge.[313] Organized by ENISA, it brings together winners of national competitions to solve challenges in web and mobile security, crypto puzzles, reverse engineering and forensics as well as network with potential employers.[314] The ECSC has the same goal as national competitions - to mitigate skills shortages by

309 It is not unusual for hackathons and conferences to have a competitive side-event or for competitions to include some sort of collaborative and/or presentation aspects, hence the "crossover".

310 Cybersecurity Challenge UK, "Competitions," Cybersecurity Challenge UK, accessed November 3, 2017, https://www.cybersecuritychallenge.org.uk/competitions.

311 Cybersecurity Challenge UK, "Masterclass," Cybersecurity Challenge UK, accessed November 3, 2017, https://www.cybersecuritychallenge.org.uk/competitions/masterclass; Cybersecurity Challenge UK, "Capture the Flag," Cybersecurity Challenge UK, accessed November 3, 2017, https://www.cybersecuritychallenge.org.uk/competitions/capture-the-flag.

312 Cybersecurity Challenge UK, "Sponsors," Cybersecurity Challenge UK, accessed November 3, 2017, https://www.cybersecuritychallenge.org.uk/sponsors.

313 "More ICT Campaigns — ECSM."

314 ENISA, "EU Cyber Challenge — ENISA," Topic, accessed November 3, 2017, https://www.enisa.europa.eu/topics/cybersecurity-education/eu-cyber-challenge; "European Cybersecurity Challenge ECSC 2018," accessed November 3, 2017, https://www.europeancybersecuritychallenge.eu/next.html.

targeting students, university graduates or even non-ICT professionals.[315] In 2018, the contest will feature fifteen European countries, each bringing their ten best cybersecurity talents.[316]

Conferences are primarily intended to disseminate up-to-date knowledge of relevant cybersecurity trends and often feature a competitive side event. The annual *"DefCamp"* hosted in Bucharest, Romania, combines a conference type event with a cybersecurity competition.[317] In a similar manner, the TROOPERS conference organized in March 2017 in Heidelberg, Germany, offered training workshops alongside lectures.[318] Conferences are the most common form of organization, followed by a smaller number of well-established cybersecurity competitions.

A hackathon is an event which brings together programmers, graphic designers, interface designers and other experts from the software industry to collaborate on various software related projects.[319] It may or may not pertain to cybersecurity. For example: *"What the Hack - The Hackathon against DDoS"*, organized by *NL-ix* in The Hague in 2017 brought together various IT specialists to build new software solutions for dealing with DDoS-related issues.[320]

All of these events have a tiered sponsorship structure, based on joint participation of public and private sector entities as regards their financing and organization. Private sector involvement is often irrespective of geographic location with mixes of international and European companies being the norm, which makes it difficult to differentiate exclusively 'European' initiatives.

6.4 Cyber insurance

Another part of the solution, adopted by an increasing number of companies, is to transfer the cyber risk to an insurer. Cyber-security insurance offers a way to protect businesses while preserving industry's ability to innovate. The past five years have witnessed advances in cyber insurance adoption rates. According to a survey conducted by Marsh, nearly half (47%) of the surveyed businesses either already purchased cyber insurance or are in the process of obtaining one.[321] The remaining 53% are believed to be lacking the necessary information to make a value-based judgment on the risk-transfer options currently available to them.[322]

315 "European Cybersecurity Challenge," accessed November 3, 2017, https://www.europeancybersecuritychallenge.eu/index.html.

316 "European Cybersecurity Challenge ECSC 2018."

317 "Hacking Village – DefCamp 2017," accessed November 3, 2017, https://def.camp/hacking-village/.

318 "TROOPERS 2017 – the 10th Anniversary!," accessed November 3, 2017, https://www.troopers.de/troopers17/.

319 The term "hackathon" originated in 1999 and represents a portmanteau of the words "hack" and "marathon", in which "hack" refers to writing programming code in general - not the colloquial reference to computer crime.

320 "What the Hack - The Hackathon against DDoS," accessed November 3, 2017, https://www.thehaguesecuritydelta.com/cyber-security/events/event/1559-what-the-hack-the-hackathon-against-ddos-2017-09-14.

321 Marsh, "Continental European Cyber Risk Survey: 2016 Report," 10.

322 Marsh, 10.

In terms of geography, regions with established cybersecurity-related legislation tend to have higher cyber insurance adoption levels than regions with recent or no legislation.[323] The United Kingdom, in particular, exhibits a higher level of maturity when compared to the rest of the region. In terms of company size, large companies are more likely to be insured than smaller ones, which often regard premiums as too high. In terms of sectors, financial services emerged as the most insurance-aware sector, followed by communications, media and technology, retail and – more recently – manufacturing.[324] Although cyber insurance experiences lower rates of adoption than other insurance sectors, the growth projections remain high. The global cyber insurance market is projected to reach $7.5 billion in annual sales by 2020 – tripling the 2015 amount – and over $20 billion by 2025.[325] The implementation of both the NIS Directive and the GDPR are expected to positively influence this growth.

Cyber insurance was developed in order to address risk that cannot be mitigated by security measures. Although it initially started in a limited form, it has developed to cover more and more types of cyber risk. The core coverage offered by most insurers today includes first and third party risk, as detailed below.

First party risk coverage	Data breach, data leakage, business interruption, cyber extortion
Third party risk coverage	Privacy liability, electronic media liability
Non-common coverage	Business revenue, digital assets disruption, non-intentional insider threat, intellectual property, reputational harms, and targeted attacks
Extra coverage	Forensics, fraud, legal costs, PR measures, and ransomware

Table 6: Categorization of cyber insurance coverage offered by most insurers[326]

Results of a survey carried out by Hiscox point to two big drivers that motivate companies to take out cyber insurance. The cost of a potential breach and the need for the peace of mind that protection brings constitute the first one. The second quoted factor is concern about data security.[327] Reasons for not taking out cyber insurance include scepticism and lack of trust that an insurer will pay out in the event of a cyber attack; perception that a cyber insurance policy is not relevant; lack of understanding regarding what cyber insurance is or what it would cover; belief that cyber cover is already provided as part of already existing insurance coverage.[328] The insurance industry needs to invest additional

323 ENISA, "Cyber Insurance: Recent Advances, Good Practices and Challenges — ENISA," Report/Study, November 7, 2016, https://www.enisa.europa.eu/publications/cyber-insurance-recent-advances-good-practices-and-challenges.

324 Marsh, "Continental European Cyber Risk Survey: 2016 Report," 10.

325 Quoted in: ENISA, "Cyber Insurance," 5.

326 ENISA, "Cyber Insurance."

327 Hiscox, "The Hiscox Cyber Readiness Report 2017," 20.

328 Hiscox, 20–22.

effort in instilling trust in its policies, delivering clarity over what is covered, simplifying the way coverages are written, and develop customised solutions for the SME market.[329]

6.5 Cyber communities as a form of collective cyber defence

Professional associations and collectivities provide venues for private companies to come together, share information and experience, pool knowledge and resources, and increase their resilience against cyber attacks.

At the national level, collaborative efforts such as the **Digital Trust Centre** (DTC) in the Netherlands are being set up to help bridge the aforementioned trust gap. Set in motion by the Ministry of Economic Affairs and the Ministry of Justice and Security, the DTC will help enterprises in the non-critical sector increase their cybersecurity. The Centre will do so by notifying, warning and advising in case of cyber attacks. For enterprises in critical sectors – such as telecommunications or energy – a similar knowledge center already exists: the National Cybersecurity Centre (NCSC), which also serves the needs of government organizations. SMEs currently lack such point of contact. The new DTC will start working in 2018, and in close collaboration with the NCSC. Although devised to serve the needs of SMEs, the DTC will place emphasis on partnerships and collaboration between SMEs, large organizations and associations.[330]

The **Hague Security Delta** (HSD) is the leading security cluster in Europe, consisting of 272 members, of which 240 are private companies.[331] The approach adopted by HSD revolves around the concept of 'Triple Helix Cooperation', which refers to the collaboration between the public and private sector and research institutions. The core idea behind this type of collaboration is that potential for innovation and economic development in modern societies lies in giving a more prominent role to universities, creating a new, hybrid, form of production.[332] Thus, through increased cooperation, all available skills and knowledge are put to use, leading to better outcomes.[333] A notable initiative launched by the HSD is the Security Operational Centre (SOC) association of several companies in the Netherlands that possess SOCs with the aim to encourage information exchange on cyber attacks among them.[334] HSD seeks to provide an objective and independent platform that helps build trust among association members.[335]

329 Hiscox, 1.

330 "Dutch Cabinet Invests 2.5 Million in New Digital Trust Centre," The Hague Security Delta (HSD), September 25, 2017, https://www.thehaguesecuritydelta.com/news/newsitem/947-new-cybersecurity-centre-for-entrepreneurs.

331 Interview with Mr. Richard Franken, HSD, 6 November 2017.

332 Triple Helix Research Group, Stanford University, "The Triple Helix Concept | Triple Helix Research Group," accessed November 14, 2017, https://triplehelix.stanford.edu/3helix_concept.

333 Hague Security Delta, "Triple Helix Cooperation," accessed November 14, 2017, https://www.thehaguesecuritydelta.com/market/triple-helix-cooperation.

334 Interview with Mr. Richard Franken, HSD, 6 November 2017.

335 Interview with Mr. Richard Franken, HSD, 6 November 2017.

At the European level, the **European Digital SME Alliance** brings together small and medium-sized enterprises working in the field of ICT. The Alliance is the result of a joint effort of 28 regional and national SME associations from EU Member States and neighboring countries, and it currently represents around 20,000 digital SMEs across the EU.[336] By means of trainings, seminars, digital skills campaign, and the sharing of knowledge, the Alliance not only helps strengthen Europe's cybersecurity industry, but it also creates new opportunities for SMEs that deliver innovative cybersecurity solutions, by promoting their work in the EU and global markets.[337] In order to facilitate SMEs' cybersecurity ecosystem, and to boost the offer and the demand for SMEs' cybersecurity solutions, the Alliance's next key proposals include the establishment of a European cybersecurity SMEs HUB to connect SMEs and foster their ad hoc cooperation on specific projects, and the development of territorial cooperation strategy to help SMEs access cybersecurity protection measures.[338]

The Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity (**Global EPIC**) was inaugurated in October 2017 in Krakow, Poland, with the goal to enable the development and sharing of new knowledge in the field of cybersecurity and, as such, to create economic, societal and technological impact across the globe. The overall aim of the Global EPIC is to strengthen collaboration between existing regional initiatives. It currently comprises 14 ecosystems from 10 different countries and 3 continents,[339] bringing together academia, industry and governments from all around the world to tackle cybersecurity challenges together. Global EPIC has set a target of 50 member cybersecurity ecosystems by October 2020, which reflects its ambition to build a global community collaborating on projects, sharing expertise, and creating solutions for both current and emerging cybersecurity challenges.[340]

336 "European DIGITAL SME Alliance," European Digital SME Alliance (blog), accessed November 16, 2017, https://www.digitalsme.eu/about/european-digital-sme-alliance/.

