icom
institute for competitiveness

MAKING EUROPE SAFER

DATA, NETWORKS AND CLOUD: DRIVERS OF CYBERSECURITY IN EUROPE?

EU STUDY 1.18

icom
institute for competitiveness

MAKING EUROPE SAFER

DATA, NETWORKS AND CLOUD: DRIVERS OF CYBERSECURITY IN EUROPE?

APRIL 2018

EDITOR

Stefano da Empoli

AUTHORS

Silvia Compagnucci

Maria Rosaria Della Porta

Gloria Marcotullio

Giusy Massaro

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Digitalization is revolutionizing our society transforming human existence, business models and the relationship between authorities and citizens.

Focusing on the European context, data shows that in the different Member States EU citizens and companies have a different level of computer skills and, more generally, a **different awareness of the advent of the digital age**, accessing available digital services with a different intensity and interest.

Chapter 1 provides a photograph on Internet usage, digital skills and digital service penetration in the EU. In particular, the analysis aims to describe some factors conditioning Internet usage (age, gender, Internet connection) and the most popular activities carried out online (par. 1.1.). At European level, data shows Northern Europe's primacy, a direct relationship between age and Internet usage and a greater interest of large companies - being more aware of digitalization's opportunities and having more resources to invest in the digital channel. Focusing on digital service penetration in Europe, par. 1.2.1. underlines that there are more than 4 billion people worldwide using the Internet, with the number of people using the top platform in each country increasing by almost 1 million new users every day during the past 12 months. **More than 3 billion people worldwide now use social media each month,** with 9 in 10 of those users accessing their chosen platforms via mobile devices. Globally, social media users have increased by 13 percent in the past 12 months.

The following paragraphs (1.2.2.) analyze e-commerce and Internet banking. Concerning **e-commerce**, it registered a new peak with **1.6 billion worldwide users who purchased products online and spending almost $ 2 trillion, an amount that could double by 2020.** Among the 10 countries with the highest penetration rates of online sales by mid-2017, we find China and South Korea (83%) at the top, followed by the United Kingdom (82%). Regarding the nationality of sellers, it's interesting to note that in 2017, in the European Union, **there was a preference for sellers from other EU countries** or within Member States. No big differences were shown between males and females while for age, individuals aged between 16-24 years and 25-54 years were more active in online shopping.

The **banking sector** (par. 1.2.3.) is also experiencing the digital revolution. Internet and mobile device penetration is reshaping the relationship between banks and customers, introducing new services and new ways of using traditional ones. **The highest percentage of users fall into the age groups of 25-34 year olds and 35-44 year olds**. **No gender difference was found in using Internet banking.**

The last paragraph of this chapter focuses on the value of the digital economy. **The value of the digital economy in terms of the contribution of**

information and communication technology to GDP growth is estimated to be around 5% of total GDP in the European Union.

The economic impact of the Internet is growing and has a huge potential in all European countries. In **Ireland**, the digital economy contributed to **10.7%** of the GDP in 2017, followed by Sweden and Luxembourg (7.2% and 6.8%, respectively), scoring above the EU average (Fig. 1.13). Instead, in the other European countries, such as Greece, Portugal, Austria and Italy, the contribution of the digital economy to GDP was lower than 4%.

Chapter 2 addresses the **cybersecurity threats** issue. The Internet allows people to connect worldwide and has led to the spread of a mass of smart devices for both individuals and businesses. However, this relatively new way of living (always accessible, everywhere at every moment) has resulted in many new problems in terms of security, and specifically cybersecurity.

According to the WEO, **cyber risks intensified** in 2017, so much so that cyber attacks and massive data fraud appear in the top five global risks perceived. Cyber branches have almost doubled from 68 per business in 2012 to 130 per business in 2017. **The financial costs of cyber attacks have also risen over the last five years** (+62%).

The recent cyber attacks have different and broader impacts compared to those incidents of the past decade. In 2017 alone, two major attacks involved **WannaCry** (in May) and **Petya** (in June). WannaCry hit, among others, the National Health Service in the United Kingdom, Nissan Motor Manufacturing UK and Renault. According to Cyence, the potential economic losses were estimated at $8 billion. Petya mainly hit the Ukraine, where the Chernobyl Nuclear Power Plant went offline, with an estimated loss of $850 million.

Cyber attacks have been changing over the last years. Until a few years ago, they were more focused (every week, a new retailer, healthcare provider, or financial institution lost their customers' sensitive data), while **now** these attacks **are more widespread, hitting, more or less simultaneously, several different companies and sectors worldwide**.

From 2013 to 2017, cyber crime, Cyber Espionage and Information Warfare have recorded the highest number of attacks. cyber crime has gradually increased from 53% to 76%, while hacktivist attacks have progressively decreased from 39% to 7%. Cyber espionage and information warfare increased in 2017 (by 47% and 24%, respectively).

Malware are the most widespread attacks accounting for a total of 787 million, of which 2.7% spread over the mobile network. Ransom attacks also increased, accounting for 12.5 million in 2017 (+226%).

European citizens are also facing the growing reality of cyber threats. According to Eurostat data, in the European Union, **the share of Internet users having experienced certain common security issues over the Internet** – such as viruses affecting devices, abuse of personal information, financial losses or children accessing inappropriate websites – was **25% in 2015** and is forecasted to increase in the coming years

if appropriate security measures are not implemented. Being infected by a virus or other computer infection was the main problem. In fact, **slightly more than 1 Internet user out of 5 (21%) in the EU caught an online virus or other computer infection resulting in a loss of information or time**. Moreover, security concerns prevented 24% of consumers providing personal information to online communities for social and professional networking; ordering or buying goods or services online (15%); downloading software, music, video files, games or other data files (15%); carrying out banking activities online (14%); or communicating with public administrations across the EU-28 in 2015.

Instead, among the European industries, **financial Services, fanufacturing and telecommunications are the main target of cyber criminals**, especially in Germany, Belgium, Spain and Great Britain.

The last paragraph of this chapter focuses on the regulatory framework; above all analyzing the initiatives carried out by the European Institutions to ensure **data protection.** These include: Regulation 679/16, the proposal for a regulation concerning the protection of individuals in the processing of personal data by EU institutions, authorities, offices and agencies, as well as free data movement; the proposal for a regulation on confidentiality and electronic communications; the proposal for a regulation of the European Parliament and Council on a framework for the free movement of non-personal data in the EU); **cybersecurity** (EU Cybersecurity Strategy launched in 2013; the Regulation on electronic identification authentication and signature; and Directive 2016/1148 - the NIS Directive - the strategic plan for cybersecurity launched in September 2017) in the European Member States.

Chapter 3 deals with **the impact of cybersecurity on enterprises**. Nowadays, cyber criminals are continually finding new ways to monetize personal information and many enterprises and organizations have been blackmailed. Furthermore, for some companies, intellectual property and trade secrets are their most valuable assets, and they now find these have become susceptible to new and growing threats. Therefore, the range of potential attacks and attackers is widening and increasing by the day. The new technologies, mobiles, and smart devices connected to the Internet of Things expose every organization to attackers and in an increasingly digitized world, cybersecurity has jumped to the top of companies' risk agendas after a number of high profile data breaches, ransom demands, distributed denial of service (DDoS) attacks and other hacks that have occurred over the last years. No sector of the economy is immune to attack; cyber criminals are increasingly targeting power grids, chemical plants, aviation systems, transportation networks, connected cars, telecommunications systems, financial networks, etc. Very often, **cyber crime uses very simple tools and tactics, namely emails, to make a big impact and to damage companies**. In fact, email is not just a communication tool but it is also one of the prime sources of threat for users and organizations. This threat can range from unwanted emails in the form of spam

to more dangerous types, such as the propagation of ransomware or phishing campaigns. According to the Internet Security Threat Report published by Symantec a growing proportion of spam contains malware. **Agriculture, forestry and fishing, together with the wholesale trade, were the sectors most affected by emails that contained malware in 2016**. In fact, the percentage of emails classified as malware was about 1% of the total. **Agriculture was also the sector most affected by phishing in 2016**, with 0.06% of emails classified as phishing attempts followed by the finance and insurance sectors.

The main and most costly impacts on organizations that suffer a cyber attack are business disruption, loss of information, loss of revenue and damage to equipment. According to the global survey conducted by Accenture and the Ponemon Institute (2017), for 43% of the organizations interviewed, **the most damaging consequence was the loss of information**. Instead, **business disruption was mentioned by 33% of organizations** and, **finally, revenue losses and equipment damages were reported by 21% and 3%, respectively**.

To reduce cyber risks, the companies have had to adopt cyber risk mitigation measures and ICT security policies. A cybersecurity program should include at least three elements: training employees to recognize phishing attempts and malicious emails; restricting access to key data and information; and preparing an incident response plan and identifying key vendors before a cyber event. According to the global survey conducted by Kroll (2018), **the most implemented actions are employee restrictions on installing software (89% of respondents) and employee cybersecurity training (83% of respondents)**. Incident response plans (IRPs) also lead the list, with 80% of respondents indicating their company already has an IRP in place.

Instead, the top three actions the IT companies should implement in the next months are intrusion detection systems that are device-based, endpoint threat monitoring and intrusion detection systems that are networked based.

As far as Europe is concerned, **in 2015, almost one out of three enterprises in the EU-28 had ICT security policies in place**. **The issue of cybersecurity is particularly felt in large companies** and more than 70% of European large companies adopted an ICT security policy in 2015, while less than 1 in 3 SMEs had done so. Finally, **ICT and professional, scientific and technical activities are the main sectors that show interest in the cybersecurity issue** with 62% and 49%, respectively, of European enterprises defining IT security policies

Moreover, cloud computing has entered the mainstream of information technology, providing scalability in the delivery of enterprise applications. It provides improved efficiency in everyday tasks, as well as a pathway for massive amounts of data generated by IoT to travel.

At a European level, the adoption is still quite weak – just one in five European companies use a cloud

computing service, and just 14% make use of more sophisticated cloud computing services. Nonetheless, at a global level, the trend is definitely growing, and Europe cannot but fall into line.

Among the main **benefits** identified by enterprises are a **faster access to infrastructure** (62% of interviewees), **greater scalability** (61%), **higher availability** (56%) and **faster time-to-market** (51%). However, the cloud also involves challenges. These include a lack of resources and expertise, with security and managing cloud spending being the most compelling ones, although the latter has been gradually decreasing.

Companies should decide, based on their needs and capabilities, which cloud model fits best with their internal organization, choosing from among private, public or hybrid cloud models. That said, however, while adoption of the public cloud has been limited to date, future prospects seem to be markedly different and, today, many companies are moving towards public cloud solutions. This is mainly due to its ease of scalability (implying a high degree of cost-effectiveness) and also to its greater reliability, since it involves a vast network of servers, thus redistributing the load among the other data centers, should one center fail. According to the results from a recent McKinsey study, although just 40% of the companies studied has more than 10% of their workloads on public cloud platforms, about 78% are planning to increase this to more than 10% within three years or to double their cloud penetration. In addition, the worldwide public cloud services market revenue was projected to grow by 18.5% in 2017 to a total of $260.2 billion, up from $219.6 billion in 2016, and is expected to reach $411.5 billion by 2020.

As enterprises scale up their use of the public cloud, they must rethink how they can protect data and applications. In particular, they need to dramatically evolve their cybersecurity practices in order to consume public cloud services in a way that enables them both to protect critical data and to fully exploit the speed and agility that these services provide. Security is often cited as one of the top barriers to cloud migration. For this reason, companies need a proactive, systematic approach to adapting their cybersecurity capabilities for the public cloud. This approach is described in a detailed manner in section 3.4.3. In addition, **a model of Security as a Service is recently emerging. It is an outsourcing model for security management that does not require on-premise hardware and entails**, among others, **two main benefits: constant virus definition updates that are not reliant on user compliance and greater security expertise than is typically available within an organization.**

The real matter is that applications and data maintained in the cloud can be more secure than data held in on-premise corporate systems because **moving to the right kind of advanced cloud system represents a more dynamic approach to risk**. As companies digitize more and more aspects of their internal operations and external contacts, the standard approach involving the use of IT systems to detect and prevent unwanted efforts to gain entry becomes no longer effective. The problem calls for an

entirely different type of solution and the cloud may offer several benefits. In particular, **it can provide almost unlimited low-cost computational power**, which is often needed to identify suspicious activities, something that is impossible for traditional IT systems when it comes to monitoring huge volumes of data and highly complex and interconnected applications. Furthermore, **it is able to detect and respond to intrusion more dynamically, with a learning capacity that traditional IT technologies don't have**. The final strength of the cloud-based system lies, thus, in its ability to combine authentication and analytics from multiple sources. As cyber attacks become an increasingly shared problem, with a cloud-based system we can openly exchange information about the attackers' identities and the nature of the threats they pose, resulting in a shared knowledge base without compromising anyone's secure data.

Chapter 4 provides for a focus on three industries - manufacturing, energy and automotive.

For manufacturing, the IoT is at the center of the industrial transformation because of the revolutionary ways this connected technology has streamlined and simplified various manufacturing processes. Traditionally, robots have been used to perform tedious, repetitive tasks on the assembly line. Today, they are capable of mimicking more human traits, such as dexterity and memory, of providing safer working environments, as well as valuable feedback and data, thus allowing companies to make necessary adjustments more accurately. Within the EU, Germany and Italy are the two largest markets – 5th and 7th at a global level -, 36% and11%, respectively, of the overall EU market, numbering 56,000 robots sold in 2016 and expected to reach 82,600 units by 2020. **As manufacturers innovate cyber threats accelerate and become more and more sophisticated**. According to the results of a study by Deloitte and the Manufacturers Alliance for Productivity and Innovation (MAPI), **top threats**, damaging about one third of the interviewed enterprises, **include IP theft (34%) and phishing/ pharming (32%).** In addition, increasing dependence on technology-enabled connected products brings a new set of risks to manufacturers such as attacks involving mobile devices or mobile networks, that concern about one in four surveyed companies.

The challenge of implementing a secure, vigilant, and resilient cyber risk strategy is different in the age of Industry 4.0. One major problem is machine obsolescence that, once combined with connected devices, become particularly vulnerable. In addition, cybersecurity should become an integral part of the strategy, design and operations, being considered from the beginning of any Industry 4.0 – driven initiative. **A first important step is to provide the company with a formally written security policy, however,** across the EU countries, only one in three manufacturing companies has done this. Sweden ranks first among the EU countries with a 53% of manufacturing companies equipped in this sense, followed by Italy (45%). **Another major problem is the multitude of products and vendors in manufacturing settings,**

that creates a confusing picture for security experts. 46% of the manufacturing security professionals said they use six or more security vendors, and 20% more than 10 vendors. In addition, security is often outsourced, especially among small and medium-sized businesses (SMB). **Another hurdle is represented by the composition of security teams**. Nearly 60% of the manufacturing organizations said they have fewer than 30 employees dedicated to security and 25% complain about a lack of trained personnel. Finally, **manufacturers also need their IT and OT departments to share knowledge**, so as to reduce to a minimum the consequences of one's processes or downtimes on others. What companies are currently focusing on is mainly application security involving the use of software, hardware, and procedural methods to protect applications from external threats (41% of interviewed companies), as well as, security consultants (38%) and the use of anti-viruses (38%).

The cloud will lead also in manufacturing. At the manufactured-product level, cloud computing will transform everything from how products themselves are researched, designed- and developed, to how they are fabricated, manufactured and used by customers in the field. Moreover, it will play a key role towards enabling and democratizing new manufacturing production systems such as 3D printing, generative design and the Industrial Internet of Things.**Today, digital services such as cloud computing provide at least 25% of the total input that go into finished manufactured products**. One particularly important benefit of the **cloud** is that it **allows manufacturers to leverage infinitely scalable computational resources**, so that they can readily access the computational resources they require without having to purchase expensive IT equipment up-front. This is **especially important for small and medium-sized manufacturing enterprises (SMEs) that lack the financial resources to purchase expensive IT equipment.** Summing up, cloud computing is helping manufacturers innovate, reduce costs and increase their competitiveness. It allows for the use of many forms of new production systems, from 3D printing and high-performance computing (HPC) to the Internet of Things (IoT) and industrial robots, democratizing access to and use of these technologies by small manufacturers.