337 Justina Bieliauskaite, "DIGITAL SME President Oliver Grün Appointed SME Board Member at ECSO, the European Cybersecurity Organisation," European Digital SME Alliance (blog), July 12, 2016, https://www.digitalsme.eu/digital-sme-president-oliver-grun-appointed-sme-board-member-ecso-european-cyber-security-organisation/.

338 "European Cybersecurity Strategy: Fostering the SME Ecosystem | Cyberwatching," accessed November 16, 2017, https://www.cyberwatching.eu/news-events/news/european-cybersecurity-strategy-fostering-sme-ecosystem.

339 The 14 ecosystems are: bwtech@UMBC (Baltimore, U.S.A.), Centre for Secure Information Technologies – CSIT (Belfast, U.K.), Cyberspark (Be'er-Sheva, Israel), CyberTech Network (San Diego, U.S.A.), Cyber Wales (Cardiff, U.K.), Global Cybersecurity Resource – Carleton University (Ottawa, Canada), Innovation Boulevard (Surrey, Canada), INCYDE (Madrid, Spain), LSEC (Heverlee, Belgium), Politecnico di Torino (Turin, Italy), Procomer (Heredia, Costa Rica), The Hague Security Delta (The Hague, Netherlands), The Kosciuszko Institute (Krakow, Poland) and The Canadian Institute for Cybersecurity (CIC), University of New Brunswick (Fredericton, Canada).

340 Faculty of Humanities et al., "Launch of Global EPIC," PaCCS, accessed November 16, 2017, http://www.paccsresearch.org.uk/news/launch-global-epic/.

7. Conclusions and recommendations

7.1 Risk factors

As this study has shown, organizations find themselves in an increasingly complex cyber threat environment, having to face multifaceted cyber risks, both internal and external. Due to their potential to cause physical damage, operational disruptions, and reputational damage, cyber incidents should be judged as business risks. Malware and phishing constitute the most common type of threat encountered by companies across Europe. Although costs of a malware incident are relatively low in comparison to other types of attacks, its high rate of occurrence makes malware the most costly attack vector overall. Within the malware category, businesses across Europe should be particularly wary of emerging trends in ransomware attacks.

The staggering increase of Internet of Things (IoT) devices enabled sophisticated and tailor-made customer experiences, efficient business processes and innovative services. Without accompanying security measures, this development has resulted in increased DDoS attacks, in size, sophistication and frequency. Although DDoS most often target large organizations and digitized economies, inadequate mitigation strategies make SMEs and less digitized economies relatively vulnerable.

Although the number of data breaches – the third major threat category assessed in this study – has declined, the average size of data breach (number of records lost) is on the rise. Sensitive personal information – such as financial and health records – remains the key focus of cyber attacks.

Although all sectors are susceptible to cyber attacks, healthcare stands out in terms of its exposure. In contrast to financial services, the energy or the telecommunications sectors that have long been targeted by cyber attacks and have developed sophisticated defense mechanisms, healthcare lags in terms of its awareness of and preparedness for cyber attacks. The cybersecurity of the healthcare sector could be considerably strengthened through improved security hygiene, which includes backups and staff training, including against phishing scams. In addition to protecting patient health records, more focus ought to be paid towards medical devices. The Medical Devices Regulation (MDR), adopted in 2017, is important in this regard, as it enlarges the scope of applicable devices and defines more stringent post-market surveillance.[341]

In terms of company size, SMEs constitute the weak link in cyber attacks. They face rising threat levels, and pay the highest price for operating online. Despite growing threat levels, they remain ill-prepared for cyber attacks, showing lower than average maturity levels. SMEs struggle not only due to a lack of awareness, but also because they perceive cybersecurity as a costly endeavor. Being unable to fend off cyber attacks alone, SMEs and start-ups need to be included in the IoT ecosystem. Large companies have a role to play in increasing the cybersecurity of small enterprises in their supply chains. Governments, in turn, should put in place policies that stimulate SME cybersecurity,

341 European Commission, “Regulatory Framework - Growth - European Commission,” Growth, accessed November 20, 2017, /growth/sectors/medical-devices/regulatory-framework_en.

cyber skills and information exchange. As to the lack of funding, companies should consider funding as their own responsibility. Associations could be in charge of the pooling of resources.

Incoherence of methodologies, definitions and indicators of cost measurements make it difficult to determine the true economic cost of cybercrime. However, estimates indicate that indirect losses, such as reputational damage or loss of customer trust, tend to be much larger than direct costs and expenses for protection measures. Methodologies for cost calculations need to be improved.

7.2 Awareness and resilience

Governments play an important role in providing a secure business climate. This business climate, however, varies from one Member State to another. Our findings show that there is still a visible gap between countries in terms of knowledge, awareness and capacity to deploy strategies, programs and capabilities in the field of cybersecurity. While Estonia, France, Norway and the United Kingdom lead by example, countries of Southern and Eastern Europe – notably Slovenia and Slovakia – generally lag behind. The implications are twofold. First, heterogeneity of security and privacy regulations across the EU presents a hurdle to effective cross-border collaboration. Second, the fact that certain Member States lack the necessary capabilities to defend against emerging trends makes the European cybersecurity architecture disparate and vulnerable to potential attacks. Moreover, as our study has shown, there is a discrepancy between the growing digitization of society and resources spent on cybersecurity. Neither individual Member States, nor private enterprises seem to be backing their cybersecurity with appropriate resources.

The EU is an important initiator in this regard, as demonstrated by numerous actions, measures and initiatives that have been put in place to improve cyber resilience and response at the EU level. The adoption of the NIS Directive and the GDPR are of particular relevance with regards to harmonization of cybersecurity and data protection across the EU. While the NIS Directive imposes notification requirements around security incidents, the GDPR focuses on personal data breaches. As such, the EU acts as an important driver for the development of cybersecurity in both the public and private sector settings. The GDPR, in particular, is expected to change the current regulatory environment profoundly. However, it first needs to be accepted, then implemented, and only then we can judge its effectiveness in practice. On the whole, key European strategies and legislation have – up until now – primarily tackled the protection of personal data, security of operation of large scale and publically accessible information networks, and protection of operation of key infrastructures (of vital importance). The importance of cybersecurity in industrial settings has only been recognized marginally, and deserves increased attention.

At the same time, it is important to note that a decade after the 2007 cyber attacks against Estonia, there is still no procedure on how European authorities should deal with a cybersecurity crisis. Publication of a recommendation for a Blueprint on how to respond to large-scale cybersecurity

incidents is an important step in this regard[342] and to improve cooperation between civil and military cybersecurity authorities to manage breaches that affect multiple member states.[343] Measures such as sanctions could also be of value to retaliate against hackers.

7.3 Bottlenecks

Corporate Europe faces a wide range of challenges in identifying, preparing for and responding to cyber threats and incidents. Lack of trust to share information stands out as the number one inhibitor, both from an external, public policy perspective, and from the internal, company perspective. This concerns information sharing between individual member States, between governments and private enterprises, between CSIRTs, and between individual enterprises across industries and borders. Reluctance to share information makes it difficult to coordinate an effective response to cyber incidents both within and across borders. Information sharing could be improved by introducing a coordinated vulnerability disclosure (CVD) process in Europe. Trust can be fostered by setting up clear procedures for governments to inform companies as soon as a vulnerability has been detected or their systems have been breached. Mandatory requirements or penalties for non-cooperation could be put in place, in the event companies choose not to share their vulnerabilities or breaches. SMEs, for their part, need to reach a base information security management maturity to be able to consider threat intelligence sharing with industry partners and associations.

On the whole, bottlenecks that surfaced in our study are predominantly non-technical, and necessitate non-technical solutions. Lack of awareness – particularly at the board level – can trigger other issues, such as inadequate incident response planning, staff training or funding for security measures. Increasing public awareness by means of education and training should therefore be regarded as the number one priority. Changing behaviour and attitudes will require economic tools, not just technical ones. Annex I presents a number of possible recommendations for each bottleneck identified in our study.

7.4 Good practices

Although numerous inspiring examples have been put in place to improve cybersecurity of the private sector, they often come only after a company suffers damages. Companies need to be proactive rather than reactive when dealing with cyber threats. In addition, it is important to nurture a multidisciplinary approach toward cybersecurity, one that involves all key stakeholders.

As this study has shown, public-private partnerships have proven effective in dealing with cyber threats. Such partnerships can draw from the often complementary strengths that private and public

342 European Commission, "Annex to the Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises" (Brussels, September 13, 2017).

343 Anastasiya says, "EU Agency Asks Commission to 'Avoid Fragmentation' in New Cybersecurity Plans," EURACTIV.com, August 1, 2017, https://www.euractiv.com/section/cybersecurity/news/eu-agency-asks-commission-to-avoid-fragmentation-in-new-cybersecurity-plans/.

agencies possess. Private entities control much of the critical infrastructure that is vulnerable to cyber threats and have developed their own cybersecurity programs. Compared to their public counterparts, private companies are capable of mustering more cyber expertise, and can do so more rapidly, which makes them agile and enables them to respond faster. The public sector, in turn, possesses large resources and can facilitate the transfer of information from other states. In Europe, public-private partnerships exist in varying forms, with varying degrees of integration between the two actors. The case of the Netherlands was brought forward as a model for other Member States to build-upon.

In addition to public-private partnerships, 'cyber communities' have been successful in bringing a broad selection of stakeholders together, enhancing trust among them, encouraging the exchange of information and experience, and facilitating the pooling of knowledge and resources. Initiatives of professional associations and collectivities across Europe have been particularly effective in increasing the awareness of, and resilience against, cyber attacks among private companies, both large and small. Such communities extend beyond industry and government and incorporate universities as well as civil society.

Educational activities, both public and private, have been successful in raising the awareness of cybersecurity issues and enlarging the pool of highly qualified ICT professionals, including cybersecurity specialist and data experts, who are tailored to meet the needs of the cybersecurity market. Germany, UK, and the Czech Republic lead by example with regard to cybersecurity education programs offered at the national level. By means of certifications, courses, on-the-job trainings and consultancy services, the private sector also plays an important role in educating cybersecurity specialists. The majority of successful educational/training initiatives currently takes place at the associational level, as evidenced by the positive impact generated by the #DigitalSME4skills campaign. As this study has stressed, these efforts will have to be stepped up to bridge the skills gap, which is expected to reach 755,000 potential vacancies in 2020. In addition to ICT professionals, more attention ought to be paid to the shortage of cyber experts in academia and civil society, who are responsible for educational activities.

Cybersecurity challenges, competitions, hackathons and prizes constitute another strategy embraced by both the private and the public sector. On a national level, they have been successful in helping to increase the pool of ICT talent, stimulating interest in cybersecurity and combating the shortage of e-skills. They also provide the cybersecurity industry an advertising platform and a means to come into contact with potential future employees.

The uptake of cybersecurity insurance highlights our final approach observed in Europe that has helped companies address cyber risks. The cyber insurance market, however, is still very young. The implementation of both the NIS Directive and the GDPR are expected to positively influence its growth.

8. Annexes

8.1 Annex 1: Recommendations Table

The following table presents possible recommendations for each bottleneck identified in our study. The order of recommendations follows the sequence in which identified bottlenecks appear in the text of the study. It was formed on the basis on literature review and interviews with relevant stakeholders.

Bottleneck	Possible Recommendation(s)
Fragmented regulatory environment	- Increase cooperation and harmonization of approaches. Data protection rules should be applied in a uniform way in order to ensure a coherent legal framework for all companies operating in the internal market. The EU policymaking is on the 'right track' in this regard – the NIS directive and GDPR will increase uniformity across the EU. - Creating EU-wide regulations is one step, the next is putting adequate measures in place in order to assist member states and companies in implementing these regulations (similar to the GDPR implementation strategy mentioned below). - EU-wide standardization and certification is needed. Creation of an EU-wide cybersecurity certification framework is a step in the right direction.[344] - Standardize cyber hygiene practices across the EU.[345]
Lack of financial support	- Address access to finance (start-up support in particular). - Earmark more funding for cybersecurity programs and trainings within H2020. - Earmark additional resources for ENISA.[346] - In addition to the emergency fund for Member States that have suffered hacking attacks – proposed by the Commission – a European cybersecurity fund should be established. Such fund would be dedicated to attracting both public and private investment in order to support cybersecurity of SMEs, and to develop certain strategic competences in the ICT sector in general, and in cybersecurity in particular. [347]
Absence of national educational programs	- Expand skill sets through education, training and certification.[348] Introduce cybersecurity educational programs

344 Catherine Stupp, "Ansip Plans New EU Cybersecurity Centre," EURACTIV.com, July 20, 2017, https://www.euractiv.com/section/cybersecurity/news/ansip-plans-new-eu-cybersecurity-centre/.

345 ENISA, "Review of Cyber Hygiene Practices."

346 Catherine Stupp, "EU Cybersecurity Agency Seeks Funds and Power to Police Attacks," EURACTIV.com, May 22, 2017, https://www.euractiv.com/section/cybersecurity/interview/eu-cybersecurity-agency-seeks-remit-funds-to-police-attacks/.

347 https://www.euractiv.com/section/cybersecurity/interview/cybersecurity-partnership-europe-lacks-strategic-tech-muscle/

348 "European Cybersecurity Industry Leaders Recommendations on Cybersecurity for Europe," January 20, 2016.

	starting at an early age. - Given the increasing recognition of the need for an interdisciplinary approach to cybersecurity, in addition to technical disciplines, cybersecurity should be instructed in non-technical academic domains (law, politics, economics, defense).[349] - Most end-users are overwhelmed by the opportunities offered by digital technologies. It is important to develop educational and awareness-raising programs that also target general public and end-users. - In addition to ICT professionals, more attention should be paid to increasing the number of available cyber experts in academia and civil society, who would be responsible for educational activities.
Discrepancies in threat intelligence sharing policies	- Leverage and support existing intelligence sharing platforms, instead of enacting new ones. - Private entities should participate in or establish joint industry (or cross-industry) threat intelligence sharing platforms. - Public entities should promote an EU-level ISAC cooperation between the Member States and private companies.
Vulnerability disclosure debate	- Introduce a coordinated vulnerability disclosure (CVD) process in Europe.
GDPR-related bottlenecks	- Adopt a GDPR implementation strategy. - Implement master-data-management solutions to enable the level of control and oversight of data required by GDPR.[350]
General lack of awareness	- Promote a proactive rather than reactive approach so that organizations are prepared to deal with an incident strategically and minimise the overall damage. - Nurture a more multidisciplinary approach toward cybersecurity. Cyber risk should be managed by all key stakeholders, not just IT departments. Instead, it must be a collaborative effort of a broad selection of participants from different branches of the company.[351] - Engage top level management and promote attitude change toward cybersecurity.

349 Rademaker et al., "Dutch Investments in ICT and Cybersecurity - Putting It in Perspective."

350 Stibo Systems, "THE GDPR – HOW CAN MASTER DATA MANAGEMENT HELP?," accessed November 20, 2017, http://www.data2020summit.com/assets/whitepapers/gdrp_stibo_systems.pdf.

351 Rademaker et al., "Dutch Investments in ICT and Cybersecurity - Putting It in Perspective."

Lack of skills and training	- Expand skill sets through education, training and certification.[352] The private sector, educational institutes and all levels of government need to work together to develop effective vocational training programs and apprenticeships. - Set up training and awareness-raising activities among non-IT staff members to improve cyber hygiene practices across the entire organization.
Inadequate cybersecurity spending	- Large companies have an obligation towards the small ones that are part of their supply chains. They should help them increase their cybersecurity without power pressure. - Rather than relying on governments for the provision of funds, companies should consider funding as their own responsibility. Professional associations could be in charge of the pooling of resources.
Corporate under-reporting	- Incident response plans should include clear policies regarding breach disclosure.[353]
Lack of awareness about the implications of the GDPR	- GDPR training should be offered at associational and company level. - Promote legal assistance/consultancy for SMEs.
Lack of detection capabilities	- Develop more sophisticated predictive indicators based on past events and behaviors. Machine learning and self-teaching algorithms can help develop better analytics and indicators of compromise.[354] - Artificial Intelligence (AI) based solutions can help predict, detect and stop cyber attacks with higher speed and accuracy.
Technological vulnerability	- Create a level-playing field regarding privacy and security between Europe and the United States.[355] Facilitation of mergers would lead to a better consolidation of the currently fragmented market. - Facilitate private procurements oriented towards European SMEs. - Improve the protection levels of SMEs. - Improve security update experience. - Technological vulnerability can be reduced through: advanced backup and data recovery systems and procedures, as this

352 "European Cybersecurity Industry Leaders Recommendations on Cybersecurity for Europe."

353 Joseph Steinberg, "Could You Go to Prison for Not Reporting a Cybersecurity Breach?," Inc.com, January 25, 2017, https://www.inc.com/joseph-steinberg/sec-investigation-raises-terrifying-question-could-your-employees-go-to-prison-f.html.

354 Dave Shackleford, "Active Breach Detection: The Next-Generation Security Technology?," February 2016, https://www.sans.org/reading-room/whitepapers/analyst/active-breach-detection-next-generation-security-technology-36812.

355 "European Cybersecurity Industry Leaders Recommendations on Cybersecurity for Europe," 16.

	significantly reduces the harm inflicted by a data breach; advanced encryption, both for stored data and communications; two-factor authentication; password management systems. - Based on the WannaCry experience, software companies should keep offering security updates continuously, even on older software versions. If this becomes too costly, consumers should be informed and given sufficient time to install later versions without being exposed to cyber risks. - Technological deterrents need to be balanced with people-centric efforts.
Lack of incident response plans	- Companies need to evaluate their cyber risk and focus on building resilience for the inevitable. An essential starting point is to adopt adequate incident response plans. Companies first need to recognize they need a plan, then make it enterprise-wide and then operationalize it. Adoption of an ICT security policy in itself is not enough. Implementation and regular review of policies and protocols are crucial.
Average detection times	- Implement automated detection and response.[356]
Lack of trust to share information	- To improve security and reduce the potential for future risks, greater information sharing and coordination among stakeholders is needed. The capability to withstand cyber shocks is a team effort and has to be built across enterprises, sectors, countries and regions. Greater and more significant participation is needed. - Foster trust by setting up clear procedures for governments to inform companies as soon as possible when their systems have been breached or a vulnerability has been detected. - Install penalties for non-cooperation (when companies choose not to share their vulnerabilities or breaches). This will give companies a feeling others will follow suit. - It is important to increase cooperation among enterprises facing similar problems, which most often belong to the same sector. - SMEs need to reach a base information security management maturity to be able to consider threat intelligence sharing with industry partners and associations.
Organisational design	- Boards must be engaged. Cyber incidents ought to be judged as business risks due to their potential to cause physical damage, operational disruption, and reputational damage. Effective cyber risk management should thus start with awareness at the board level. - Cybersecurity/IT-security should become a top-level