The security aspects are very important when cloud computing is used given that **the security strategies that have been developed so far are not suitable**. **This is probably the reason why the degree of adoption of cloud computing services – especially those of medium and high level of sophistication - is still quite low across EU manufacturing enterprises (17% and 9%, respectively).** However, one major benefit associated with cloud computing, according to some, is that it can actually make manufacturing IT systems more secure. This is because **cloud-computing providers employ best-of-breed cybersecurity practices that are often far more sophisticated than what individual companies can achieve by themselves** on a one-off basis, which is particularly true for SMEs lacking the needed resources

and expertise. **Thus, cloud computing may represent an opportunity to have better data security at affordable prices**.

The **growing digitalization** of the economy has also exposed the energy sector to cybersecurity risks. **Utilities are increasingly exposed to IT risks**, due to the **smart electricity** networks with thousands of interconnected users. As other companies, utilities are threatened by economic cyber risks (e.g. a hacker wishing to profit from an attack, by diverting money to an account or stealing industrial information). However, the main concern for energy companies is relevant to the cyber attacks that could affect electricity generation plants and transmission grids.

Although utilities were among the first companies to computerize, today the **need for a renewal** has emerged. Many utilities use **equipment** that works very well from an industrial point of view, but they are **obsolete from an IT point of view** (e.g. old control systems).

Cybersecurity is becoming a priority in the energy sector so that, in 2015, **40% of European energy companies had already formally adopted an ICT security policy**. Among risks, energy companies are less worried by the unavailability of ICT services due to an attack from outside (e.g. Denial of Service attack), with only 29% of European enterprises having formally defined a specific ICT security policy against this cyber threat. While 37% are concerned about data destruction or corruption resulting from an attack or unexpected incident.

Following the description of the four energy **cybersecurity priorities** by the EECSP-Expert Group[1], the study addresses two topics that from the point of view of cybersecurity can be seen as a strength or as a weakness - smart grids and the cloud.

Smart grids have a huge potential in terms of safety, productivity, improvement of service quality and operational efficiency, despite **requiring more care** in terms of cybersecurity. A distributed energy system unquestionably has a **higher number of potential vulnerabilities** and access points. However, the **effects** and the **impacts** of possible attacks **can be reduced and isolated to a specific part of the system**. It is therefore **crucial to establish an adequate security system**, in order to safely carry information on the digital network and prompt reply malfunctions and interruptions in the electricity supply. Due to the possible impact of a successful attack on consumer trust and the rise in security questions along the value chain, smart grids should be equipped with sophisticated protection mechanisms that can evolve rapidly and adapt to the continuous development of malware.

Thanks to the evolving energy paradigm – increasingly focused on **decentralized model** and **energy storage systems**, as well as electricity **producers and consumers**, **all working together through remote control and monitoring** as virtual power plants –

1 Identified priorities:
- to formalize an effective threat and risk management system at EU level
- to establish an effective response framework at regional level
- to boost the improvement of cybersecurity resilience
- to make available adequate energy cybersecurity skills and competences.

the energy cloud is becoming increasing important. Supported by technological progress, it encompasses platforms to enable the matching of traditional market players and customers. In 2016, **19% of European energy enterprises used at least one of the cloud computing services**. Finland and Sweden were the most active in the energy cloud, 49% and 44%, respectively. Looking at the type of services used[2], 9% of European energy enterprises used high cloud services. The best performers in the use of high cloud services were Finland (34%) and the Netherlands (27%). **Many cloud experts believe that trusted cloud data centers have better security than in-house data centers**. From this point of view, security is contingent upon the reliability of the provider. Therefore, although the main reason for adopting the cloud was not originally for security, security itself could become a key success factor for cloud computing companies.

The study also showed some attacks recently occurred in the energy sector, a tiny part of all occurring cyber incidents.

Concerning **cybersecurity in the automotive sector, the number of connected vehicles** in the world is constantly increasing. According to some estimates, connected vehicle installations in China, North America, Europe and Japan **should reach 68 million by the end of 2018, an increase of 278% compared to 2013. Autonomous vehicles** of level 4 and 5 **will begin to mainstream after 2028 and the analysts forecast about 80 million level 4 and 5 autonomous cars in China, North America and the European Union by 2030**.

Connected and autonomous cars take us toward a mode of transport that is more efficient, by enabling an interconnected driving experience but there is concern because **interconnecting via Internet could expose vehicles – and the people in them – to potential risks from online threats.** The cybersecurity risk for connected cars is of particular importance because external access to a car's network not only compromises the privacy of a driver's data, but also the cybersecurity threat to connected cars can become a matter of life and death, threatening the industry's road map towards autonomous and connected vehicles.

According to the results of a survey (Foley, 2017) conducted on 83 automotive and technology executives between America and Asia, **IT security and privacy - selected by 31% of respondents - are an important concern for connected cars and the main obstacle to their development**. In addition, **cybersecurity attacks emerged as the top legal issue for 63 % of respondents** that must be addressed in developing technology for connected cars and/or autonomous vehicles. **Not only companies but also consumers are worried about cybersecurity in connected cars**. The Irdeto Global Consumer Connected Car Survey examined consumer awareness of cyberattacks targeting connected cars and autonomous vehicles and,

2 According to the Eurostat ranking there are three levels of services:
- Low: email, office software, storage of files;
- Medium: email, office software, storage of files, hosting of the enterprise's database;
- High: accounting software applications, CRM software, computing power.

according to this survey, **85% of global consumers indicated that they believe any connected car has the potential to be targeted by a cyber attack and 59% of connected car owners are concerned that their vehicle could be targeted by a cyber attack**.

After describing of the concerns about cybersecurity in the automotive sector, the study addresses the topic related to the role of cloud computing. Cloud-based services offer new navigation systems to drivers and passengers. Moreover, cloud connectivity is also changing infotainment and supporting the evolution of autonomous driving and can help automotive companies to redefine and personalize customer relations and transform and optimize operations. Furthermore, the cloud ensures the cutting edge technology to improve **its performance in cybersecurity through platforms able to hinder any cyber attack attempts**.

Only through the thoughtful use of disruptive technologies such as big data, machine learning, artificial intelligence and the use of cloud computing can we help build a better, safer and more secure connected vehicle ecosystem.

PART 1

THE DIGITAL ECONOMY AND SOCIETY IN EUROPEAN COUNTRIES

1. THE DIGITAL ECONOMY AND SOCIETY IN EUROPEAN COUNTRIES

1.1. DIGITAL SKILLS IN THE EUROPEAN UNION

Digitalization is revolutionizing our society. Increasing nearly 900 per cent, from 400 million in 2000 to 3.5 billion users today, the Internet has had a huge impact on the economies and societies around the world. At the same time, the Internet has been transformed by society becoming an essential tool to communicate, collaborate and conclude transactions, and not only for sending and receiving emails and a "place" to find information.

The Internet will introduce drastic shifts across all sectors in the future Internet economy. Every economic sector will be touched by technology and only those able to adapt quickly to technological changes will be successful and competitive.

Innovative technologies, platforms and systems such as the Internet of Things, Big Data & Analytics, Blockchain, Artificial Intelligence, Cloud Computing, Augmented Reality & Virtual Reality, Advanced Robotics & 3D Printing and 5G are the new enabling tools of the digital economy able to revolutionize human life, business models and the relationship between authorities and citizens.

Focusing our attention on the European context, data shows that, in different Member States, EU citizens and companies have a different level of computer skills. As well, they have a different awareness of the advent of the digital age, accessing available digital services with a different intensity and interest.

However, Northern Europe leads in the field of digitalization. Regarding Internet usage by individual, in 2017, Denmark, Luxembourg and Sweden (2%), the Netherlands (3%) and the United Kingdom (4%) were the best performers with only a tiny percentage of individuals not using the Internet. The lowest performers, on the other hand, were registered in Bulgaria, Greece, Croatia and Romania, where the percentage of individuals never accessing the Internet in 2017 was 30%, 28%, 28% and 27%, respectively (Fig. 1.1).

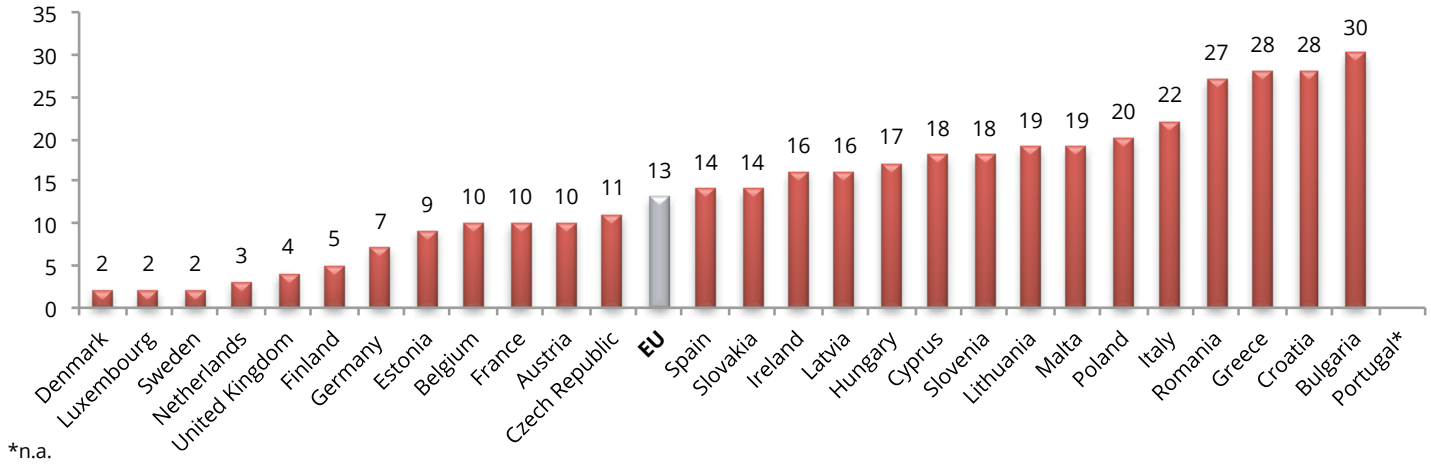
Concerning daily Internet use, Luxemburg and Denmark, the Netherlands and Sweden registered the best performance with 91% and 90% of individuals daily accessing the Internet in 2017.

Focusing on factors potentially affecting Internet usage (age, gender, Internet connection), a reverse relationship between age and Internet usage could be depicted. Younger people are on average more inclined to use the Internet (92% of 16-24 year olds, 89% of 25-34, 82% of 35-44) than older people who reveal – due the lack of skills and digital culture and different habits – lower usage (73% for 45-54 year olds, 57% for 55-64 and 39% for 65-74). This trend, however, is weaker in the more digitally mature Member States – in Denmark and Luxembourg, 86% and 82% of people aged between 55 and 64 years and 74% and 78% of those aged 65-74 used the Internet daily in 2017 (Fig. 1.2).

Analyzing Internet access by gender and, in particular,

Fig. 1.1 % of individuals who never used the Internet (2017)

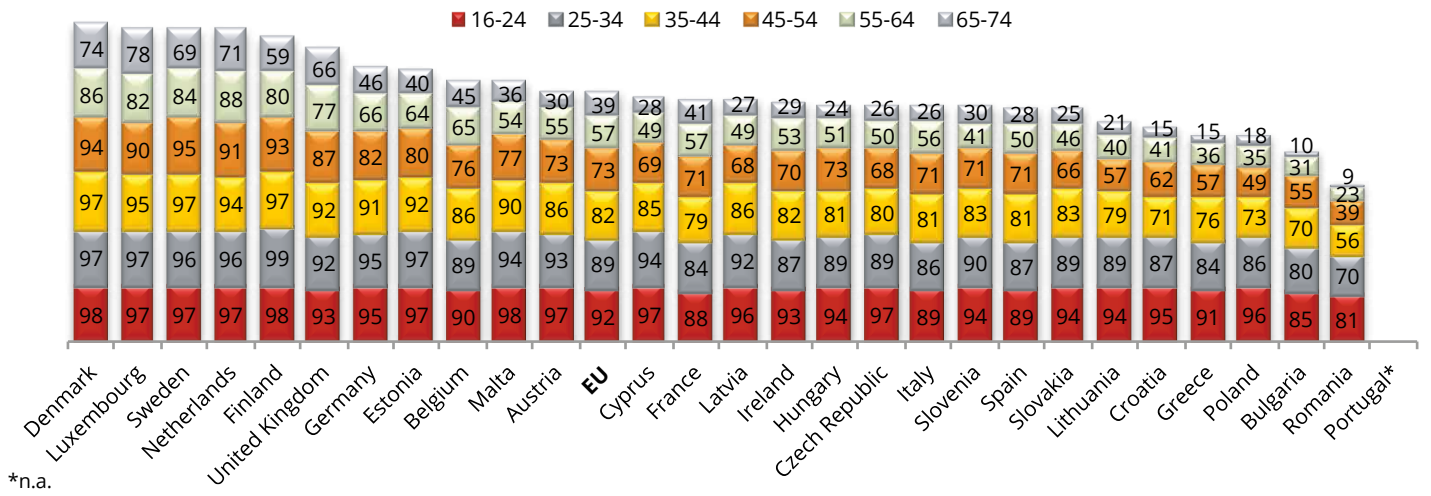
Source: Eurostat



*n.a.

Fig. 1.2 Daily Internet usage, by age bracket (% of individuals, 2017)

Source: Eurostat



*n.a.

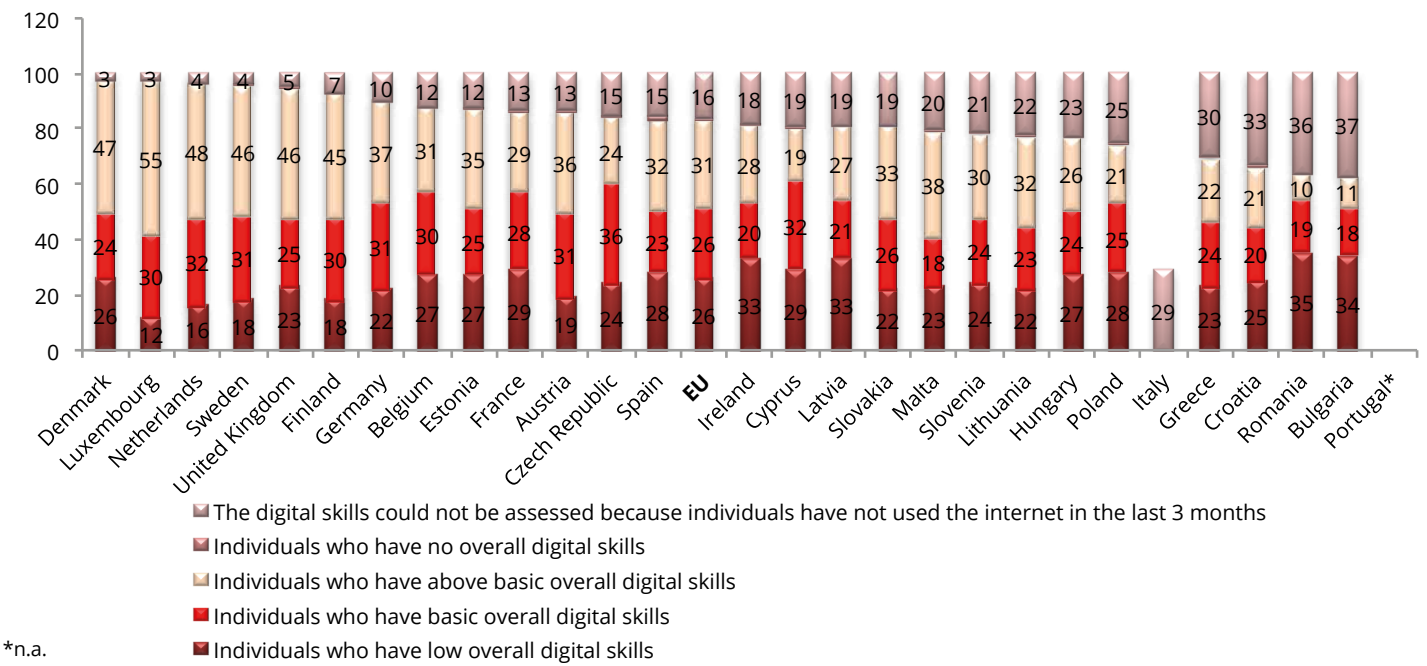
people aged between 16-24 and 25-54 years old, there was no gender difference in Internet access at a European level. In each age range access percentages are similar (only for individuals aged from 55 to 74 years there was a gap of 8% – males 53%, females 45%).

Countries with the highest percentages of Internet usage are also those where the highest percentages of households connected to the Internet and where individuals have above basic overall digital skills. In the Netherlands, Luxemburg, Finland, Sweden and the United Kingdom, 98%, 97% and 93%, respectively, of households are connected to the Internet and in Luxembourg, the Netherlands and Denmark, 55%, 48% and 47% of individuals have above average digital skills (Fig. 1.3).

Focusing on activities carried out online, at a European level, the most popular are sending and receiving emails (72% of individuals) and information searches for goods and services (65%), followed by participation in social networks and phone/video calls that concerned 56% and 39% of Europeans, respectively, in 2017 (Fig. 1.4).

Fig. 1.3 Individual level of digital skills (% of individuals, 2017)

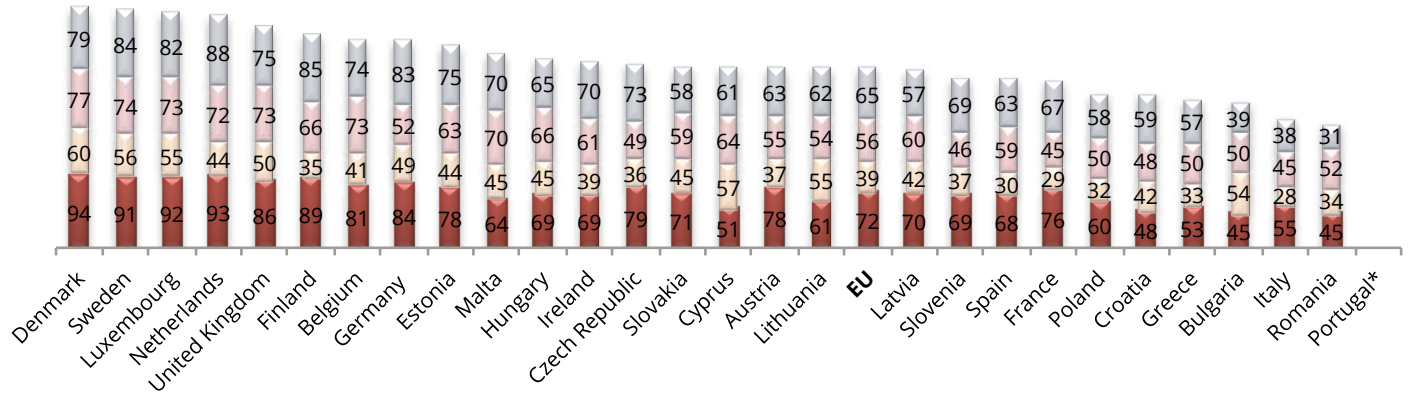
Source: Eurostat



*n.a.

Fig. 1.4 Internet use and activities (% of individuals, 2017)

Source: Eurostat



*n.a.

1.2. DIGITAL SERVICE PENETRATION IN EUROPE. INDIVIDUAL AND BUSINESS USE OF SOCIAL NETWORKS, E-COMMERCE AND INTERNET BANKING

1.2.1. Social networks

Social networks are one of the most interesting digital services to analyze. They have become, for individuals/consumers, the preferred domain to communicate, make new friends, share experiences and find information, whereas for businesses it has become one of the most important tools to promote their business and know their current or potential customers and competitors.

The 2018 Digital Report highlights the importance of the digital channel. It reveals that there are more than 4 billion people worldwide using the Internet, with the number of people using the top platform in each country increasing by almost 1 million new users every day during the past 12 months. More than 3 billion people worldwide now use social media each month, with 9 in 10 of those users accessing their chosen platforms via mobile devices. Globally, social media users have increased by 13 percent in the past 12 months (Fig. 1.5). Facebook is the most widely used platform with 2.167 million users, followed by Youtube and FB Messenger.

Focusing on the profile of Facebook users, Fig. 1.6 reveals a prevalence of males, with a prevalence of females only in the age group 55-64 and 65+.

Social networks are also a very important channel for citizens and enterprises in Europe, with Northern Europe being the best performer. In Denmark, Belgium, Sweden and the United Kingdom, the percentage of

Fig. 1.5 Annual growth of social media users (%, January 2018)

Source: Digital in 2018, We Are Social

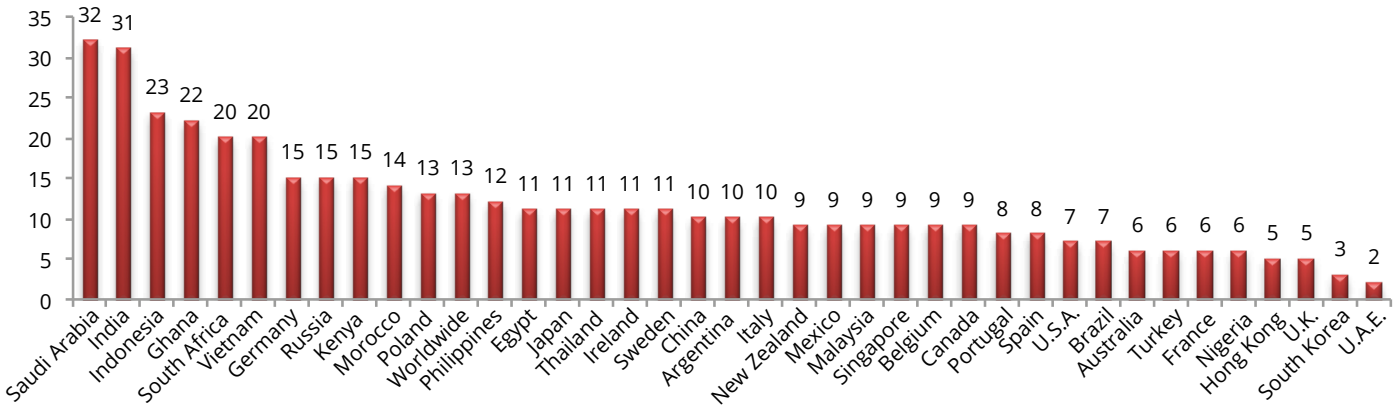
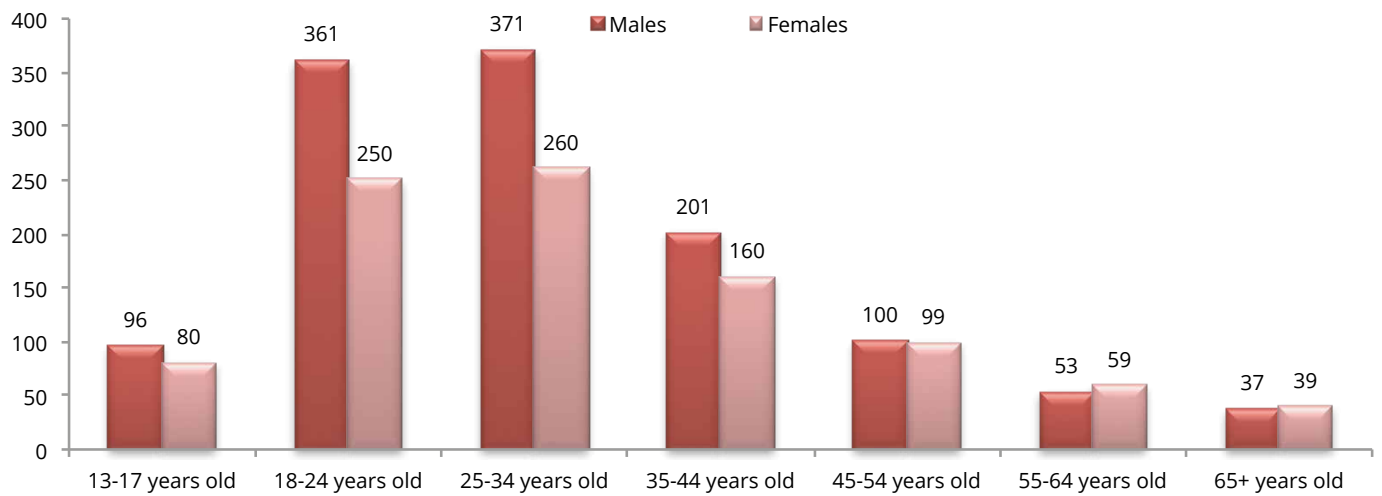


Fig. 1.6 Profile of Facebook users (millions, January 2018)

Source: Digital in 2018, We Are Social



individuals accessing social networks was 75%, 72% and 71%, respectively. Instead, the worst performers were Italy and France, Slovenia and Croatia where the percentage of individuals active on social media was 43%, 45% and 47%, respectively.

Individuals aged between 16-24, 25-34 and 35-44 were the most inclined to be on social networks at the European level and in the individual countries.

Social networks are also an important tool for businesses to promote their activity, offer customer support and analyze customer needs and market trends.

At a European level, and in Member States, in 2017, 68% of large companies showed a greater interest in using social networks (usually being more aware of digitalization opportunities and having more resources to invest in the digital channel). Focusing on national data, Malta was the best performer, even if, where large and medium enterprises were concerned, Cyprus registered higher percentages (Fig. 1.7).

1.2.2. E-commerce

In 2017, e-commerce registered a new peak with 1.6 billion worldwide users purchasing products online and spending almost $2 trillion, an amount that could double by 2020. Among the 10 countries with the highest penetration rates of online sales in mid-2017, we find China and South Korea (83%) at the top, followed by the United Kingdom (82%). The United States (77%) was in 7th position overtaken by Germany (81%) accomplishing an important growth (Fig. 1.8).

Fig. 1.7 % of enterprises using social networks (2017)

Source: Eurostat

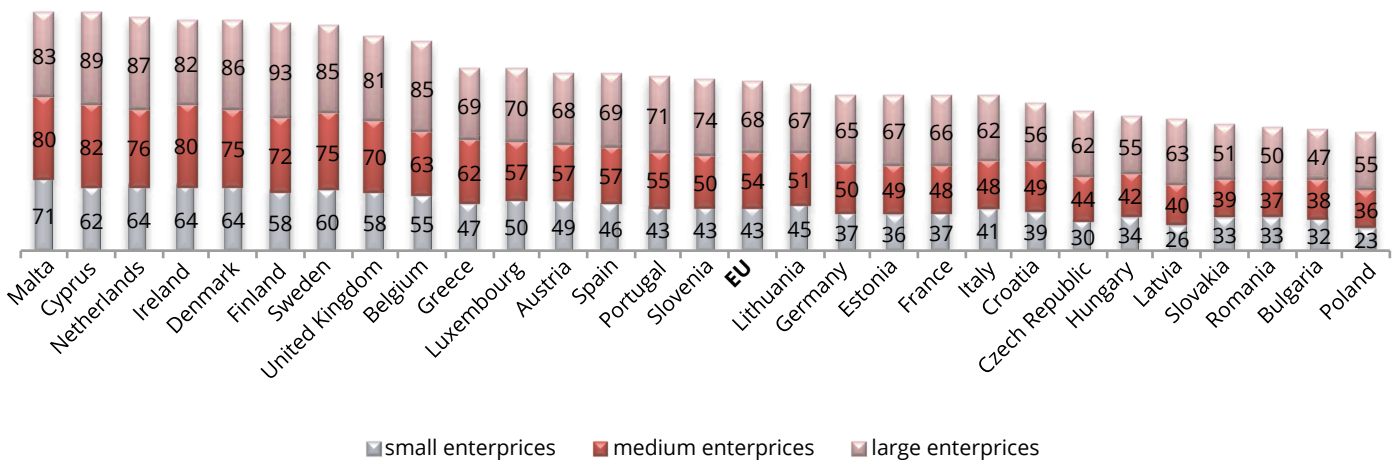
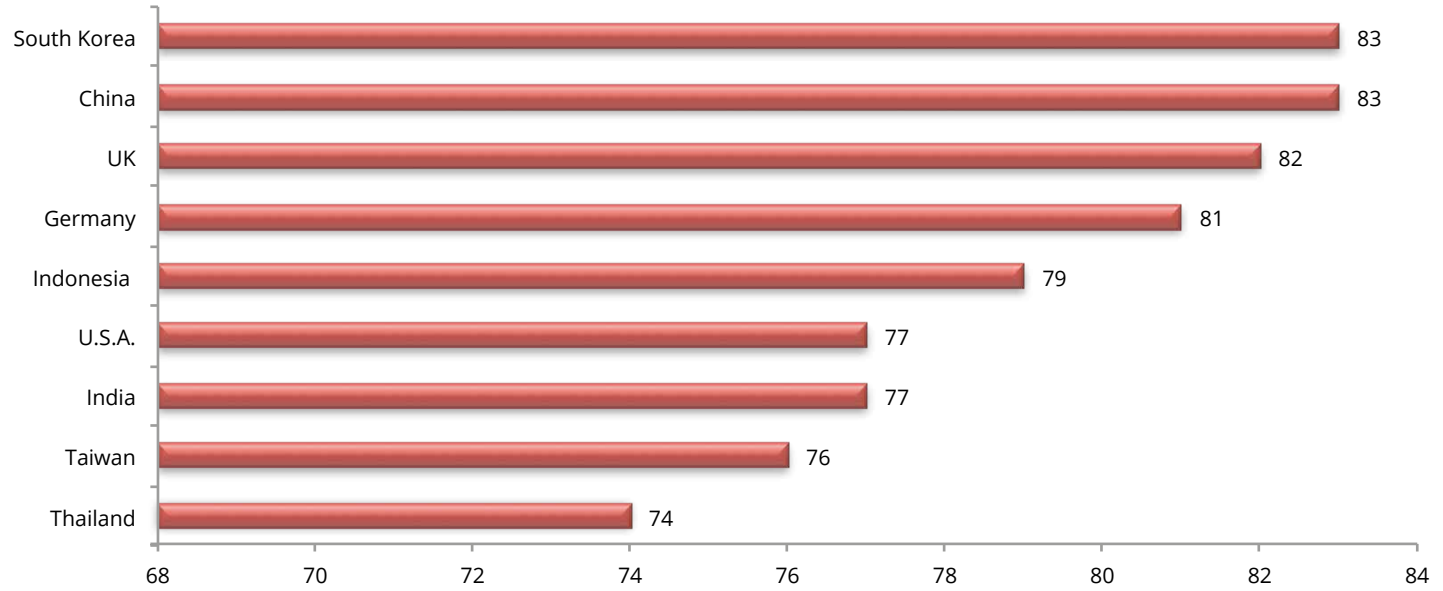


Fig. 1.8 Markets with the highest penetration rate of online shopping (%, 2017 2Q)

Source: statista.com



In Europe, in 2017, 65% of European individuals used the Internet to find information about goods and services and 57% bought online in the previous 12 months (Fig.1.9).