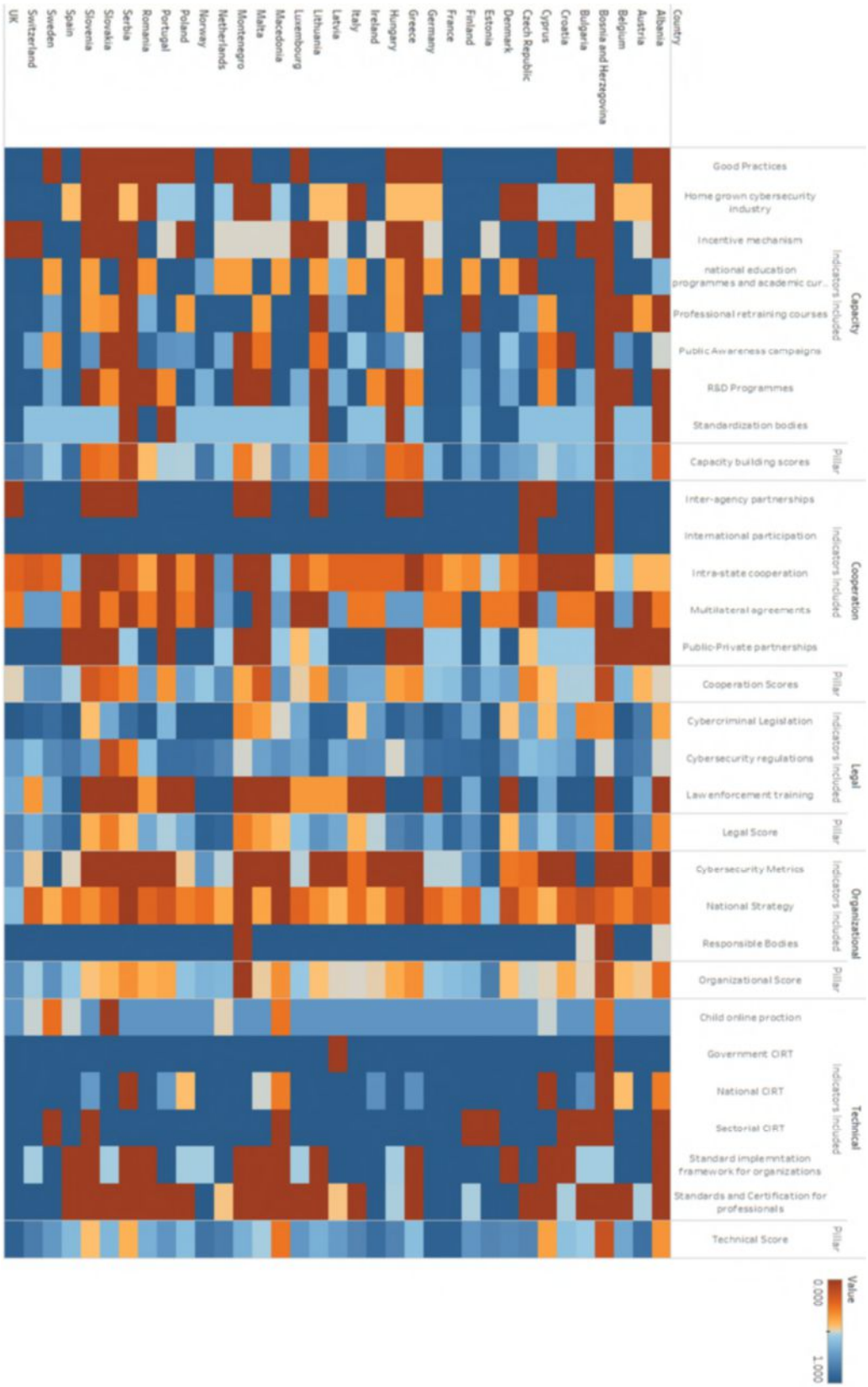
356 Shackleford, "Active Breach Detection: The Next-Generation Security Technology?," 9.

	management issue. In other words, cybersecurity should be sufficiently prioritized at the core (processes) of an organization. - Where this is not the case, there should be a person appointed who will be directly responsible for cybersecurity (CISO).
Cyber interdependence	- Greater inter-industry and regional coordination on cyber defense and crisis management of critical infrastructure is needed.[357] - All key industry sectors should stress-test their interdependencies by means of simulated cyber attack scenarios or realistic wargaming designed to inform risk management.[358]

357 Chertoff, "Good Neighbours Make Good Security: Coordinating EU Critical Infrastructure Protection Against Cyber Threats."

358 PwC, "Strengthening Digital Society against Cyber Shocks."

8.2 Annex 2: Heatmap of National Commitments according to ITU GCI 2017



8.3 Annex 3: Index Limitations

National Cybersecurity Index (NCSI)

The NCSI is promoted as a global index, a global database and a tool for cybersecurity capacity building. Contrary to its self-advertising, NCSI only evaluates 41 countries throughout the world, making it very difficult to accurately compare the performance of the European bloc as a whole to other key, global players. In addition, this database excludes several EU MS, such as Austria, Belgium and France. As the ITU notes, France is one of the leading countries globally in terms of cyber commitment and is ranked by the ITU as the second most committed EU nation behind Estonia. To use the NCSI index, which neglects to mention such a powerful and influential player in the cyber world, would lead to an underestimation of the level of cyber preparedness of Europe. The lack of comprehensive coverage of the entire European Union indicates that the NCSI is ill-suited for the analysis of cyber preparedness through the EU-28 states.

Cyber Readiness Index 2.0 (Melissa Hathaway, The Potomac Institute for Policy Studies)

This is a very comprehensive index that takes into account many more indicators than the ITU index that was used for this report. While it is very comprehensive, it does not offer a general index ranking. Rather, it details in great detail the cyber readiness of individual countries. This index is of incredible value and that value will increase over time as it becomes completed. Of the 125 countries that the Cyber Readiness Index intends to analyze, it has only analyzed 9 thus far (5 of which are members of the EU). Lacking a comprehensive, global index, along with the caveat of only having analyzed 5 out of the 28 EU member states as of this time, it is not an ideal index to be used. Once the Cyber Readiness Index 2.0 covers all 28 Member States, it can be used as a primary resource, as its "Readiness at a Glance" in depth analysis on a country by country basis can give deep insights into differences among EU Member States. However, at this time, it is far from complete.

Cyber Power Index (Economist Intelligence Unit, Booz Allen Hamilton)

The Cyber Power Index is an index developed jointly by the Economist's Intelligence Unit and Booz Allen Hamilton. While the publication includes a comprehensive list of 39 indicators and sub-indicators grouped into four categories, it covers only 20 countries which are part of the G20. Thus, many EU Member States are not covered and thus would not be evaluated if this study proceeded with the Cyber Power Index. While the index includes a scoring and ranking mechanism for individual countries, and focuses on the technical aspects and industry application, its geographical limitation of assessing only the G20 countries would have limited the scope of our analysis.

Network Readiness Index (World Economic Forum)

The Networked Readiness Index measures, on a scale from 1 (worst) to 7 (best), the performance of 139 economies in leveraging information and communications technologies to boost competitiveness, innovation and well-being. It does not extensively cover cyber-preparedness in a comprehensive manner, so would be ill-suited to evaluate the level of cyber commitment throughout the EU.

Kaspersky Cybersecurity Index

The Kaspersky Cybersecurity Index is a strong index that is based on bi-yearly survey data of thousands of internet users around the world. This index focuses on Internet use on a micro,

individual level. Its scope does not extend to government level initiatives. Therefore, while it provides a comprehensive analysis on an individual basis, it is ill-suited to be used as the basis for ranking states against one another both on the public and the private level. In addition to the aforementioned limitation, the survey does not cover the entirety of EU-28 countries.

BSA EU Cybersecurity Dashboard

The BSA Dashboard is focused on policy and organizational aspects of cybersecurity, with a strong reference to legal foundations as well as cooperation between public and private sector. The BSA Dashboard is focused on policy aspects of cybersecurity, and includes 25 criteria across 5 themes: legal foundations for cybersecurity, operational entities, public private partnership, sector-specific cybersecurity plans and education. While this dashboard covers all EU MS, this assessment is based on publicly available data, without a survey component. The most recent version of the dashboard was published on January 1st, 2015. Therefore, any developments since that time have not been taken into account. Many countries have made significant progress with regard to their cyber preparedness in the last few years and those changes would not have come to light if the BSA Dashboard was used. In addition to the currently outdated aspect, the lack of a survey based data collection exercise and ranking mechanisms contributed to the decision not use the BSA Dashboard as the primary index for this study.

8.4 Annex 4: Interview Questionnaire

The Hague Centre for Strategic Studies is a think tank based in The Hague, The Netherlands. We conduct analysis and provide strategic advice to high-level decision makers of European governments, NATO and the EU. We have been commissioned by the European Economic and Social Committee (EESC) to conduct a study on cybersecurity and resilience across corporate Europe, and on the degree of engagement of European businesses in tackling this issue.

For the purpose of our study, we are conducting a limited number of interviews focusing on policy challenges corporate Europe faces in implementing cybersecurity practices, and inspiring examples and practices that have been put in place to improve cybersecurity.

We will be more than happy to share the results of our study with you. They will feed into a report that will very likely be published in the beginning of 2018. The information you provide us with during the interview will be used in our report without direct personal attribution. With your permission we would like to record the interview to ensure that we preserve everything of value that will be said during this conversation, and we can get back to it later on. If you would like to share something 'off the record', please indicate so, and we will not use the information.

Threat awareness

1. Do companies participating in [INSERT NAME] allocate sufficient budget for cybersecurity? Has companies' spending on cybersecurity increased or decreased in recent years?

2. What is the majority of budget generally allocated for? (training/education, software, hardware)

3. Is there a sector/industry that stands out most in terms of number of attacks and lack of preparedness in case of an attack?

4. What approaches do companies participating in [INSERT NAME] most often adopt to decrease the cost of cybercrime? (Examples: internal security procedures such as strong password authentication, offsite data backup, mandatory obligations for all employees, etc.)

5. What inspiring examples/good practices have you observed companies/associations/states put in place in order to improve cybersecurity of businesses across the EU?

Challenges and policy instruments

6. What are the main challenges that companies face in implementing good cybersecurity practices? Are they mainly *external* (relating to legal and regulatory frameworks, lack of financing, absence of educational initiatives) or *internal* (relating to organisational and technological vulnerabilities, lack of skilled personnel, etc.)?

7. GDPR: According to a Survey carried out by Symantec, by the end of 2016, 96% of the surveyed companies lacked comprehension of the GDPR. Does [INSERT NAME] take any steps or initiatives to help its organizations comply with GDPR? How successful have they been?

8. How aware are the companies participating in your platform of the upcoming regulation and its implications? To what extent is GDPR implementation a policy priority for organisations participating in [INSERT NAME]?

9. What other legal instruments do you think would be helpful?

10. Sharing of threat intelligence with industry partners/associations has been identified as an effective way to reduce the cost of cybercrime. Are companies *willing* or *reluctant* to share threat intelligence? What is the underlying cause for the lack of trust? Please elaborate.

11. How useful has the work of [INSERT NAME] been in furthering cooperation and threat intelligence sharing among companies, and among private and public sector?

12. Do you think the current level of cooperation between the private sector and the public sector is sufficient? How could it be enhanced further?

13. What other types of PPP do you think would be useful?

14. Do you consider current funding and/or subsidies for the adoption and/or implementation of IT security measures adequate? Have you observed differences among large and small companies with regard to access to funding?

15. How is the interrelationship evolving between the security sector and business? What is the current level of information sharing between the private sector and security agencies (defense, secret services)?