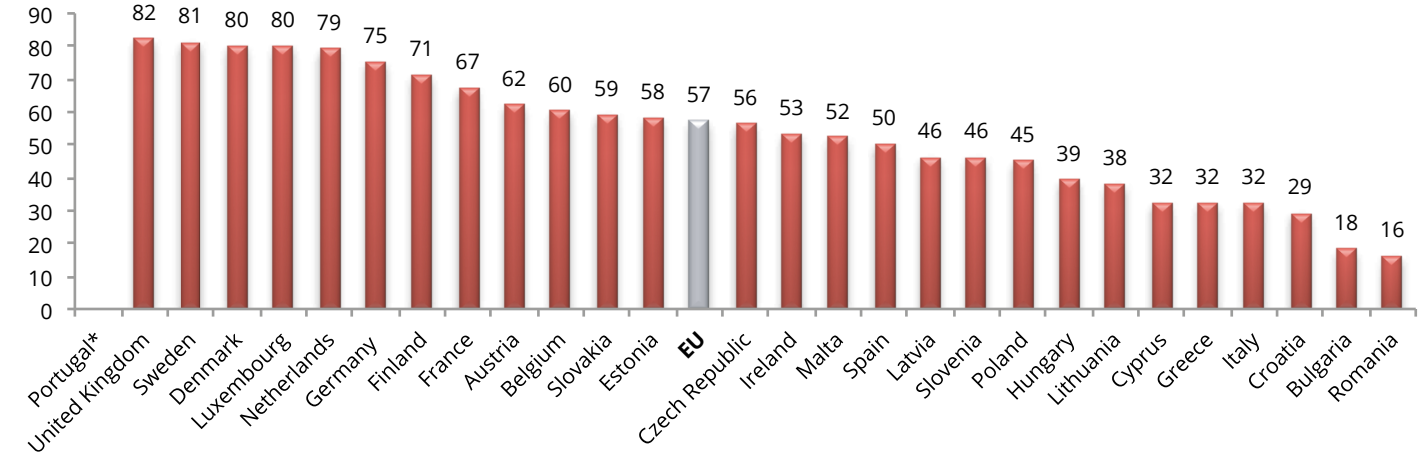
Regarding the nationality of sellers, it's interesting to note that in 2017 there was a clear preference for sellers from other EU countries rather than from non-EU countries (Fig. 1.10). For example, in Luxembourg, which topped the ranking, 77% of individuals bought from EU sellers while only 34% purchased from non-EU sellers.

Analyzing factors such as gender and age, no big differences were shown between males and females (at a EU level in each age bracket – with the exception of individuals aged between 55 and 74 years – males and females showed the same interest in online purchasing); while for age, individuals aged between 16 -24 years and 25-54 years were more active in online shopping.

As far as purchases are concerned, sporting goods and clothing are the primary targets (37%), followed by travel and holiday accommodation (31%) and household goods (26%). E-commerce's success is based on the low percentage of individuals facing problems

Fig. 1.9 % of individuals purchasing online in the last 12 months (2017)

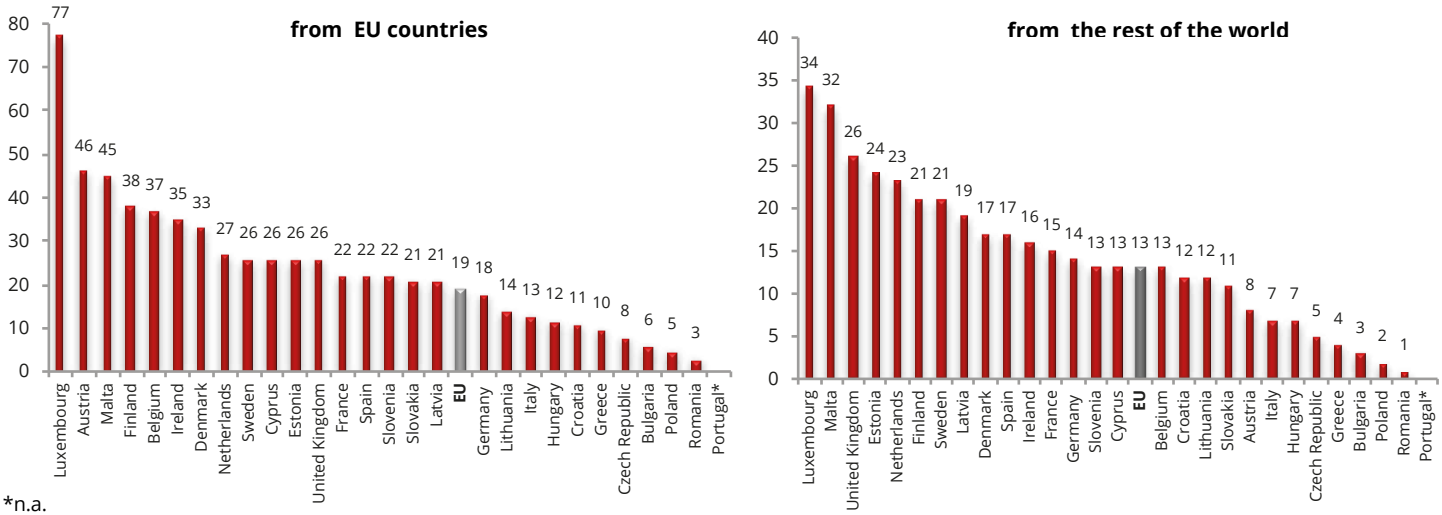
Source: Eurostat



*n.a.

Fig. 1.10 Online purchases (% of individuals, 2017)

Source: Eurostat

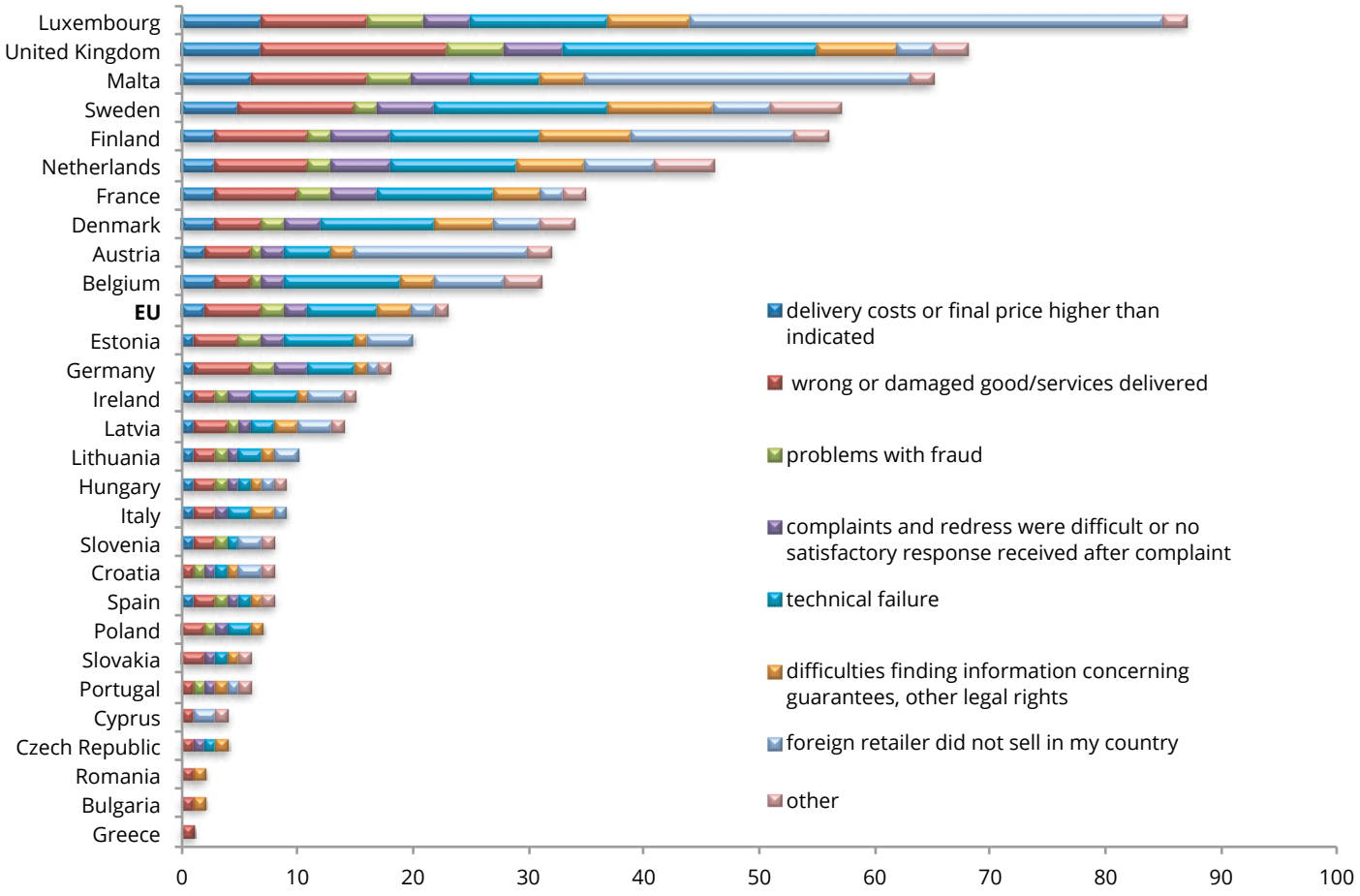


*n.a.

when making purchases over the Internet in Europe. (Fig. 1.11). However, it's interesting to note that one of the most important critical issues raised in some Member States involves the impossibility of making purchases from retailers not selling in some countries (41% in Luxembourg, 28% in Malta).

Fig. 1.11 Online purchases: problems encountered by individuals (2017)

Source: Eurostat



Focusing on enterprises, Eurostat data shows that especially large enterprises, having more resources to invest in digital and being more aware of e-opportunities, benefit from e-commerce (representing 26% of their turnover on average in the EU). Ireland was the best performer, with 42% and 23% of the turnover of large and medium enterprises, respectively, generated by e-commerce. Concerning small enterprises, the United Kingdom was the best performing country (35%).

Internet banking

Internet and mobile device penetration is reshaping the relationship between banks and customers, introducing new services and new ways of using traditional ones.

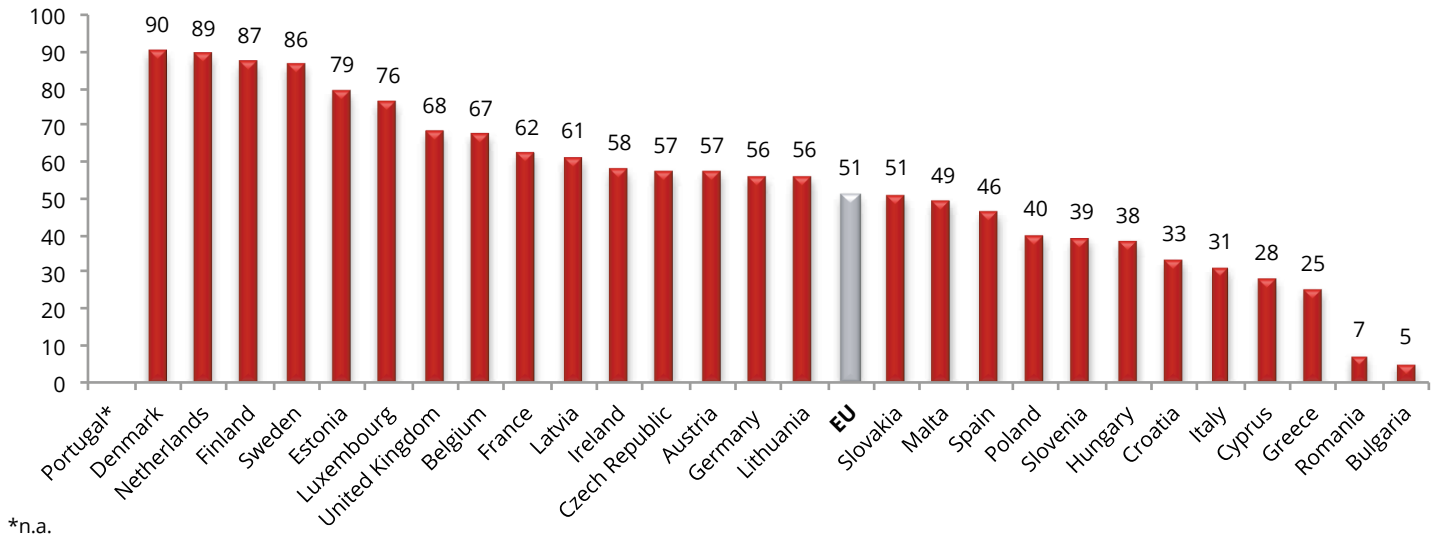
Denmark leads the EU ranking with 90% of individuals using Internet banking in 2017, followed by the Netherlands (89%) and Finland (87%); the lowest percentages, on the contrary, were registered by Bulgaria, Romania and Greece, with 5%, 7% and 25%, respectively (Fig. 1.12).

The highest percentage of users fall into the age groups of 25-34 year olds and 35-44 year olds. The best performers are Denmark, the Netherlands and Finland, with theworst, being Bulgaria, Romania and Greece (Fig. 1.13).

Overall in the EU, no gender differences were found in using Internet banking. For each age bracket, access percentages were similar (a significant difference – 8% – was found only for individuals aged between 55-74 years- males 40%, females 32%).

Fig. 1.12 Individuals accessing Internet banking (% of individuals, 2017)

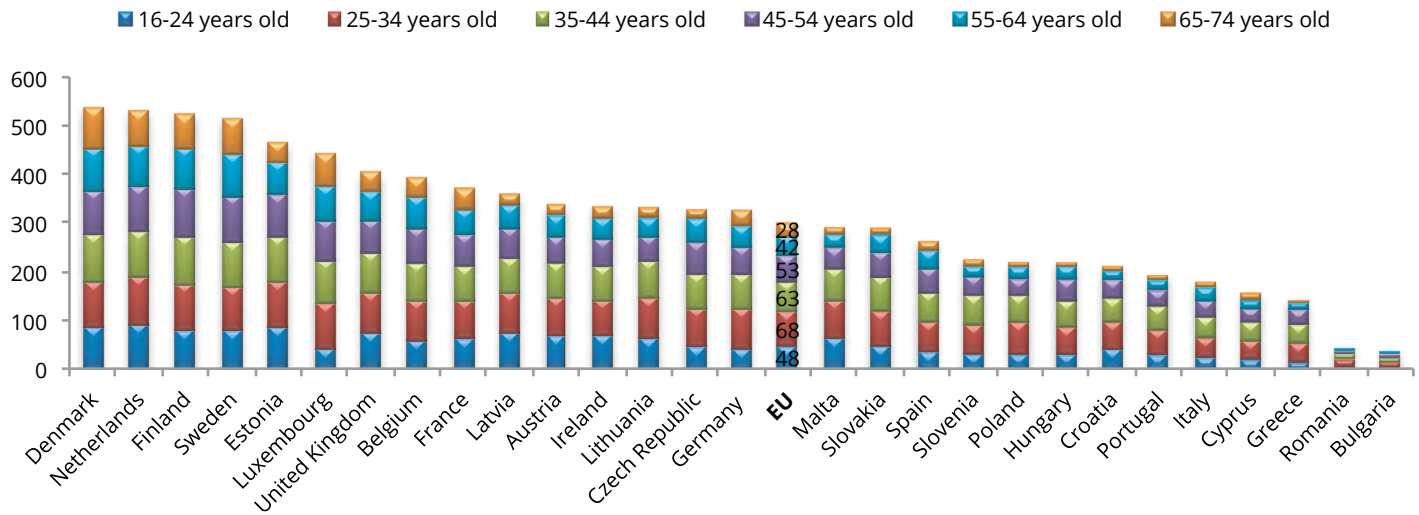
Source: Eurostat



*n.a.

Fig. 1.13 Individuals accessing Internet banking by age bracket (% of individuals, 2017)

Source: Eurostat



1.3. HOW MUCH IS THE DIGITAL ECONOMY WORTH?

The digital economy is developing rapidly worldwide and can be found in countless aspects of daily life, impacting sectors as varied as banking, retail, energy, transportation, education, publishing, media and health. Information and Communication Technologies are transforming how social interaction and personal relationships occur, with fixed, mobile and broadcast networks converging, and devices and objects increasingly connected to shape the Internet of Things. Progress in the development of the digital economy is regarded as critical to improve the competitiveness of the EU's economy. ICTs have quickly become an integral part of how enterprises function. Their extensive use has had a profound impact on how businesses are run, touching upon a range of aspects such as how they organize their internal communications, share their information with business partners, or communicate with their customers.

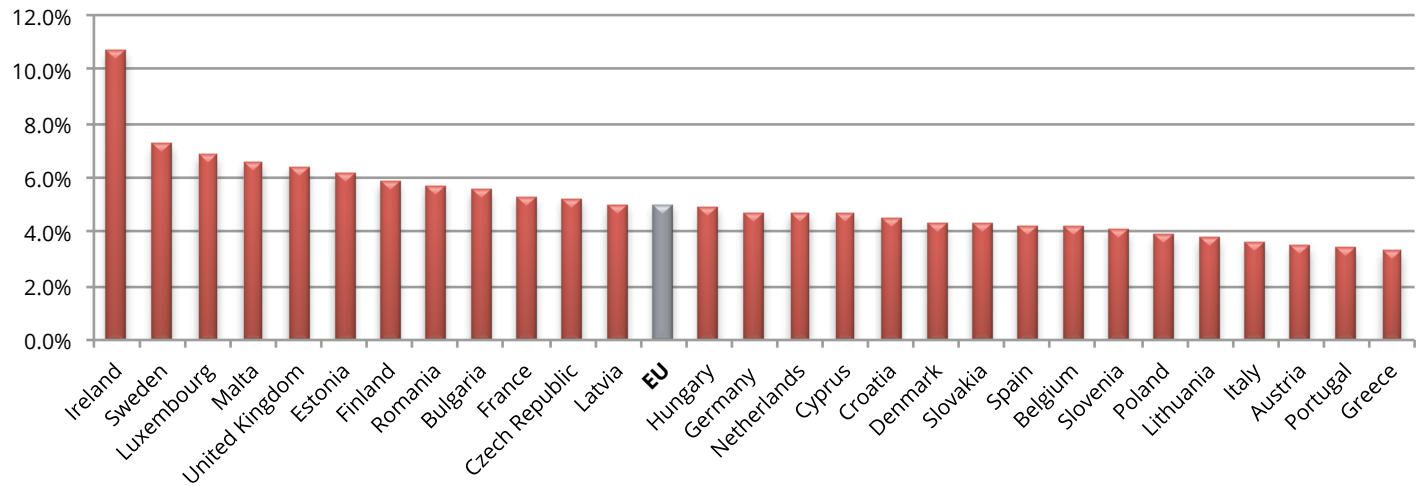
ICT investment and more effective ICT production and usage could give a very significant contribution to economic growth in Europe.

The value of the digital economy in terms of the contribution of Information and communication technology to GDP growth is estimated to be around 5% of total GDP in the European Union.

The economic impact of the Internet is growing and has a huge potential in all European countries. In Ireland, the digital economy contributed to 10.7% of the GDP in 2017, followed by Sweden and Luxembourg (7.2% and 6.8%, respectively), scoring above the EU average (Fig. 1.14). Instead, in other European countries, such as Greece, Portugal, Austria and Italy, the contribution of the digital economy to GDP was lower than 4%.

Fig. 1.14 Contribution of the digital economy to GDP (2017)

Source: I-Com elaboration on Eurostat data



PART 2

THE CHALLENGES OF THE DIGITAL REVOLUTION: A SAFER INTERNET

2. THE CHALLENGES OF THE DIGITAL REVOLUTION: A SAFER INTERNET

2.1. THE CYBERSECURITY THREATS IN THE INFORMATION AGE

The digital revolution has transformed everyday life. Thanks to the Internet, connecting people across the world has never been as easy as it is today. Moreover, the IoT (Internet of Things) has led to the spread of a mass of smart devices for people and businesses. This relatively new way of living (always accessible, everywhere and at every moment) has brought to light many new problems in terms of security, specifically cybersecurity.

According to the WEO Global Risks Perception Survey 2018, cyber risks intensified in 2017, so much so that cyber attacks and massive data fraud appear in the top five perceived global risks. For businesses, cyber breaches have almost doubled from 68 per business in 2012 to 130 per business in 2017.

The number and the financial costs of cyber attacks are also increasing. These recent events have different and broader impacts compared to those of the past decade. In 2017 alone, two attacks should be highlighted – WannaCry (in May) and Petya (in June). WannaCry hit, among others, the National Health Service in the United Kingdom, Nissan Motor Manufacturing UK and Renault. According to Cyence, the potential economic losses were estimated at $8 billion. Petya hit the Ukraine the most, where the Chernobyl Nuclear Power Plant went offline with an estimated loss of $850 million.

These examples reveal the dramatic change occurring in cyber events over a short period. If until few years ago, cyber attacks were more focused (every week a new retailer, healthcare provider, or financial institution lost sensitive data from their customers), now these attacks are more widespread, hitting, more or less simultaneously, several different companies and sectors worldwide.

As mentioned above, in recent years, the frequency and severity of cyber attacks has been intensifying. In Table 2.1, a list of the most common types of cyber threats to be aware of are reported.

Tab 2.1 Most common types of cyber threats

Source: I-Com

THREATS	WHAT IT IS	WHAT IT CAN DO
BOTs	Collection of software that creates an army of infected computers that are remotely controlled.	Send spam emails with viruses attached. Spread all types of malware. Can use computers as part of a denial of service attack against other systems.
DDoS (Distributed Denial of Service) attack	Network of bots used to damage a specific website or server, contacting those over and over again.	Shut-down the system, denying access to legitimate users.

Tab 2.1 Most common types of cyber threats

Source: I-Com

HACKING	The process by which cyber criminals gain access to computers.	Find weaknesses in security settings and exploit them in order to access information. Install a Trojan horse, providing a back door for hackers to enter and search for information.
MALWARE	Software that infects computers, such as computer viruses, worms, Trojan horses, spyware, and adware (advertising-supported software).	Attack computers through pop-up messages on security failing or other false problems. Reformat the computers causing the loss of information. Alter or delete files. Steal sensitive information. Send emails. Take control of computer.
PHARMING	A common type of online fraud.	Redirect users to an illegitimate website through a legitimate URL.
PHISHING/SPOOFING	Fake emails, text messages and websites created to look like they are from legitimate sources.	Trick users into giving them information by asking to update, validate or confirm the account data. Provide cyber criminals with users' username and passwords. Send spam to users' contact list.
RANSOMWARE	A type of malware that restricts access to computers or files and displays a message that demands payment in order for the restriction to be removed.	Display an image that prevents accessing the computer. Encrypt files on attacked system's hard drive and sometimes on shared network drives.
SPAM	A common method of both sending information out and collecting it.	Annoy users with unwanted junk mails. Create a burden for communications service providers and businesses to filter electronic messages. Phish for information by tricking users into following links or entering details with too-good-to-be-true offers and promotions. Provide a vehicle for malware, scams, fraud and threats to your privacy.
SPYWARE	It is used by third parties to infiltrate a user's computer.	Collect information. Send users' usernames, passwords, surfing habits to a third party. Change the way the computer runs. Take users to unwanted sites.
TROJAN HORSES	A malicious program that is disguised as, or embedded within, legitimate software.	Delete files. Use users' computers to hack into other computers. Watch through computer web cam. Log users' keystrokes. Record usernames, passwords and other personal information.

Tab 2.1 Most common types of cyber threats

Source: I-Com

VIRUSES	Malicious computer programs that are often sent as an email attachment, or a download, with the intent of infecting computers. Just visiting a site can start an automatic download of a virus.	Send spam. Provide criminals with access to users' computers and contact lists. Scan personal information like passwords. Hijack web browser. Disable your security settings.
WIFI EAVESDROPPING	A virtual "listening in" on information that is shared over an unsecure (not encrypted) WiFi network.	Potentially access users' computers with the right equipment. Steal personal information including logins and passwords.
WORM	A common threat to computers and the Internet as a whole.	Spread to everyone in users' contact lists. Cause a tremendous amount of damage by shutting down parts of the Internet, wreaking havoc on an internal network and costing companies enormous amounts in lost revenue.
KRACK	Allow a malicious actor to read encrypted network traffic on a Wi-Fi WPA2 router and send traffic back to the network.	Affect both personal and enterprise networks. Use vulnerability to steal sensitive information, and also insert malware or ransomware.
VULNERABILITIES	Human oversight or software vulnerabilities.	Expose the system to the aforementioned threats.

Basically, identity theft and sensitive data breaches emerged as the main serious issues related to cyber threats. Other significant issues that should be addressed are annoying and unsolicited messages and advertising.

2.2. GLOBAL CYBER ATTACK TRENDS

According to a 2017 Clusit study, out of a sample of 6,866 serious attacks[1] occurring worldwide between 2011 and 2017, 1,127 were recorded during the last year (+7.33%

1 Serious attacks are those with a significant impact on victims in terms of economic losses, damage to reputation, the dissemination of sensitive personal and non-personal data, or that herald particularly worrying scenarios.

Fig. 2.1 Number of cyber attacks

Source: I-Com elaboration on Clusit

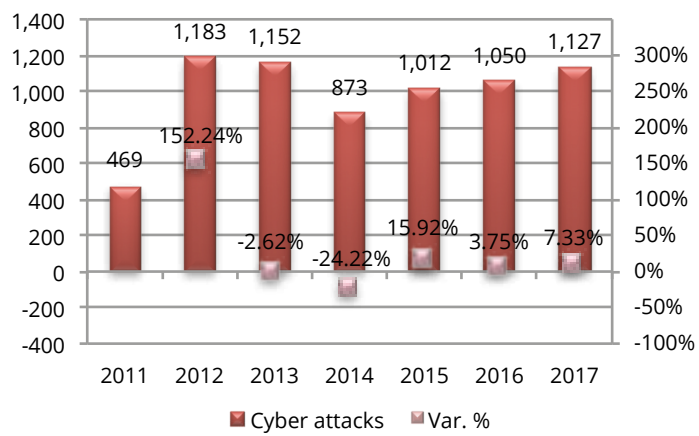


Fig. 2.2 Cyber attacker distribution over the last five years

Source: I-Com elaboration on Clusit

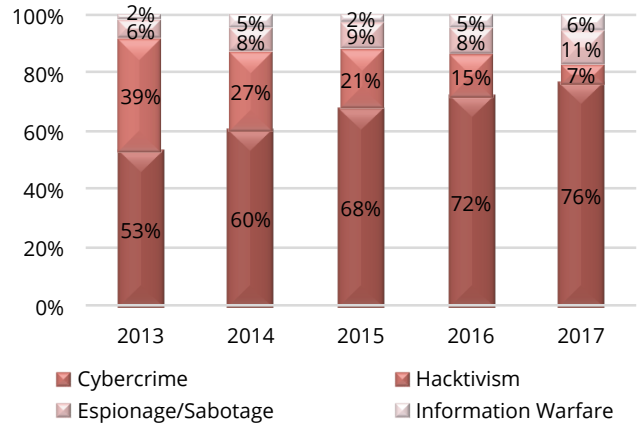
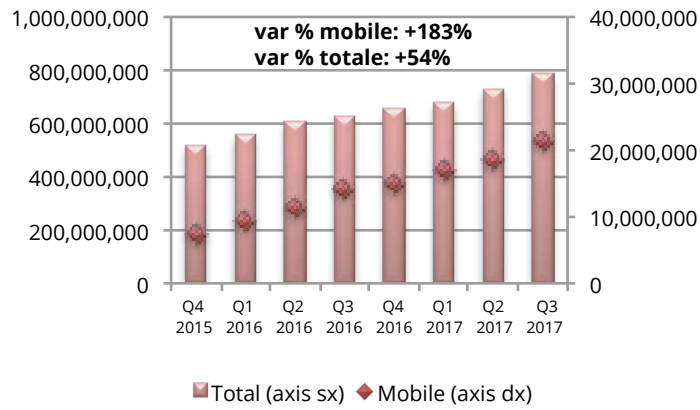


Fig. 2.3 Malware attacks

Source: I-Com elaboration on McAfee



compared to 2016) (Fig. 2.1).

In recent years, cyber crime, Cyber Espionage and Information Warfare have recorded high numbers of serious attacks (Fig. 2.2). Cyber crime has gradually been increasing, from 53% in 2013 to 76% in 2017, while hacktivist attacks have progressively decreased, from 39% to 7%, with 79 attacks during the last year. Cyber espionage and information warfare increased in 2017, by 47% and 24%, respectively.

Currently, Malware is the most widespread type of attack, accounting for a total of 787 million, of which 2.7% spread over the mobile network. Over 140 million new Malwares were detected between January and September 2017. According to McAfee, the rise in new malwares is in part due to an increase in malware installers and the Faceliker Trojan[2] (Fig. 2.3).

Ransom attacks also increased from 2015 to 2017, accounting for 12.5 million (+226% in the period). On the other hand, reaching 1.5 million, new ransomware rose by over 30% in the last observed quarter (Q3 2017), boosted by a big increase in Android screen-locking threats (Fig. 2.4).

Threat hunting is essential in cybersecurity, enabling attacker behavior to be studied and building more visibility into an attack chain. It is generally seen as a proactive approach to finding attacks and compromised machines without waiting for alerts. The underlying assumption is that, at every moment, there is at least one compromised system in the network. This results in a more proactive approach for security operations centers, shifting the focus on earlier detection, faster reaction times, and enhanced risk mitigation.

In May 2017, after the WannaCry and Petya attacks, McAfee surveyed more than 700 IT and security professionals

2 This tool is able to install itself on the browser and hijack the likes of the user on Facebook content that has never been viewed.

Fig. 2.4 Ransomware attacks

Source: I-Com elaboration on McAfee

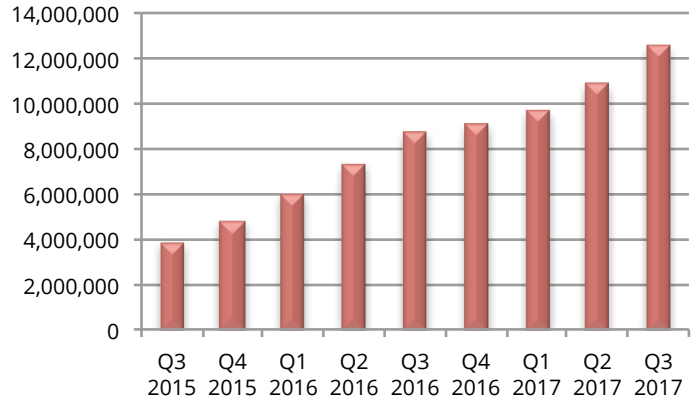
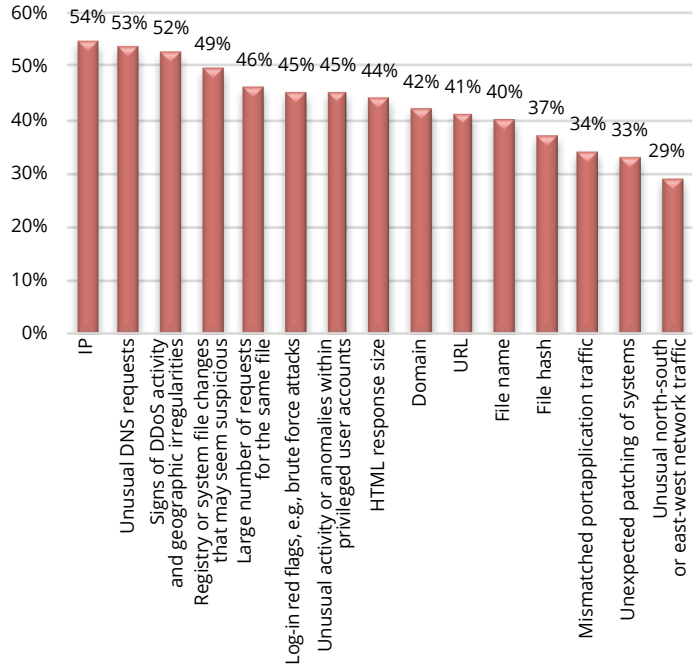


Fig. 2.5 Indicators of compromise

Source: McAfee



around the world to better understand how threat hunting is used in organizations today and how they plan to improve their threat hunting capabilities in the future.