8.5 Annex 5: List of acronyms and abbreviations

AI	Artificial Intelligence
ANNSI	National Agency for Security of Information Systems (France)
C3N	Center for the Fight against Digital Crime
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CDT	Cyber Diplomacy Toolbox
CERT	Computer emergency response team
CERT-EU	European Union Computer Emergency Response Team
CNAIP	National Center of Child Pornography Images
CoE	Council of Europe
CSIRT	Computer Security Incident Response Team
CSIS	Centre for Strategic and International Studies
CVD	Coordinated Vulnerability Disclosure
DDoS	Distributed Denial of Service
DESI	Digital Economy and Society Index
DG CONNECT	Directorate-General Communications Networks, Content and Technology
DNS	Domain Name System
DTC	Digital Trust Centre (Netherlands)
EC3	European Cybercrime Centre
EC-Council	International Council of Electronic Commerce Consultants
EC	European Commission
ECJ	European Court of Justice
ECP	Electronic Commerce Platform (Netherlands)
ECSM	European Cybersecurity Month
ECSO	European Cybersecurity Organisation
ECVCU	Economic Crime Victim Care Unit
EDA	European Defence Agency
EEAS	European External Action Service
EHR	Electronic Health Records
EMEA	Europe, Middle East, and Africa
ENISA	European Union Agency for Network and Information Security
EPSC	European Political Strategy Centre
EU	European Union
EU INTCEN	EU Intelligence and Situation Centre
EUROPOL	European Union Agency for Law Enforcement Cooperation
G7	Group of Seven
GCI	General Communication Inc.
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GISWS	Global Information Security Workforce Study
Global EPIC	Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity

GP	General Practitioner
HCSS	Hague Centre for Strategic Studies
HSBC	Hongkong and Shanghai Banking Corporation
HSD	Hague Security Delta
IBM	International Business Machines Corporation
ICMP	Internet Control Message Protocol
ICS2	International Information System Security Certification Consortium
ICT	Information and Communications Technology
IDC	International Data Corporation
IOCTA	Internet Organised Crime Threat Assessment
IoT	Internet of Things
IP	Intellectual Property
IRP	Incident Response Plan
ISACA	Information Systems Audit and Control Association
ISAC	Information Sharing and Analysis Centre
ISCO	International Standard Classification of Occupations
IT	Information Technology
ITU	International Telecommunication Union
NACE	Nomenclature of Economic Activities
NATO	North Atlantic Treaty Organization
NCSA	National Cybersecurity Alliance (United States)
NCSC	National Cybersecurity Center (Netherlands)
NHS	National Health Service (United Kingdom)
NIS	Network and Information Systems (Directive)
NRN	National Response Network (Netherlands)
OECD	Organisation for Cooperation and Development
OSCE	Organisation for Security and Co-operation in Europe
PPP	Public-Private Partnership
PREDICT	Prospective Insights in ICT R&D
PwC	PricewaterhouseCoopers
R&D	Research & Development
SME	Small and Medium-sized Enterprise
SOC	Security Operations Center
TB	Terabyte
TCP	Transmission Control Protocol
UK	United Kingdom
UNGGE	United Nations Group of Governmental Experts
UN	United Nations
US	United States
WEF	World Economic Forum

9. Bibliography

"7 Top Security Certifications You Should Have in 2017." InfoSec Resources, October 13, 2017. http://resources.infosecinstitute.com/7-top-security-certifications-you-should-have/.

"10 Ideas for the Future of Europe's Digital Economy - 'SMEs as the Engines of Digital Change.'" European Digital SME Alliance, March 11, 2016.

Abraham, Inge. "How General Data Protection Regulation Can Unlock Value." Accenture Insights, February 24, 2017. https://www.accenture-insights.nl/en-us/articles/gdpr-general-data-protection-regulation-opportunities.

Anderson, Ross, Chris Barton, Rainer Boehme, Richard Clayton, Michel J.G. van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. "Measuring the Cost of Cybercrime." presented at the 11th Workshop on the Economics of Information Security, Berlin, Germany, June 26, 2012. http://www.econinfosec.org/archive/weis2012/presentation/Moore_presentation_WEIS2012.pdf.

Anthe, Charlie, Michael Johnson, Siddharth Pavithran, Evan Argyle, Jeff Jones, Daryl Pecelj, Eric Douglas, et al. "Microsoft Security Intelligence Report - Volume 21 | January through June, 2016." Redmond, WA, USA: Microsoft, 2016.

Apostle, Julia. "The Uber Data Breach Has Implications for Us All." *Financial Times (FT)*, November 27, 2017. https://www.ft.com/content/e2bf6caa-d2cb-11e7-a303-9060cb1e5f44.

Ashford, Warwick. "DDoS Is Most Common Cyber Attack on Financial Institutions." ComputerWeekly.com. Accessed October 16, 2017. http://www.computerweekly.com/news/4500272230/DDoS-is-most-common-cyber-attack-on-financial-institutions.

Bengales, E., L. Hernandez, C. Minguez, J. Perez, M. Solaz, M. Lopez-Cobo, and F. Rossetti. "The 2017 PREDICT Dataset Methodology." Joint Resarch Centre, 2017. http://publications.jrc.ec.europa.eu/repository/bitstream/JRC106713/jrc106713_2017_predict_dataset_methodology.pdf.

Bernik, Igor. "Cybercrime: The Cost of Investments into Protection." *Journal of Criminal Justice and Security*, no. 2 (n.d.): 105–16.

Bieliauskaite, Justina. "DIGITAL SME President Oliver Grün Appointed SME Board Member at ECSO, the European Cybersecurity Organisation." *European Digital SME Alliance* (blog), July 12, 2016. https://www.digitalsme.eu/digital-sme-president-oliver-grun-appointed-sme-board-member-ecso-european-cyber-security-organisation/.

Boeke, Sergei. "National Cyber Crisis Management: Different European Approaches." *Governance*, September 2017, 1–16.

Bogart, Andy, and Lillian Ablon. "Zero Days, Thousands of Nights The Life and Times of Zero-Day Vulnerabilities and Their Exploits." RAND Corporation, n.d.

Bran, Mirel. "Romania: 'Hackerville', Capital of Global Cybercrime." France 24, December 7, 2012. http://www.france24.com/en/20121207-reporters-romania-hackerville-ramnicu-valcea-cyber-crime-fraud-scams-hackers-internet-police-fbi-cia-bitdefender.

BSA. "BSA Country: Estonia." BSA, 2015. http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_estonia.pdf.

———. "BSA Country: France." BSA, 2015. http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_france.pdf.

Burgess, Matt. "UK Gov Wants Teens to Practice Cybersecurity in Their Spare Time." WIRED UK, June 26, 2017. http://www.wired.co.uk/article/cyber-skills-uk-cybersecurity-skills-shortage.

Bursztein, Elie, Kylie McRoberts, and Luca Invernizzi. "Tracking Desktop Ransomware Payments." Accessed September 20, 2017. https://www.blackhat.com/docs/us-17/wednesday/us-17-Invernizzi-Tracking-Ransomware-End-To-End.pdf.

"CCDCOE." CCDCOE. Accessed January 12, 2018. https://www.ccdcoe.org.

CEPS. “Software Vulnerabilities Disclosure: The European Landscape.” Centre for European Policy Studies, July 31, 2017. https://www.ceps.eu/publications/software-vulnerabilities-disclosure-european-landscape.

Chertoff, Philip. “Good Neighbours Make Good Security: Coordinating EU Critical Infrastructure Protection Against Cyber Threats.” GLOBSEC Policy Institute, August 28, 2017.

Cisco. “Healthcare Security: Improving Network Defenses While Serving Patients.” Amsterdam: Cisco, 2016.

Comodo Threat Research Labs. “Comodo Threat Research Labs - Q1 2017 Report.” Quarterly Report, 2017. https://www.comodo.com/ctrlquarterlyreport/q1/Comodo_Q1Report_062817.pdf.

———. “Comodo Threat Research Labs - Q2 2017 Report.” Quarterly Report, 2017. https://www.comodo.com/ctrlquarterlyreport/q1/Comodo_Q1Report_062817.pdf.

“Connecting Europe Facilities — Cybersecurity Digital Service Infrastructure.” Digital Single Market, April 2, 2016. https://ec.europa.eu/digital-single-market/en/news/connecting-europe-facilities-cybersecurity-digital-service-infrastructure.

Csulak, Emery, Theresa Meadows, Joshua Corman, George DeCesare, Anura Fernando, David Finn, Mark Jarrett, et al. “Report on Improving Cybersecurity in the Health Care Industry.” Health Care Industry Cybersecurity Task Force, June 2017.

“Cybersecurity Boost for UK Firms - GOV.UK.” gov.uk, January 16, 2015. https://www.gov.uk/government/news/cyber-security-boost-for-uk-firms.

Cybersecurity Challenge UK. “Capture the Flag.” Cybersecurity Challenge UK. Accessed November 3, 2017. https://www.cybersecuritychallenge.org.uk/competitions/capture-the-flag.

———. “Competitions.” Cybersecurity Challenge UK. Accessed November 3, 2017. https://www.cybersecuritychallenge.org.uk/competitions.

———. “Masterclass.” Cybersecurity Challenge UK. Accessed November 3, 2017. https://www.cybersecuritychallenge.org.uk/competitions/masterclass.

———. “Sponsors.” Cybersecurity Challenge UK. Accessed November 3, 2017. https://www.cybersecuritychallenge.org.uk/sponsors.

Cybok. “The Cybersecurity Body Of Knowledge.” cybok.org. Accessed November 3, 2017. https://www.cybok.org/.

“Data Protection - Better Rules for Small Businesses.” European Commission, n.d. http://ec.europa.eu/justice/smedataprotect/index_en.htm.

Deloitte. “Dealing Efficiently with Cybercrime - Cyber Value at Risk in The Netherlands 2017.” Accessed October 16, 2017. https://view.deloitte.nl/rs/834-ESS-180/images/deloitte-nl-risk-cyber-value-at-risk-in-the-netherlands-2017-report-web.pdf?mkt_tok=eyJpIjoiWkRKallqbGxaamsxWVRRMyIsInQiOiJ3NlBKYlBFbWlQSlN6S0hRYnpGRW5CNWZoMVdYeDhYWncyWXduRlBBdjhFTjRMcE93R25UXC9tQ2pCdExcL29iMWhqN3EwK3ZsQ1FKuijtUQmpsOWVvdHgxVmZyb3RPZ3UwTGF1TjFoY0hPTzlvV2lMWERVN1wvbUNiZXRiRWVrSjM2MyJ9.

———. “Deloitte EMEA Cyber Academy Cyber Training, Education and Awarenesss,” 2017. https://www2.deloitte.com/content/dam/Deloitte/hu/Documents/risk/hu-cyber-cyberacademy-leaflet-noexp.pdf.

Di Matteo, Bendetta. “New EU Cyber Strategy Leaves Key Security Gaps.” Global Risks Insight, October 15, 2017. https://globalriskinsights.com/2017/10/new-eu-cyber-strategy-leaves-key-security-gaps/.

“DigiDuck – Safer Online | GCCS 2015.” gccs2015.com. Accessed November 3, 2017. https://www.gccs2015.com/nl/node/556.

DIGITALEUROPE. “Facts and Figures.” digitaleurope.org. Accessed October 16, 2017. http://www.digitaleurope.org/Our-Work/Projects/Past-projects/eSkills-for-Jobs/Facts-and-Figures.

“Digitizing Industry (4.0) and Cybersecurity.” European Parliament, November 2017.

drjim. “When It Comes To Cyber Threats, CIOs Don’t Like To Share.” The Accidental Successful CIO, November 11, 2015. http://theaccidentalsuccessfulcio.com/security-2/when-it-comes-to-cyber-threats-cios-dont-like-to-share.

“Dutch Cabinet Invests 2.5 Million in New Digital Trust Centre.” The Hague Security Delta (HSD), September 25, 2017. https://www.thehaguesecuritydelta.com/news/newsitem/947-new-cybersecurity-centre-for-entrepreneurs.

“Economic Crime Victim Care Unit (ECVCU).” Text. Action Fraud, October 13, 2016. https://www.actionfraud.police.uk/support-and-prevention-economic-crime-victim-care-unit.

“Education Map - ENISA.” European Union Agency for Network and Information Security (ENISA), 2017. https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/universities.

ENISA. “CSIRTs by Country - Interactive Map — ENISA.” European Union Agency for Network and Information Security. Accessed September 20, 2017. https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map.

———. “CSIRTs in Europe — ENISA.” Topic. European Union Agency for Network and Information Security. Accessed September 20, 2017. https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities?tab=details.

———. “Cyber Insurance: Recent Advances, Good Practices and Challenges — ENISA.” Report/Study, November 7, 2016. https://www.enisa.europa.eu/publications/cyber-insurance-recent-advances-good-practices-and-challenges.

———. “Cybersecurity Information Sharing: An Overview of Regulatory and Non-Regulatory Approaches,” December 2015.

———. “Definition of National/Governmental CERTs - Baseline Capabilities — ENISA.” Page. European Union Agency for Network and Information Security. Accessed September 20, 2017. https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/baseline-capabilities.

———. “ENISA National Cybersecurity Strategies (NCSSs) Map.” Topic. European Union Agency for Network and Information Security. Accessed September 20, 2017. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map.

———. “ENISA Threat Landscape Report 2016 - 15 Top Cyber-Threats and Trends.” Report/Study. Heraklion, Greece: European Union Agency For Network and Information Security, January 2017. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016.

———. “EU Cyber Challenge — ENISA.” Topic. Accessed November 3, 2017. https://www.enisa.europa.eu/topics/cybersecurity-education/eu-cyber-challenge.

———. “Review of Cyber Hygiene Practices.” Heraklion, Greece: European Union Agency For Network and Information Security, December 2016. https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport.

“Europe Code Week 2017 - About EU Code Week.” codeweek.eu. Accessed November 3, 2017. http://codeweek.eu/about/.

“Europe Code Week 2017 - Europe Code Week.” codeweek.eu. Accessed November 3, 2017. http://codeweek.eu/.

“Europe Code Week 2017 - Resources and Guides.” codeweek.eu. Accessed November 3, 2017. http://codeweek.eu/resources/.

European Commission. “A Guide to ICT-Related Activities in WP2016-17,” July 25, 2016. https://ec.europa.eu/programmes/horizon2020/sites/horizon2020/files/Guide%20to%20ICT-related%20activities%20in%20WP2016-17%20A4%20Sept2016.pdf.

———. “Annex to the Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises.” Brussels, September 13, 2017. https://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-6100-F1-EN-ANNEX-1-PART-1.PDF.

———. “Commission Boosts Cybersecurity Industry and Steps up Efforts to Tackle Cyber-Threats.” europa.eu, July 5, 2016. http://europa.eu/rapid/press-release_MEMO-16-2322_en.htm?locale=FR.
———. “COMMISSION STAFF WORKING DOCUMENT ASSESSMENT OF THE EU 2013 CYBERSECURITY STRATEGY,” September 13, 2017. http://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF.
———. “COMMUNICATION FROM THE COMMISSION - Strengthening Europe’s Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry,” July 5, 2016. https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-410-EN-F1-1.PDF.
———. “COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: ICT Standardisation Priorities for the Digital Single Market,” April 19, 2016.
———. “Digital Economy and Society Index — Digital Scoreboard - Data & Indicators.” Digital Single Market - Digital Economy & Society, 2017. http://digital-agenda-data.eu/charts/desi-components#chart={"indicator":"DESI_4_IDT","breakdown-group":"DESI_4_IDT","unit-measure":"pc_DESI_4_IDT","time-period":"2017"}.
———. “EU Cybersecurity Initiatives - Working towards a More Secure Online Environment,” January 2017. http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf.
———. “European Attitudes Toward Cybersecurity,” 2017. http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/79734.
———. “JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU,” September 13, 2017. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017JC0450.
———. “Pledge for the Digital Skills and Jobs Coalition.” Digital Single Market. Accessed November 3, 2017. https://ec.europa.eu/digital-single-market/en/pledge-for-digital-skills-jobs-coalition.
———. “Pledges for Action.” Digital Single Market. Accessed November 3, 2017. https://ec.europa.eu/digital-single-market/en/pledges-action.
———. “Regulatory Framework - Growth - European Commission.” Growth. Accessed November 20, 2017. /growth/sectors/medical-devices/regulatory-framework_en.
———. “Special Eurobarometer 464a Europeans’ Attitudes towards Cybersecurity,” September 2017.
———. “The Digital Skills and Jobs Coalition.” Digital Single Market. Accessed November 3, 2017. https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition.
“European Cybersecurity Challenge.” Accessed November 3, 2017. https://www.europeancybersecuritychallenge.eu/index.html.
“European Cybersecurity Challenge ECSC 2018.” Accessed November 3, 2017. https://www.europeancybersecuritychallenge.eu/next.html.
“European Cybersecurity Industry Leaders Recommendations on Cybersecurity for Europe,” January 20, 2016.
“European Cybersecurity Strategy: Fostering the SME Ecosystem.” European Digital SME Alliance, July 31, 2017.
“European Cybersecurity Strategy: Fostering the SME Ecosystem | Cyberwatching.” Accessed November 16, 2017. https://www.cyberwatching.eu/news-events/news/european-cybersecurity-strategy-fostering-sme-ecosystem.
“European DIGITAL SME Alliance.” *European Digital SME Alliance* (blog). Accessed November 16, 2017. https://www.digitalsme.eu/about/european-digital-sme-alliance/.

European Parliament, and Council of the European Union. “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,” July 19, 2016. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN.

European Political Strategy Centre, European Commission. “Building an Effective European Cyber Shield.” ec.europa.eu, May 8, 2017. /epsc/publications/strategic-notes/building-effective-european-cyber-shield_en.

Europol. “The Internet Organised Crime Threat Assessment (IOCTA) 2016.” The Hague, Netherlands, 2016. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016.

Eurostat. “ICT Security in Enterprises.” Eurostat - Statistics Explained, December 2015. http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises.

Eurostat, Konstantinos Giannakouris, and Maria Smihily. “ICT Security in Enterprises, 2010.” Industry, trade and services. Eurostat, July 2011. http://ec.europa.eu/eurostat/documents/3433488/5578468/KS-SF-11-007-EN.PDF/03f32f6d-5029-4049-9de3-4da4513a3bea.

“FireEye - Marsh & McLennan Cyber Risk Report 2017 - Cyber Threats: A Perfect Storm About to Hit Europe?” Milpitas, CA, USA: FireEye, Inc., 2017. https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/Fireye%20Cyber%20Report-01-2017.pdf.

Flinders, Karl. “HSBC Online Services Hit by DDoS Attack.” ComputerWeekly.com, January 29, 2016. http://www.computerweekly.com/news/4500272109/HSBC-online-services-hit-by-DDoS-attack.

Franceschi-Bicchierai, Lorenzo. “Inside ‘Hackerville,’ Romania’s Infamous Cyber Crime Hub.” Motherboard, June 17, 2015. https://motherboard.vice.com/en_us/article/4x3jnd/inside-hackerville-romanias-infamous-cyber-crime-hub.

Fuentes, Mayra Rosario. “Cybercrime and Other Threats Faced by the Healthcare Industry.” TrendLabs, 2017.

Gehem, Maarten, Artur Usanov, Erik Frinking, and Michel Rademaker. “Assessing Cybersecurity - A Meta-Analysis of Threats, Trends, and Responses to Cyber Attacks.” Security. The Hague, Netherlands: The Hague Centre for Strategic Studies, April 16, 2015. http://beta.hcss.nl/sites/default/files/files/reports/HCSS_Assessing_Cyber_Security.pdf.

Gemalto. “2016 Mining for Database Gold - Findings from the 2016 Breach Level Index.” Gemalto, 2016. http://breachlevelindex.com/assets/Breach-Level-Index-Report-2016-Gemalto.pdf?utm_source=press-release&utm_medium=full-report&utm_term=bli&utm_content=bli-report&utm_campaign=bli-2016-full-report.

Gerstein, Daniel M. “The WannaCry Virus, a Lesson in Global Unpreparedness.” Text, May 17, 2017. http://nationalinterest.org/feature/the-wannacry-virus-lesson-global-unpreparedness-20719.

“Global Cybersecurity Index 2017: Europe.” International Telecommunication Union (ITU), 2017. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/EUR_GCIv2_report.pdf.

Global Forum on Cyber Expertise. “Coordinated Vulnerability Disclosure - Initiative.” www.thegfce.com, September 16, 2015. https://www.thegfce.com/initiatives/r/responsible-disclosure-initiative-ethical-hacking.

Graham, Chris. “NHS Cyber Attack: Everything You Need to Know about ‘biggest Ransomware’ Offensive in History.” *The Telegraph*, May 13, 2017. http://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/.

Graham, Luke. “Cybercrime Costs the Global Economy $450 Billion: CEO.” www.cnbc.com, February 7, 2017. https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html.

GrantThornton. “Cyber Attacks Cost Global Business over $300bn a Year.” Grant Thornton International Ltd. Home, September 22, 2015. https://www.grantthornton.global/en/insights/articles/cyber-attacks-cost-global-business-over-$300bn-a-year/.

“Hacking Village – DefCamp 2017.” Accessed November 3, 2017. https://def.camp/hacking-village/.

Hague Security Delta. “Triple Helix Cooperation.” Accessed November 14, 2017. https://www.thehaguesecuritydelta.com/market/triple-helix-cooperation.

Härmä, Katriina, and Tomáš Minárik. “European Union Equipping Itself against Cyber Attacks with the Help of Cyber Diplomacy Toolbox.” The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), September 18, 2017. https://ccdcoe.org/european-union-equipping-itself-against-cyber-attacks-help-cyber-diplomacy-toolbox.html.