Indicators of compromise (IOCs) can be used in threat hunting. Overall, the most common indicators of compromise, used by half or more of all respondents in the study, are: IP addresses, unusual domain name system (DNS) requests, signs of distributed denial of service activity and geographic irregularities, and suspicious registry of system file changes (Fig. 2.5).

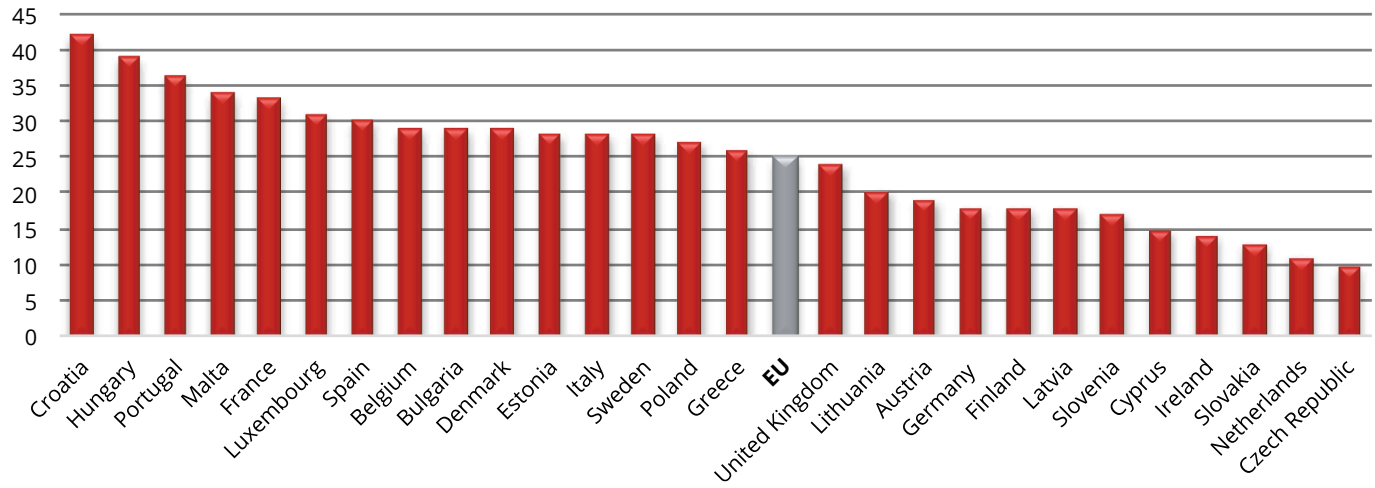
2.3. CYBERSECURITY IN EUROPEAN COUNTRIES

According to Eurostat data, in the EU, the share of Internet users having experienced certain common security issues over the Internet – such as viruses affecting devices, abuse of personal information, financial losses or children accessing inappropriate websites – stood at 25% in 2015 (Fig. 2.6). Across Member States, fewer than 15% of Internet users experienced security related problems in the Czech Republic (10%), the Netherlands (11%), Slovakia (13%) and Ireland (14%). On the contrary, Croatia (42%), Hungary (39%), Portugal (36%), Malta (34%) and France (33%) were above the European average.

Being infected by a virus or other computer infections (e.g. a worm or trojan horse) was the main problem. Slightly more than 1 Internet user out of 5 (21%) in the

Fig. 2.6 Share of Internet users who experienced security problems (% of individuals who used Internet whithin the last year, 2015)

Source: Eurostat



EU caught an online virus or other computer infection resulting in a loss of information or time. Across Member States, the share of Internet users having caught a virus was highest in Croatia (41%), followed by Hungary (36%), Portugal (33%), France (29%), Bulgaria and Malta (both 28%). In contrast, fewer than 10% of Internet users caught a virus or computer infection in the Netherlands (6%), the Czech Republic (8%) and Slovakia (9%).

Compared with 2010, the share of Internet users who caught a virus or other computer infection resulting in loss of information or time dropped in all Member States by 2015, except for Croatia. The most remarkable fall was observed in Slovakia (a decrease of 38 percentage points), followed by Bulgaria (-30 p.p.) and Latvia (-24 p.p.). At the EU level, the proportion of Internet users having caught a virus online decreased by 10 percentage points, from almost a third (31%) in 2010 to about a fifth (21%) in 2015 (Fig. 2.7)[3].

Privacy violations and abuse of personal information (e.g. abuse of pictures, videos, personal data uploaded on community websites) were experienced by 3.4% of Internet users in the European Union in 2015, even if a negative trend in most countries compared to 2010 can be seen. Malta, Italy and Spain were the countries with the highest number of Internet users experiencing personal data breaches (8.2%, 5.9%, 5%, respectively in 2015). On the contrary, Lithuania, Cyprus and the Czech Republic were the last in the ranking (Fig. 2.8). Compared with 2010, the most significant fall was observed in Latvia, Bulgaria and the Netherlands.

3 http://ec.europa.eu/eurostat/documents/2995521/7151118/4-08022016-AP-EN.pdf/902a4c42-eec6-48ca-97c3-c32d8a6131ef

Fig. 2.7 Individuals who caught a virus or other computer infection resulting in loss of information or time (% of Internet users)

Source: Eurostat

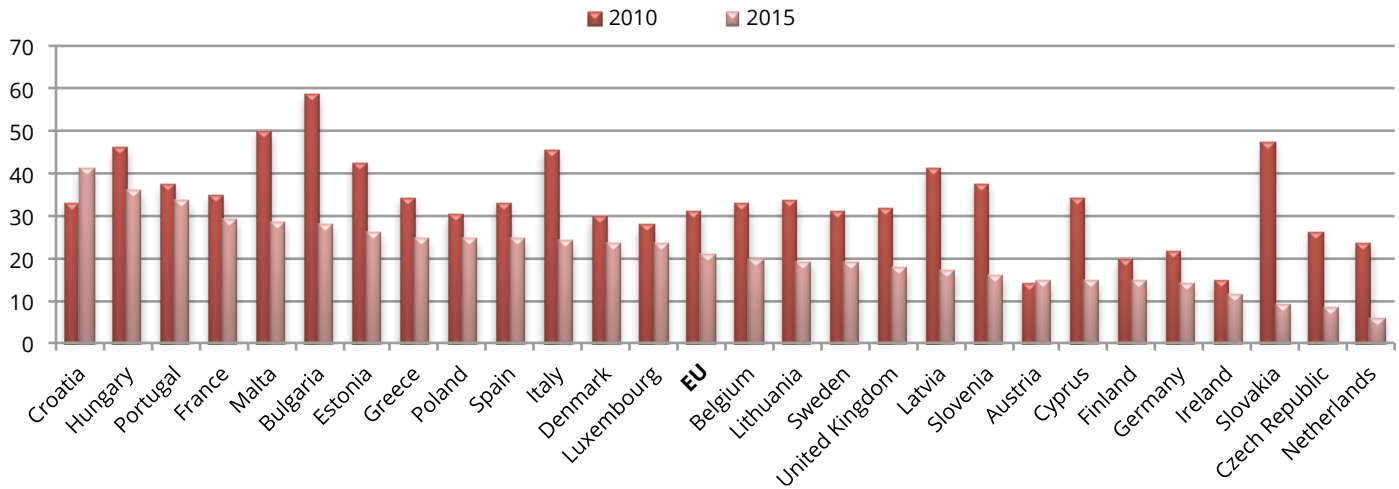
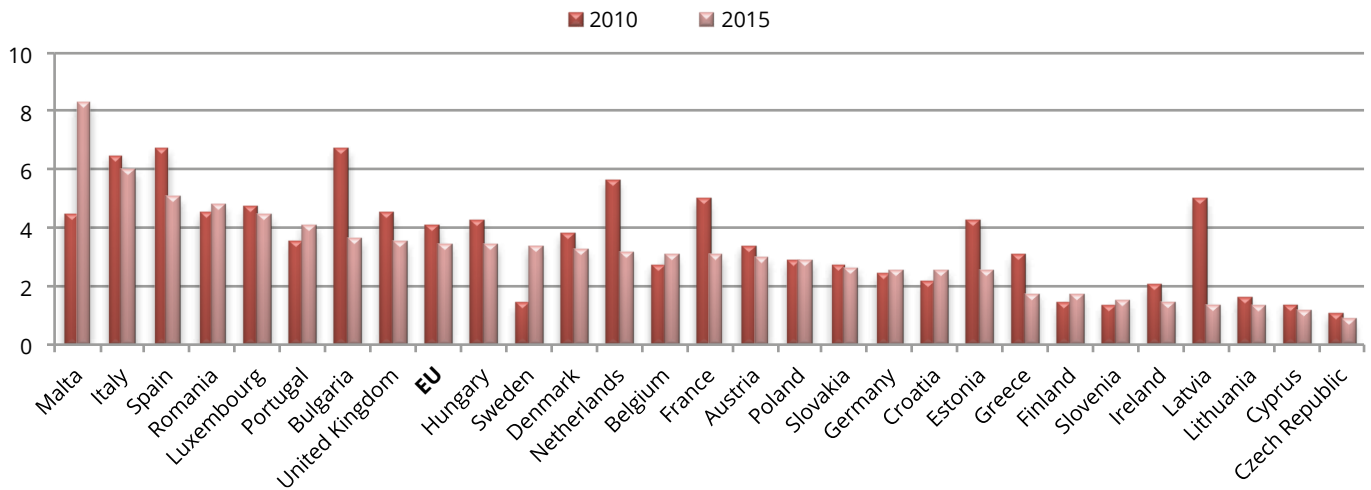


Fig. 2.8 Individuals who experienced abuse of personal information and/or other privacy violations (% of Internet users)

Source: Eurostat



Moreover, 3% of European individuals experienced financial losses while using the Internet. Among the EU Member States, 9% of Internet users in Belgium suffered from financial losses because of fraudulent messages, compared with very few in Estonia, Greece, the Czech Republic, Cyprus and Latvia. Compared with 2010, the share of Internet users experiencing financial losses has increased significantly in Belgium, Luxembourg, Denmark and Sweden, whereas in Latvia a marked drop was recorded (Fig. 2.9).

Security concerns prevented 24% of consumers from providing personal information to online communities for social and professional networking; ordering or buying goods or services online (15%); downloading software, music, video files, games or other data files (15%); carrying out banking activities online (14%); or communicating with public administrations across the EU-28 in 2015 (Fig. 2.10).

Fig. 2.10 Online activities avoided because of security concerns – EU (% of individuals)

Source: Eurostat

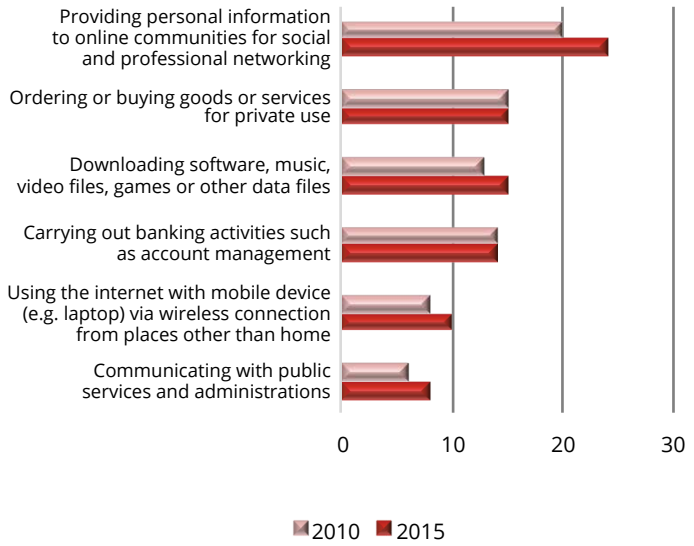
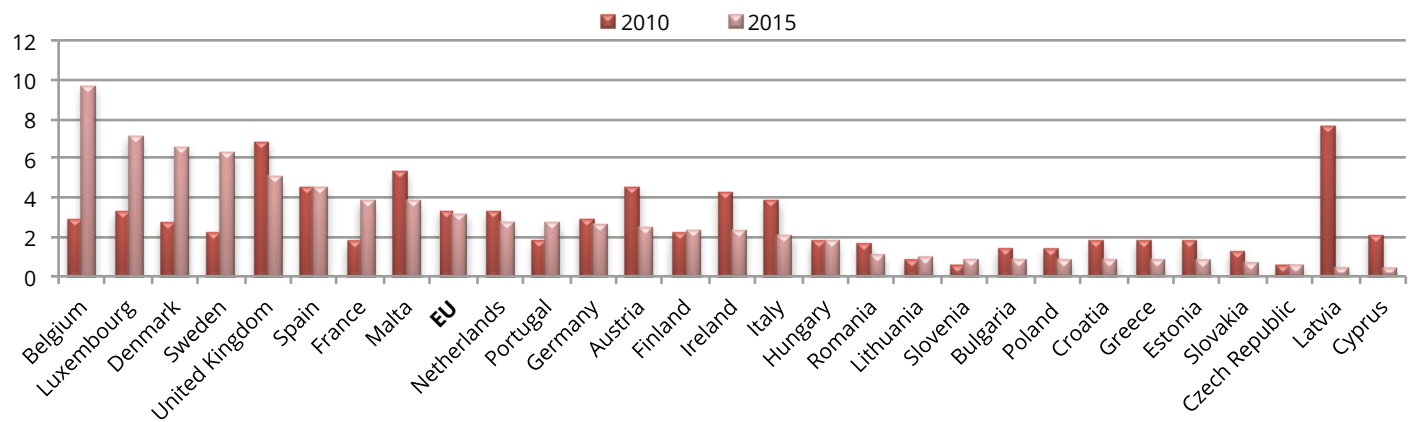


Fig. 2.9 Individuals who experienced financial losses (% of Internet users)

Source: Eurostat



According to the MMC CYBER HANDBOOK 2018, Europe's largest economies remain the top targets, but the focus varies broadly across the continent. In 2016, hackers most often targeted financial, manufacturing and telecom industries and governments in Germany (19%), Belgium (16%), Spain and Great Britain (12%), as well as in Italy, Sweden, Denmark and Finland, although the latter with a lower percentage (Fig. 2.11).

The three industries drawing the greatest attention in Europe in terms of malware were financial services, manufacturing and telecommunications. From January to September 2016, the number of malware events targeting financial services was over 50, while in manufacturing and telecommunications was 49 and 40, respectively. The industries less affected were retailing, transportation and entertainment (Fig. 2.12).

Fig. 2.11 Targeted malware detection (Jan-Sep 2016)

Source: MMC CYBER HANDBOOK 2018

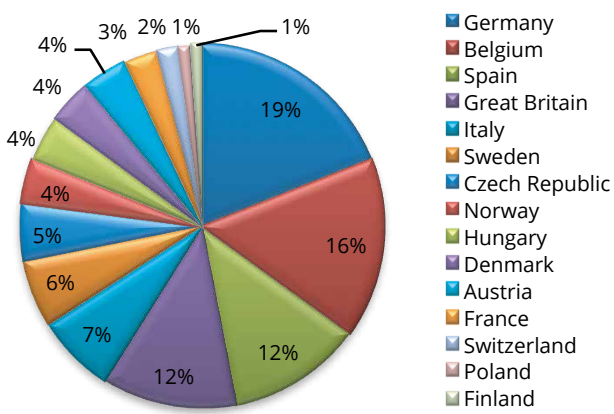
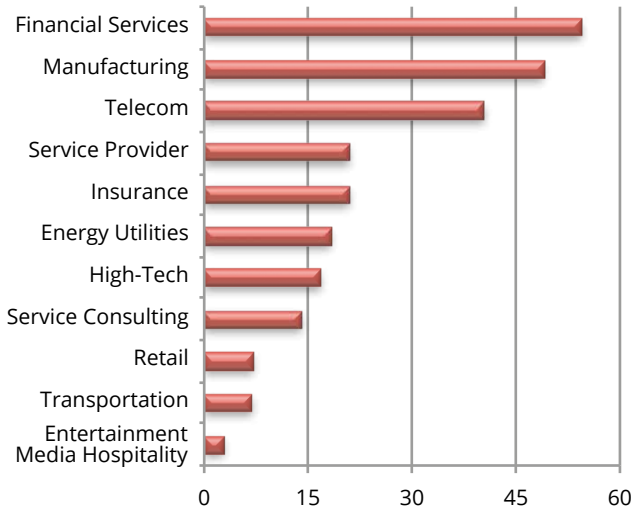


Fig. 2.12 Targeted malware detection across Europe (number of events, Jan-Sep 2016)

Source: MMC CYBER HANDBOOK 2018



2.4. THE EUROPEAN REGULATORY FRAMEWORK

Privacy and network security are essential to ensure high cybersecurity standards in the European Union.