Hathaway, Melissa, Chris Demchak, Jason Kerben, Jennifer McArdle, and Francesca Spidalieri. “France Cyber Readiness At A Glance.” Arlington, VA: Potomac Institute, 2016. http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_france.pdf.

“Healthcare Cybersecurity and Ransomware Report 2017.” *Cybersecurity Ventures* (blog), March 31, 2017. https://cybersecurityventures.com/healthcare-cybersecurity-report-2017/.

Hewlett, Ryan. “Cyber Crime against the Healthcare Sector.” Kennedys Insurance, January 2017.

Hiscox. “The Hiscox Cyber Readiness Report 2017.” London, United Kingdom: Hiscox Group, 2017. http://www.hiscox.com/cyber-readiness-report.pdf.

HM Government. “Cyber Essentials - OFFICIAL SITE.” cyberaware.gov.uk, 2016. https://www.cyberaware.gov.uk/cyberessentials/faq.html.

———. “National Cyber Secuirty Strategy 2016-2021.” Accessed November 14, 2017. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

“How Estonia Became a Global Heavyweight in Cybersecurity.” e-Estonia, June 2017. https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/.

Hulme, George V. “Tackling Cybersecurity Threat Information Sharing Challenges.” CSO Online, January 17, 2017. https://www.csoonline.com/article/3157540/security/tackling-cybersecurity-threat-information-sharing-challenges.html.

Humanities, Faculty of, Social Sciences University of Bath, Claverton Down Bath, and Ba2 7ay. “Launch of Global EPIC.” PaCCS. Accessed November 16, 2017. http://www.paccsresearch.org.uk/news/launch-global-epic/.

Husing, Tobias, Werner B. Korte, and Eriona Dashja. “Trends and Forecasts for the European ICT Professional and Digital Leadership Labour Markets (2015-2020).” Empirica, November 2015. http://eskills-lead.eu/fileadmin/lead/brochure-lead/working_paper_-_supply_demand_forecast_2015_a.pdf.

IDC. “Worldwide Revenue for Security Technology Forecast to Surpass $100 Billion in 2020, According to the New IDC Worldwide Semiannual Security Spending Guide.” www.idc.com, October 12, 2016. http://www.idc.com/getdoc.jsp?containerId=prUS41851116.

Imperva Incapsula. “Global DDoS Threat Landscape | Q1 2017 | Incapsula.” www.incapsula.com, 2017. https://www.incapsula.com/ddos-report/ddos-report-q1-2017.html.

Inc, Spiceworks. “Many Companies Unprepared for GDPR Compliance Deadline in 2018,” June 27, 2017. https://community.spiceworks.com/research/gdpr-impact-on-it.

“Independent Study Reveals Incident Response Perception Gap Among EU Companies.” IBM Resilient, June 1, 2015. https://www.resilientsystems.com/news-and-events/incident-response-press-releases/gap-among-eu-companies/.

Ismail, Nick. “Sharing Cyber Threat Intelligence Is Necessary to Combat Data Theft.” *Information Age* (blog), August 16, 2017. http://www.information-age.com/sharing-cyber-threat-intelligence-necessary-combat-data-theft-123467953/.

Jay, Jay. “Europe May Face Cyber-Security Skills Gap of 350,000 Workers by 2022.” TEISS, June 6, 2017. https://teiss.co.uk/news/europe-may-face-cyber-security-skills-gap-350000-workers-2022/.

Juniper Research Ltd. “Cybercrime Will Cost Businesses Over $2 Trillion by 2019.” www.juniperresearch.com, May 12, 2015. https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion.

Kaspersky Lab. “Measuring Financial Impact of IT Security on Business - IT Security Risks Report 2016,” 2016. https://media.kaspersky.com/en/business-security/kaspersky-it-security-risks-report-2016.pdf.

Kerravala, Zeus. “John Chambers’ 10 Most Memorable Quotes as Cisco CEO.” Network World, July 24, 2015. https://www.networkworld.com/article/2952184/cisco-subnet/john-chambers-10-most-memorable-quotes-as-cisco-ceo.html.

Khalimonenko, Alexander, and Oleg Kupreev. “Kaspersky Securelist DDOS Attacks in Q1 2017.” www.securelist.com, May 11, 2017. https://securelist.com/ddos-attacks-in-q1-2017/78285/.

Klimburg, Alexander. *The Darkening Web: The War for Cyberspace*. New York: Penguin Press, 2017.

Kriz, Danielle. “Passage of EU NIS Directive Is a Milestone, but next Steps Matter Even More.” *Palo Alto Networks* (blog), July 6, 2016.

Lab, Kaspersky. “A True Cost of Cyberattacks,” February 16, 2016. https://www.kaspersky.com/blog/cost-cyberattack-enterprise/5195/.

Lloyd’s of London. “Extreme Cyber-Attack Could Cost as Much as Superstorm Sandy.” www.lloyds.com, July 17, 2017. https://www.lloyds.com/news-and-insight/press-centre/press-releases/2017/07/cyber-attack-report.

Magazine, Author: Yudhijit Bhattacharjee Yudhijit Bhattacharjee. “How a Remote Town in Romania Has Become Cybercrime Central.” WIRED, January 31, 2011. https://www.wired.com/2011/01/ff_hackerville_romania/.

Markus, Riek, Ciere Michael, Hernandez Ganan, and Carlos van Eteten. “Estimating the Costs of Consumer-Facing Cybercrime: A Tailored Instrument and Representative Data for Six EU Countries.” TU Delft, 2016. http://pure.tudelft.nl/ws/files/28985021/WEIS_2016_paper_54_2.pdf.

Marsh. “Continental European Cyber Risk Survey: 2016 Report,” October 2016. http://www.hkbb.ch/uploads/6869.

Marsh & McLennan Companies. “2017 Cyber Threats: A Perfect Storm about to Hit Europe?” FireEye, Inc., January 2017. https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-world-eco-forum.pdf.

Mas, M, J Frenandez de Guevara, J.C. Robledo, and M. Lopez-Cobo. “The 2017 PREDICT Key Facts Report.” Joint Resarch Centre, 2017. http://publications.jrc.ec.europa.eu/repository/bitstream/JRC106658/kjna28594enn.pdf.

Matthews, Tim. “The Anatomy of a Distributed Denial-of-Service Attack.” Incapsula Blog, January 12, 2016. https://www.incapsula.com/blog/anatomy-of-ddos-attack.html.

McAfee, and Center for Strategic and International Studies. “Net Losses: Estimating the Global Cost of Cybercrime Economic Impact of Cybercrime II.” Santa Clara, CA, USA: McAfee & Center for Strategic and International Studies, June 2014. https://www.mcafee.com/de/resources/reports/rp-economic-impact-cybercrime2.pdf.

Microsoft. “Microsoft Security Intelligence Report Bulgaria,” 2017. https://www.microsoft.com/en-us/security/Intelligence-report.

———. “Microsoft Security Intelligence Report Romania,” 2017. https://www.microsoft.com/en-us/security/Intelligence-report.

Monteleone, Shara, and Laura Puccio. “From Safe Harbour to Privacy Shield: Advances and Shortcomings of the New EU-US Data Transfer Rules.” European Parliamentary Research Service (EPRS), January 2017.

“More ICT Campaigns — ECSM.” Cybersecuritymonth.eu. Accessed November 3, 2017. https://cybersecuritymonth.eu/about-ecsm/more-ict-campaigns.

Morgan, Steve, and Cybersecurity Ventures. “Hackerpocalypse Cybercrime Report.” *Cybersecurity Ventures* (blog), August 12, 2016. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). “Cybersecuritybeeld Nederland CSBN 2017.” The Hague, Netherlands: Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), June 2017. https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/cybersecuritybeeld-nederland/cybersecuritybeeld-nederland-2017/1/CSBN2017.pdf.

National Cybersecurity Centre. “NCSC-Certified Degrees - NCSC Site.” NCSC.gov.uk, September 8, 2017. https://www.ncsc.gov.uk/information/ncsc-certified-degrees.

Netherlands Ministry of Economic Affairs. “Digital Agenda for the Netherlands Innovation, Trust, Acceleration.” The Hague, Netherlands: Netherlands Ministry of Economic Affairs, July 1, 2016. https://www.government.nl/documents/reports/2017/04/11/digital-agenda-for-the-netherlands-innovation-trust-acceleration.

Netherlands National Cybersecurity Centre. “ISAC’s.” National Cybersecurity Centre - Ministry of Security and Justice. Accessed September 20, 2017. https://www.ncsc.nl/english/Cooperation/isacs.html.

“New Ponemon Institute Study Reveals Nearly 80 Percent of German Organizations Aren’t Prepared for a Cybersecurity Incident.” IBM Resilient, February 3, 2016. https://www.resilientsystems.com/news-and-events/incident-response-press-releases/new-ponemon-institute-study-reveals-nearly-80-percent-german-organizations-arent-prepared-cyber-security-incident/.

Nexusguard. “Distributed Denial of Service (DDoS) Threat Report Q1 2017.” Threat Report. San Francisco, CA, USA: Nexusguard, 2017. https://www.nexusguard.com/hubfs/Nexusguard_DDoS_Threat_Report_Q1_2017_EN.pdf?hsCtaTracking=b0aa2b53-b6e8-417a-b313-fec3fff4cff6%7C8a68fea1-c169-4f36-a600-e4d4641b4f55.

———. “Hidden Danger Behind DDoS Attacks | Nexusguard.” nexusguard.com. Accessed October 16, 2017. https://www.nexusguard.com/genius/whitepapers/hiddendangerbehindddosattacks.

“NHS Trusts ‘at Fault’ over Cyber-Attack.” *BBC News*, October 27, 2017, sec. Technology. http://www.bbc.com/news/technology-41753022.

Nickelson, David. “Medical Systems Hacks Are Scary, but Medical Device Hacks Could Be Even Worse.” Harvard Business Review, May 15, 2017. https://hbr.org/2017/05/medical-systems-hacks-are-scary-but-medical-device-hacks-could-be-even-worse.

O’Brien, Stuart. “Demand for Cybersecurity Professionals on the Rise – Total...” *Total Security Summit* (blog), June 12, 2017. https://totalsecuritysummit.co.uk/demand-for-cyber-security-professionals-on-the-rise/.

Panda Security. “Pandalabs Quarterly Report Q1 2016,” 2016. http://www.pandasecurity.com/mediacenter/src/uploads/2016/05/Pandalabs-2016-T1-EN-LR.pdf.

———. “Pandalabs Quarterly Report Q1 2017,” 2017. http://www.pandasecurity.com/mediacenter/src/uploads/2017/05/Pandalabs-2017-T1-EN.pdf.

Piggin, Richard. “Cybersecurity of Medical Devices.” BSI Group, 2017.