Cybersecurity strategy

The massive spread of digital services is causing a huge increase in cyber crime, bringing the cybersecurity challenge to the center stage.

Since the adoption of the EU Cybersecurity Strategy in 2013, the European Commission has planned actions to better protect Europeans online. In particular, the **EU Cybersecurity Strategy**, launched in 2013, established

5 priorities: 1) increasing cyber resilience; 2) drastically reducing cyber crime; 3) developing an EU cyber defense policy; 4) developing the industrial and technological resources for cybersecurity; and 5) establishing a coherent international cyberspace policy for the EU.

Following on from this strategy, several initiatives emerged from both the European Commission and the European Parliament.

A European Agenda on Security was launched by the European Commission in 2015, setting 3 priorities – terrorism, organized crime and cybercrime – and proposing, with regard to the latter, the following actions:

- placing renewed emphasis on the implementation of existing policies on cybersecurity, attacks against information systems, and fighting child sexual exploitation;
- reviewing and possibly extending legislation on fighting fraud and counterfeiting of non-cash means of payments to take account of newer forms of financial tool crime and counterfeiting;
- reviewing obstacles to criminal investigations on cyber crime, notably on issues of competent jurisdiction and rules on access to evidence and information;
- enhancing cyber capacity-building action under external assistance tools.

The **Regulation on Electronic Identification Authentication and Signature (EIDAS)** entered into force on September 17, 2014 and became applicable starting from July 2016, in the field of electronic identification and trust services for electronic transactions in the internal market, and representing another important measure to increase security in the European Union.

It provides a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities. More specifically, it ensures that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available and creates a European internal market for eTS – namely electronic signatures, electronic seals, time stamps, electronic delivery services and website authentication – by ensuring that they will work across borders with the same legal status as traditional paper-based processes. Only by providing certainty on the legal validity of all these services, will businesses and citizens begin using the digital interactions as their natural way of interaction.

This regulation provides for a predictable legal framework for individuals, companies (in particular, SMEs) and public administrations to safely access services and carry out transactions online and across borders. Indeed, rolling out eIDAS means higher security and more convenience for any online activity such submitting tax declarations, enrolling in a foreign university, remotely opening a bank account, setting up a business in another Member State, authenticating Internet payments, bidding in online tender calls and so on.

On July 6, 2016, **Directive 2016/1148** (c.d. NIS Directive) was adopted, setting measures for a common high level security for networks and information systems in the Union. This is of extreme importance as, for the

first time, the cybersecurity challenge has been tackled, revolutionizing cybersecurity in Europe. The Directive recognizes that network and information system security is essential for economic and social activities and, above all, for the functioning of the internal market.

To this end, the Directive: 1) has prescribed Member States to adopt a national strategy on network security and information systems; and 2) has established a cooperation group to support and facilitate strategic cooperation and information exchange among Member States and to build trust among them. This group is made up of representatives from the Member States, the Commission and ENISA and carries out its activities on the basis of two-year work programs; 3) creates a network of cybersecurity action teams in the event of an accident to contribute to the development of trust among Member States and to promote rapid and effective operational cooperation; 4) establishes security and notification obligations for operators of essential services and for digital service providers; 5) mandates Member States to identify competent national authorities, single contact points and CSIRTs with tasks related to network security and information systems.

The national strategy must regulate several aspects, in particular, the objectives and priorities, a governance framework to achieve the objectives and priorities set, the identification of preparedness, response and recovery measures, including collaboration between the public sector and the private sector, the indication of training, awareness and education programs, research and development plans and a risk assessment plan (Article 7).

The NIS Directive also requires Member States to designate one or more competent authorities to control the application of the directive at national level. A single point of contact should be designated by each Member State, to ensure international cooperation and connection with other nations through the cooperation mechanisms identified in the directive itself.

Finally, each Member State must designate one or more Computer Security Incident Response Team (CSIRTs) responsible for monitoring incidents at the national level, providing timely alerts and announcements with the aim of disseminating information on risks and incidents.

Cooperation among institutions of individual Member States is a crucial part of the NIS directive. To this end, a cooperation group consisting of representatives of the Member States, the Commission and ENISA was set up with four areas of work – planning, guiding, reporting and sharing.

The last of the main points of the directive concerns operators of essential services for the nation and providers of digital services. In particular, public or private companies operating in energy, transport, banking and healthcare, in financial market infrastructures, in the supply and distribution of drinking water and in the digital infrastructures must adopt security measures able to prevent risk, guarantee the security of systems, networks and information and manage accidents.

As well, digital service providers – meaning the digital services online market, online search engines and cloud services (cloud computing) – will be required, according to the NIS directive, to implement appropriate security

measures and to notify relevant incidents. In addition to the measures already envisaged for operators of essential services, the NIS Directive prescribes other specific security measures for digital service providers, such as the security of systems and installations, the management of business continuity, monitoring and testing, and compliance with international standards. The transposition process must be completed in each Member State by May 9, 2018.

In September 2017 the Commission launched the **Strategic Plan for Cybersecurity**. The Plan aims to increase defense, deterrence and the resilience of information systems, based on three fundamental pillars: 1) building a resilient European system increasing the level of cybersecurity in the European Union; 2) creating an effective and univocal response to computer crimes, adapting penalties to the seriousness of the criminal action; and 3) encouraging international collaboration.

One of the most important aspects of the proposal concerns the creation of a European Agency on Cybersecurity – the result of the strengthening of the already existing European Union Agency For Network And Information Society (ENISA) – with a full and permanent mandate, with more tools and targets, to come into effect by 2020, when the current Agency mandate will expire. Ongoing training in security systems tops the objectives. The Agency will simulate computer attacks to allow Member States, in coordination with the European institutions and their agencies, to prepare forms of response to potential attacks, improving information and intervention times, thanks also to the creation, by 2018, of a platform for training.

Concerning collaboration among Member States, the proposal aims to set up a research center in 2018, to address the important topic of R&D investment in new technologies.

The EU plan also aims to create a single system certification of cybersecurity to overcome the fragmentation currently existing with the presence of 4 main certifications (CPA, CSPN, BSPA, SOG-ISMRA) and to increase reliability, in terms of security, of purchased products.

Last, but certainly not least, a review of the criminal policy in the Member States. Here, the Commission encourages greater uniformity in the penalties applied in the Member States and the affirmation of the right of access to information by the victims of such crimes. It offers an adequate and simple assistance system and the creation of a close collaboration within the Union's whole judicial system, through strengthening existing structures and local Contact Points.

Data protection

To ensure cybersecurity, privacy regulation is very important. In early 2016, the Parliament reformed the legal framework on data protection and issued the **General Data Protection Regulation (GDPR**) – Regulation 679/16 –, aiming at protecting all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from when the 1995 Directive was established.

The GDPR sets the foundations for the lawfulness of data processing, strictly indicated times, contents and modalities of information, defines the rights of

the interested parties (access, cancellation-forgetting, limitation of treatment, opposition, portability), identifies the subjective characteristics and responsibilities of owners and data controllers and regulates international data transfers.

The key-principle of the discipline is that of "privacy by design", by which we refer to the choice of guaranteeing data protection rights from the planning and design stage of a treatment preventing possible critical issues (for example, the provision of impact assessments before data processing).

Concerning subject-matter and objectives, the GDPR lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules related to the free movement of personal data and protects the fundamental rights and freedom of natural persons, particularly, their right to personal data protection. In establishing the principles related to personal data processing, art. 5 states that personal data shall be processed lawfully, fairly and in a transparent manner relative to the data subject, collected for specified, explicit and legitimate purposes. It should not be further processed in a manner that is incompatible with those purposes, but be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed, being accurate, and kept in a form which permits the identification of data subjects and stored for no longer than is necessary for the purposes for which the personal data is processed, ensuring appropriate personal data security.

The following art. 6 sets the conditions for the lawfulness of processing and, in particular, in the presence of a consent given by the data subject, when processing is necessary for carrying out a contract to which the data subject is party, or in order to take steps to meet the request of the data subject prior to entering into a contract. Therefore there is a legal obligation to which the controller is subject, in order to protect the vital interests of the data subject or of another natural person, for the performance of a task carried out in the public interest or in the exercising of official authority vested in the controller and for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular, where the data subject is a child.

Regarding consent, art. 7 establishes that the data controller must prove the presence of consent, stating that if it is provided through a written declaration also covering other issues, the request for consent must be presented in a manner clearly distinguishable from other subjects, in a comprehensible and easily accessible form, using a simple and clear language. The same provision recognizes the right of the interested party to withdraw their consent at any time, providing that the withdrawal of consent is expressed with the same ease with which consent is granted.

Art. 15, instead, recognizes the data subject's right of access to data and some information concerning the purpose of the processing and defined the categories of data in question, the recipients or categories of

recipients to whom the personal data have been or will be communicated, the retention period of the personal data, the existence of the right of the interested party to ask the data controller to rectify or delete personal data or limit the processing of personal data concerning them or to oppose their treatment, the right to lodge a complaint with a supervisory authority, if the data are not collected from the data subject, with all information available on its origin, as well as the existence of an automated decision-making process.

Art. 17 establishes the right to erasure ("right to be forgotten"), setting the right of the data subject to obtain from the controller the erasure of personal data concerning them without undue delay and the obligation – in the presence of specific conditions – of the controller to erase personal data without undue delay.

Other important provisions concern the right to data portability (art. 20) and the right of the data subject to receive the personal data in a structured, commonly used and machine-readable format with the right to transmit said data to another controller.

Chapter IV on the controller and processor, instead, establishes features of their responsibility, fixes the obligation to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, encourages the drawing up of codes of conduct intended to contribute to the proper application of the Regulation, provides the establishment of data protection certification mechanisms and of data protection seals and marks for the purpose of demonstrating compliance with the Regulation of processing operations by controllers and processors. The GDPR also regulates transfers of personal data to third countries or international organizations fixing the general principle for transfers and specific exceptions.

The same Regulation defines competences, tasks and the powers of authorities, cooperation modality and the characteristics and powers of European data protection Board.

Considering that this regulation required that Regulation (EC) 45/2001 was adapted to the principles and rules established in Regulation (EU) 2016/679 in order to provide a solid and consistent data protection framework in the Union, on January 10, 2017, a **proposal for a regulation concerning the protection of individuals concerning the processing of personal data by the institutions, authorities, offices and agencies of the Union, as well as free data movement** was launched, repealing Regulation (EC) 45/2001 and decision n. 1247/2002 / EC. This proposal aims to align the current rules, which go back to 2001, to the new stricter rules set out in 2016, guaranteeing higher standards of protection. The proposed regulation, conforming to the model and the general discipline established by Regulation 2016/679, identifies the principles applicable to the processing of personal data (lawfulness, correctness, transparency, adequacy, relevance, limitation) and the conditions for consent, regulating the transmission of personal data to recipients, other than Union institutions and agencies, established in the Union and subject to Regulation (EU) 2016/679 or Directive (EU) 2016/680. It identifies the situations in which the processing does not require

identification, clearly declines the rights of the data subject (right of access to data, rectification, oblivion, right to limit processing, data portability, objection to processing), obligations and responsibilities, and it introduces with regard to transfers of personal data to third countries or international organizations the principle of adequacy and provides specific means of appeal. From an institutional point of view, this proposal for a regulation establishes a European Data Protection Supervisor, setting tasks and powers and the forms of cooperation with the individual national authorities.

The Commission also proposed the **regulation on confidentiality and electronic communications** aimed at guaranteeing greater protection of people's private life and offering new business opportunities. Furthermore, the proposal, starting from the observation of the importance for Europeans to maintain the confidentiality of e-mails and online messages and the necessity to define a unitary protection within the Union and the applicability of the current ePrivacy Directive only to traditional telecommunications operators, provides for the extension of privacy rules to new operators providing electronic communication services (such as WhatsApp, Facebook Messenger, Skype, Gmail, iMessage, Viber) and specifies that this protection covers contents and metadata of electronic communications (for example, call time and location). Fixing a single set of rules applicable within the Union, the Commission also aims to create new business opportunities for companies and, in fact, once consent is given to the processing of communications data (content and/or metadata), traditional telecommunication operators will have more opportunities to use the data and provide additional services. In order to ensure users greater control over the settings, allowing for easy acceptance or refusal of the monitoring of cookies and other identifiers in the event of risks to privacy, the proposal provides for the simplification of the so-called "cookie provision" which has resulted in an excessive number of requests for Internet user consent. The proposal clarifies that consent is not necessary for non-intrusive cookies that improve the user experience (for example, those that allow you to remember shopping cart history) and for cookies that count the number of users visiting a website. The proposal also introduces measures against spam, prohibiting unwanted electronic communications through emails, text messages and, in principle, also telephone calls if users have not given their consent. To complete the set of protections, the proposal imposes the authors of telephone calls for commercial purposes, the obligation to show their telephone number or use a special prefix that indicates the nature of the call. As far as the competence to ensure compliance with this framework is concerned, the national data protection authorities are identified as the responsible parties.

Returning to the data protection area, a **proposal for a regulation of the European Parliament and of the Council on a framework for the free movement of non-personal data in the European Union** was adopted on September 13, 2017. This proposal, after specifying the objective, the scope of the regulation and the applicable definitions establishes: 1) the principle

of free movement of non-personal data in the Union (Art. 4: any obligation to locate data is prohibited, except when this is justified for public security); 2) ensuring the availability of data for regulatory controls by the competent authorities, prohibiting users from rejecting data access for the competent authorities on the basis that the data is stored or otherwise processed in another Member State; 3) encouraging service providers and professional users to develop and implement codes of conduct that specify information on data portability conditions (including technical and functional requirements); 4) providing the designation, by each Member State, of a single point of contact which acts as a link with the contact points of the other Member States and the Commission regarding the application of the Regulation; 5) providing for the Committee on Free Movement of Data, assisting the European Commission; and 6) carrying out a review within five years from the date of application of the regulation.


PART 3
THE IMPACT OF CYBERSECURITY ON ENTERPRISES

3. THE IMPACT OF CYBERSECURITY ON ENTERPRISES

3.1. BUSINESS IN THE CROSSHAIRS OF CYBER CRIMINALS

The digital transformation has become imperative for all businesses – small, medium and large – that operate in every economic sector (telecommunications, financial services, manufacturing, energy, healthcare, automotive, etc.). Not every company delivers goods and services primarily through digital channels, but all of them need technologies from the Internet era to be competitive. Nowadays, however, it is very difficult for organizations to map the digital environment in which they operate, or their interactions with it because every asset owned or used by the organization represents another node in the network. For this reason, "*organizations must think of themselves as having long and trailing tentacles in every direction*" [1].

The digital environment is very vast and it is an ideal ground for cyber attacks, that can be either indiscriminate or highly targeted, aiming at large and small organizations in both the public and private sectors. Therefore, Internet usage and its connected devices offer new opportunities for companies but, at the same time, create new risks. The range of potential attacks and attackers is wide and becoming more so by the day. The new technologies, mobiles, and smart devices connected to the Internet of Things expose every organization to attackers, offering them, for example, an opportunity to shut down or subvert industrial control systems. The threat may even be more dangerous – imagine an attacker able to turn off life support systems in hospitals or take control of connected cars on the road.