Ponemon Institute. “2016 Cost of Cyber Crime Study & the Risk of Business Innovation,” October 2016. https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf.

———. “2017 Cost of Data Breach Study.” Ponemon Institute, June 19, 2017. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&.

———. “The Cyber Resilient Organisation in the United Kingdom: Learning to Thrive against Threats,” January 2016. http://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/TheC

yberResilientEnterpriseUKFINAL.pdf?submissionGuid=0d7b9d75-06ee-49df-a641-a726c26d2b73.

Ponemon Institute, and Accenture. “2017 Cost of Cyber Crime Study & the Risk of Business Innovation,” October 2016. https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf.

“ProCredit - New Computer Malware Targets Clients of Bulgarian Banks,” August 31, 2015. http://www.procreditbank.bg/en/new-computer-malware-targets-clients-of-bulgarian-banks/page/300/item/28323.

Provan, Keith G., and Kenis Patrick. “Modes of Network Governance: Structure, Management, and Effectiveness.” *Journal of Public Administration Research and Theory*, August 2, 2007, 229–52. https://doi.org/10.1093/jopart/mum015.

PwC. “Cybersecurity: European Emerging Market Leaders.” PwC UK, January 2017. http://www.pwc.co.uk/deals/assets/cyber-security-european-emerging-market-leaders.pdf.

———. “Strengthening Digital Society against Cyber Shocks,” 2017. https://www.pwc.com/us/en/cybersecurity/assets/pwc-strengthening-digital-society-against-cyber-shocks.pdf.

———. “The Global State of Information Security® Survey 2017.” www.pwc.com, n.d. http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html.

Rademaker, Michel, Louk Faesen, Koen van Lieshout, and Mercedes Abdalla. “Dutch Investments in ICT and Cybersecurity - Putting It in Perspective.” Security. The Hague, Netherlands: The Hague Centre for Strategic Studies, March 8, 2017. https://www.thehaguesecuritydelta.com/media/com_hsd/report/123/document/HCSS-Dutch-Investments-in-ICT.pdf.

RCA security. “Cyber Crime and the Healthcare Industry.” RCA Security, LLC, 2013.

“Reform of Cybersecurity in Europe.” General Secretariat of the Council of the European Union, August 1, 2018. http://www.consilium.europa.eu/en/policies/cyber-security.

Riek, Markus, Rainer Bohme, and Tyler Moore. “Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance,” 2015. https://tylermoore.utulsa.edu/tdsc15riek.pdf.

“Risk and Responsibility in a Hyperconnected World.” Insight Report. Geneva, Switzerland: World Economic Forum (WEF), January 2014.

Robinson, Neil, Veronika Horvath, Jonathan Cave, Arnold P. Roosendaal, and Marieke Klaver. “Data and Security Breaches and Cyber-Security Strategies in the EU and Its International Counterparts.” Directorate General for Internal Policies Policy Department A: Economic and Scientific Policy Industry, Research and Energy, September 2013. https://www.eerstekamer.nl/eu/documenteu/ip/a/itre/nt/2013_5_data_and_security_breaches/f=/vjd6mn2lcpyg.pdf.

Roman, Jeffrey. “17 Indicted in International ATM Fraud Scheme,” March 28, 2014. https://www.bankinfosecurity.com/17-indicted-in-international-atm-fraud-scheme-a-6689.

Ross, Joe. “Cybersecurity Trends: A Look at the First Half of 2017.” *Huffington Post* (blog), July 31, 2017. https://www.huffingtonpost.com/entry/cyber-security-trends-a-look-at-the-first-half-of_us_597f48a2e4b09982b7376650.

says, Anastasiya. “EU Agency Asks Commission to ‘Avoid Fragmentation’ in New Cybersecurity Plans.” EURACTIV.com, August 1, 2017. https://www.euractiv.com/section/cybersecurity/news/eu-agency-asks-commission-to-avoid-fragmentation-in-new-cybersecurity-plans/.

Shackleford, Dave. “Active Breach Detection: The Next-Generation Security Technology?,” February 2016. https://www.sans.org/reading-room/whitepapers/analyst/active-breach-detection-next-generation-security-technology-36812.

Shalal, Andrea. “Germany Sees Rise in Cybercrime, but Reporting Rates Still Low.” *Reuters*, May 3, 2017. https://www.reuters.com/article/us-germany-cybercrime-crime/germany-sees-rise-in-cybercrime-but-reporting-rates-still-low-idUSKBN17Z26S.

"SoSo: Cybersecurity for SMEs, Local Public Administration and Individuals | Ideal-Ist," August 25, 2016. https://www.ideal-ist.eu/ps-es-101370.

Spring, Tom. "EU Struggles to Determine Growing Cost of Cyberattacks." Threatpost | The first stop for security news, August 12, 2016. https://threatpost.com/eu-struggles-to-determine-growing-cost-of-cyberattacks/119870/.

Staff, The CyberWire. "The WannaCry Ransomware Pandemic: Perspective, Reactions, and Prospects." The CyberWire. Accessed November 17, 2017. https://thecyberwire.com/articles/the-wannacry-ransomware-pandemic-perspective-reactions-prospects.html.

Steinberg, Joseph. "Could You Go to Prison for Not Reporting a Cybersecurity Breach?" Inc.com, January 25, 2017. https://www.inc.com/joseph-steinberg/sec-investigation-raises-terrifying-question-could-your-employees-go-to-prison-f.html.

Stibo Systems. "THE GDPR – HOW CAN MASTER DATA MANAGEMENT HELP?" Accessed November 20, 2017. http://www.data2020summit.com/assets/whitepapers/gdrp_stibo_systems.pdf.

Stupp, Catherine. "Ansip Plans New EU Cybersecurity Centre." EURACTIV.com, July 20, 2017. https://www.euractiv.com/section/cybersecurity/news/ansip-plans-new-eu-cybersecurity-centre/.

———. "EU Cybersecurity Agency Seeks Funds and Power to Police Attacks." EURACTIV.com, May 22, 2017. https://www.euractiv.com/section/cybersecurity/interview/eu-cybersecurity-agency-seeks-remit-funds-to-police-attacks/.

Symantec. "Attackers Target Both Large and Small Businesses." Accessed November 16, 2017. https://www.symantec.com/content/dam/symantec/docs/infographics/istr-attackers-strike-large-business-en.pdf.

———. "Businesses Underprepared for GDPR | Symantec." www.symantec.com, October 18, 2016. https://www.symantec.com/en/uk/about/newsroom/press-releases/2016/symantec_1018_01.

Teivainen, Aleksi. "OP Targeted in a Denial of Service Attack." Helsinki Times, January 2, 2015. http://www.helsinkitimes.fi/finland/finland-news/domestic/13102-op-targeted-in-a-denial-of-service-attack.html.

Tofan, Dan, Theodoros Nikolakopoulos, and Eleni Darra. "ENISA The Cost of Incidents Affecting CIIs: Systematic Review of Studies Concerning the Economic Impact of Cyber-Security Incidents on Critical Information Infrastructures (CII)." Heraklion, Greece: European Union Agency For Network and Information Security, August 2016. https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis/.

Triple Helix Research Group, Stanford University. "The Triple Helix Concept | Triple Helix Research Group." Accessed November 14, 2017. https://triplehelix.stanford.edu/3helix_concept.

"TROOPERS 2017 – the 10th Anniversary!" Accessed November 3, 2017. https://www.troopers.de/troopers17/.

Tzanou, Maria. *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance*. London: Bloomsbury Publishing Plc, n.d.

"United Kingdom (UK) GDP - Gross Domestic Product 2016." countryeconomy.com. Accessed November 14, 2017. https://countryeconomy.com/gdp/uk?year=2016.

United Nations Interregional Crime and Justice Research Institute (UNICRI). "Cybercrime: Risks for the Economy and Enterprises at the EU and Italian Level," 2014. http://www.combattingcybercrime.org/files/virtual-library/phenomena-challenges-cybercrime/cybercrime-risks-for-the-economy-and-enterprises-at-the-eu-and-italian-level.pdf.

Vanian, Jonathan. "Here's How Much Businesses Worldwide Will Spend on Cybersecurity by 2020." Fortune, October 12, 2016. http://fortune.com/2016/10/12/cybersecurity-global-spending/.

VeriSign. "Verisign Distributed Denial of Service Trends Report Volume 4, Issue 1 – 1st Quarter 2017." VeriSign, Inc., 2017. https://www.verisign.com/assets/report-ddos-trends-Q12017.pdf.

Veritas. "2017 VERITAS GDPR REPORT," 2017. https://www.veritas.com/content/dam/Veritas/docs/reports/gdpr-report-en.pdf.

Verizon. “2017 Data Breach Investigations Report 10th Edition.” Verizon, 2017. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/.

Warwick, Ashford. “New Government Plan to Support Cybersecurity Startups.” ComputerWeekly.com, January 27, 2016. http://www.computerweekly.com/news/4500271901/New-government-plan-to-support-cyber-security-startups.

Werkhauser, Nina. “German Army Launches New Cyber Command | Germany | DW | 01.04.2017.” DW.COM, April 1, 2017. http://www.dw.com/en/german-army-launches-new-cyber-command/a-38246517.

“What Is ECSM? — ECSM.” Cybersecuritymonth.eu. Accessed November 3, 2017. https://cybersecuritymonth.eu/about-ecsm/whats-ecsm.

“What the Hack - The Hackathon against DDoS.” Accessed November 3, 2017. https://www.thehaguesecuritydelta.com/cyber-security/events/event/1559-what-the-hack-the-hackathon-against-ddos-2017-09-14.

Woolf, Nicky. “DDoS Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say.” *The Guardian*, October 26, 2016, sec. Technology. http://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

World Bank. “GDP (Current US$), Germany | Data.” Accessed November 14, 2017. https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=DE.

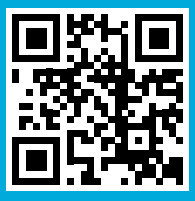
———. “Netherlands | Data.” Accessed November 14, 2017. https://data.worldbank.org/country/netherlands.

World Economic Forum. “Networked Readiness Index.” Global Information Technology Report 2016, 2016. http://wef.ch/29cCKbU.

European Economic and Social Committee

Rue Belliard/Belliardstraat 99
1040 Bruxelles/Brussel
BELGIQUE/BELGIË

Published by: "Visits and Publications" Unit
EESC-2018-48-EN
www.eesc.europa.eu



Print
QE-01-18-515-EN-C
ISBN 978-92-830-4104-7
doi:10.2864/917494

Online
QE-01-18-515-EN-N
ISBN 978-92-830-4105-4
doi:10.2864/98090

EN