In an increasingly digitalized world, cybersecurity has jumped to the top of the company risk agenda after a number of high profile data breaches, ransom demands, Distributed Denial of Service (DDoS) attacks and other hacks have occurred over the last years.

According to a global survey[2], 86% of surveyed executives said that their company experienced a cyber incident or information/data theft, loss, or attack in 2017 (+1% over 2016). The respondents reported falling victim to different types of cyber incident (virus/worm infestation, phishing, data breach and data deletion, ransomware, denial of service). The most frequent type of cyber attack reported by 36% of respondents was a virus/worm, with an increase of 3 percentage points year on year. Instead, 33% of interviewees reported suffering from an email-based phishing attack. Additionally, data breach and data deletion impacted on 27% and 25% of respondents, respectively. Finally, ransomware and denial of service attacks were the two last categories of cyber threat reported by 18% of respondents (Fig. 3.1).

No sector of the economy is immune to attack – neither industry, nor government and not even the non-profit sector. Cyber criminals are increasingly targeting power grids, chemical plants, aviation systems, transportation

1 EY, *Cybersecurity regained: preparing to face cyber attacks*. 20th Global Information Security Survey 2017–18, 2017

2 Kroll, *Global Fraud & Risk Report*, 2018

Fig. 3.1 Types of cyber attacks

Source: Kroll, Global Fraud & Risk Report 2018

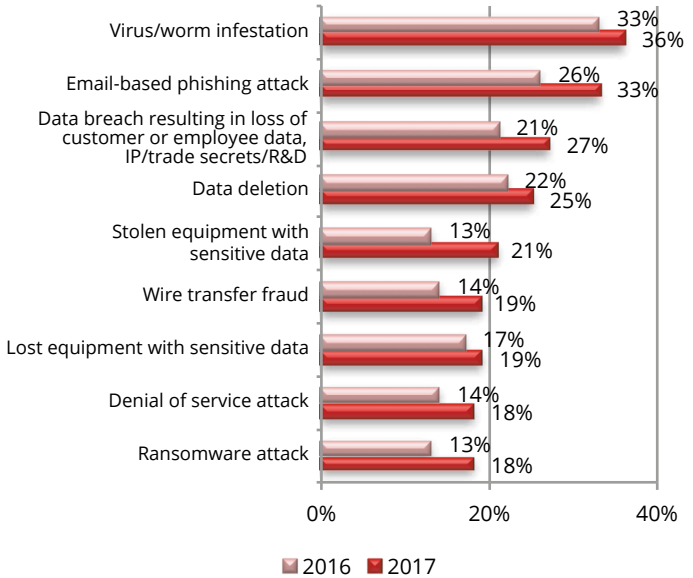
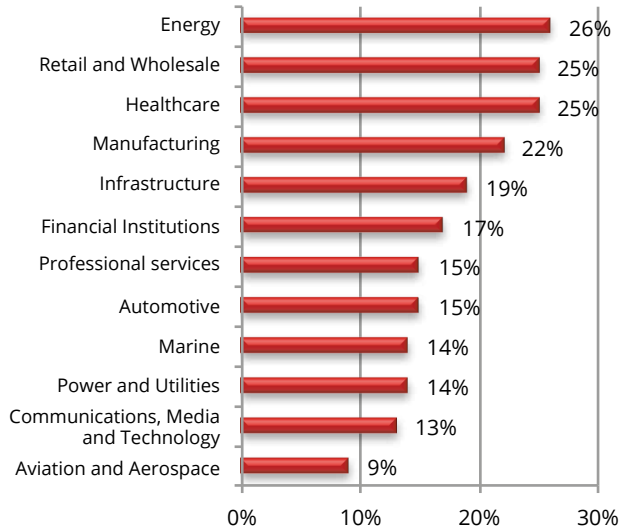


Fig. 3.2 Industries impacted by cyber attacks (% of companies, 2017)

Source: Marsh & McLennan Companies, MMC CYBER HANDBOOK 2018. Perspectives on the next wave of cyber, 2018



networks, telecommunication systems, financial networks and even nuclear facilities, and some industry sectors are bigger targets for cyber attack than others.

A global survey, conducted by Marsh & McLennan Companies (2018) on approximately 1,000 companies operating in all economic sectors, drew up a ranking of the sectors most commonly impacted by cyber attacks worldwide. 26% of respondents from the energy sector stated that their company had been a victim of cyber attacks in the past 12 months, followed by healthcare (25%) and retail and wholesale (25%). Even the manufacturing sector, with 22% of companies affected, is among the preferred targets for cyber criminals (Fig. 3.2).

Attackers frequently use very simple tools and tactics, such as email, making a big impact and damaging companies. Actually, email is not just a communication tool but it is also one of the prime sources of threat for users and organizations. This threat can range from unwanted emails in the form of spam to more dangerous types, such as the propagation of ransomware or targeted spear-phishing campaigns[3]. According to the Internet Security Threat Report published by Symantec, some industry sectors receive more spam than others even if the difference between the most targeted and least targeted sectors was low in 2016.

3 Symantec, *Internet Security Threat Report*, 2017

Fig. 3.3 Percentage of emails as spam, by sector (2016)

Source: Symantec, Internet Security Threat Report, 2017

The spam rate varied from 51.6% for public administrations to 59.5% for the construction sector (Fig. 3.3).

A growing proportion of spam contains malware. In 2016, agriculture, forestries and fishing, together with the wholesale trade, were the sectors most affected by email containing malware. In these sectors, the percentage of email classified as malware was about 1% of total emails. With the exception of retailing, which saw a drop in its email malware rate, every industry saw an increase in malware in 2016 (Fig. 3.4).

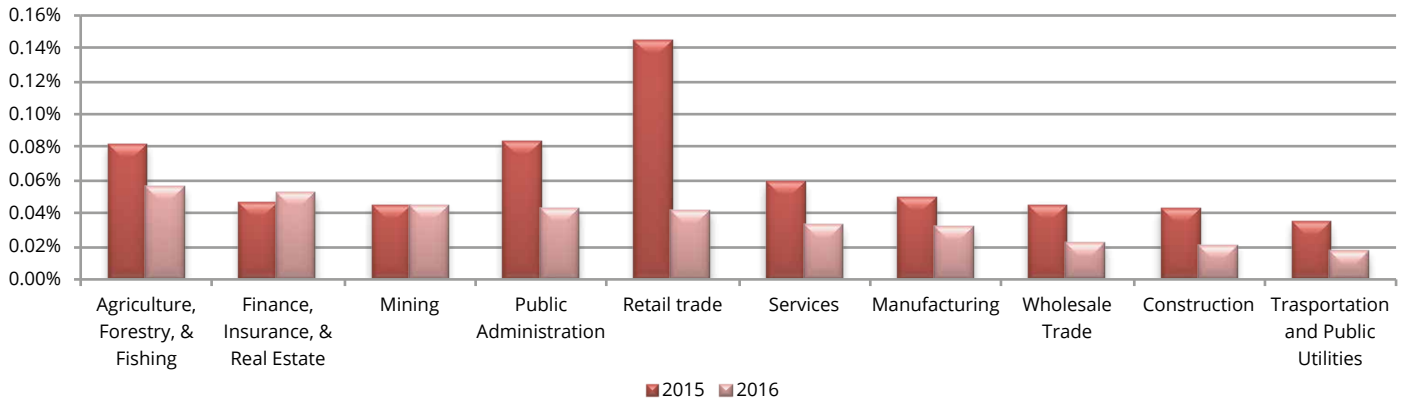
As regards to phishing, the trend is declining and the phishing rate dropped again in 2016 in all sectors (except for finance). However, agriculture was the sector most affected by phishing in 2016, with 0.06% of emails classified as phishing attempts followed by finance and the insurance sector. Instead, in 2015, retailing was the sector most exposed to this type of cyber attack (Fig. 3.5).

Fig. 3.4 Email containing malware, by sector

Source: I-Com elaboration on Symantec data

Fig. 3.5 Email containing phishing, by sector

Source: I-Com elaboration on Symantec data



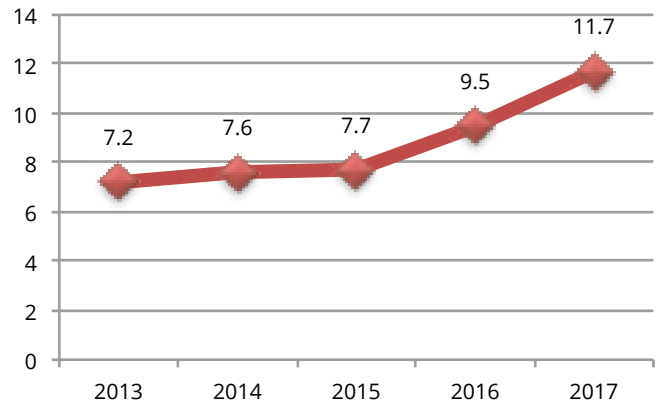
3.2. THE FINANCIAL COSTS OF CYBER CRIME

Cyber attacks are having a significant and growing financial impact on businesses worldwide. According to the Cost of Cyber Crime Study[4], published by Accenture and the Ponemon Institute (2017), the global average cost of cyber crime, which includes the total of costs incurred to detect, recover, investigate and manage the response to cyber attacks, climbed to $11.7 million in 2017, with an increase of 23% from $9.5 million reported in 2016, and 62% in the last five years (Fig. 3.6).

Comparing the different countries, companies in the United States incurred the highest total average cost at $21 million, instead Australian companies reported the lowest total average cost at $5.41 million. Among the countries analyzed, Germany experienced the most significant percentage increase (42%) with an average cost

Fig. 3.6 The global average cost of cyber crime (million $)

Source: Accenture and Ponemon Institute (2017)



4 The Cost of Cyber Crime Study surveyed 2,182 security and IT professionals in 254 large organizations (from 1,050 to over 259,000 workstations) in 7 countries – USA, United Kingdom, Germany, France, Italy, Australia and Japan.

Fig. 3.7 Average annual cost of cyber crime, by country

Source: Accenture and Ponemon Institute (2017)

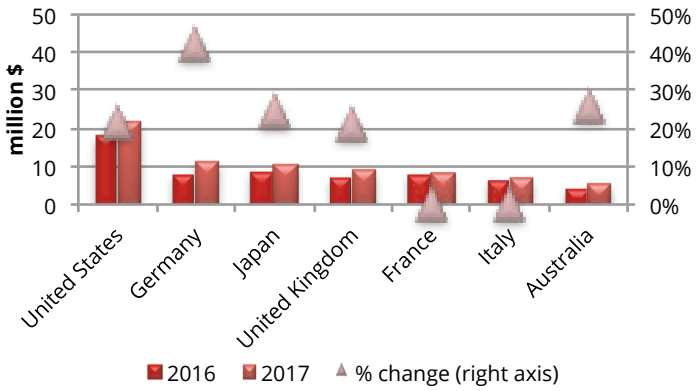
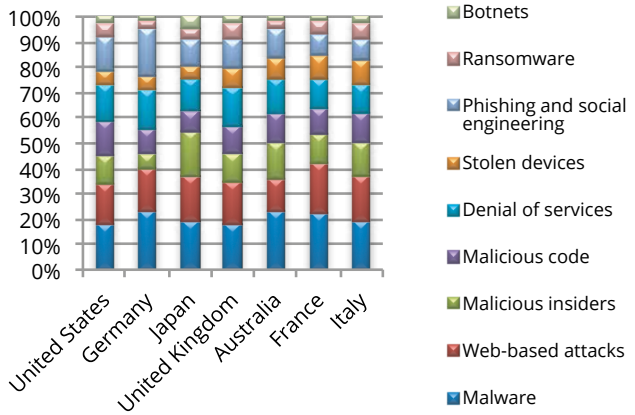


Fig. 3.8 The most expensive cyber attacks, by country

Source: Accenture and Ponemon Institute (2017)

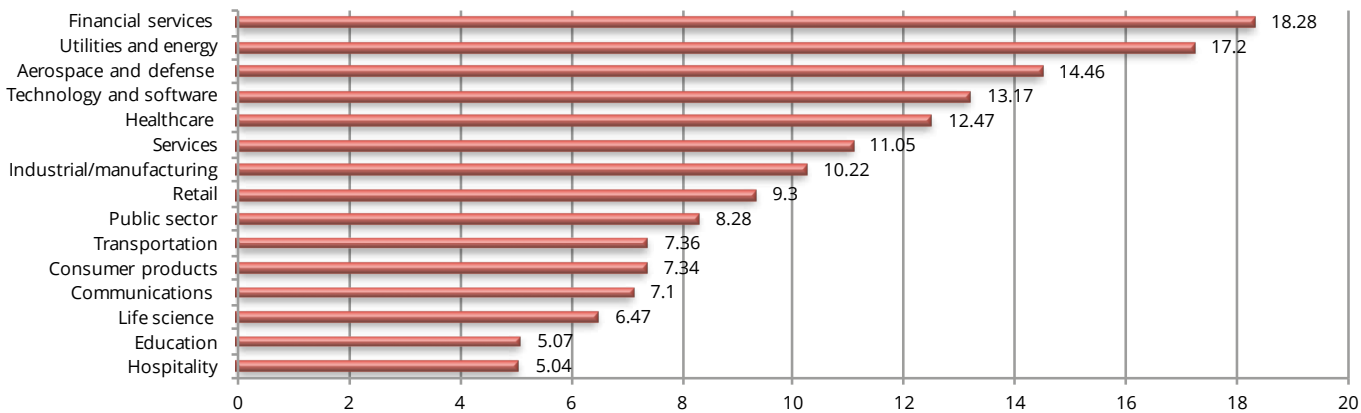


that has risen from 7.84 to 11.15 million dollars (Fig. 3.7). Malware was the most expensive cyber attack in all countries, followed by web-based attacks. In Germany and France, these categories exceeded 40% of the total average cost of cyber crime (Fig. 3.8).

Relative to the cost of cyber crime in the different

Fig. 3.9 Average annual cost of cyber crime, by sector (million $, 2017)

Source: Accenture and Ponemon Institute (2017)

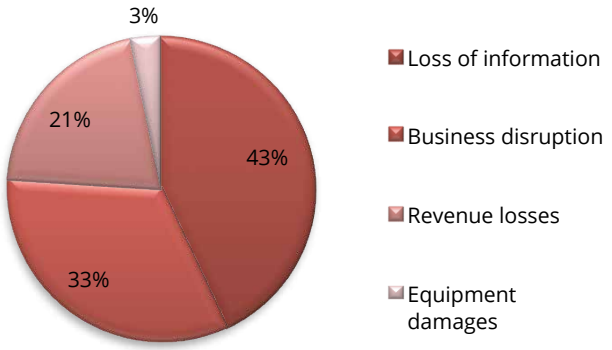


industrial sectors, companies selling financial services bore the highest cost of $18.28 million, followed by utility and energy companies with $17.2 million. Instead, companies in life sciences, education and hospitality incurred on an average much lower costs (Fig. 3.9).

The main and most costly impacts on organizations that suffered a cyber attack are business disruption, loss of information, loss of revenue and damage to equipment. For 43% of the interviewed organizations, the most damaging consequence involved loss of information. Instead, business disruption was mentioned by 33% of organizations – this involves a reduction in employee productivity and an increase in business process failures. Finally, revenue losses and equipment damages were reported by 21% and 3% of organizations, respectively (Fig. 3.10).

Fig. 3.10 The main consequences of cyber attacks (2017)

Source: Accenture and Ponemon Institute (2017)



3.3. ICT SECURITY POLICIES IN ENTERPRISES

To reduce cyber risks, companies must to adopt cyber risk mitigation measures and ICT security policies. The consequences of cyber attacks, such as business disruption, financial losses and reputation damage, make it imperative for companies to commit to establishing and supporting sustainable processes that will provide them with effective protection, now and into the future. At a minimum, a cybersecurity program should include at least the following three elements:

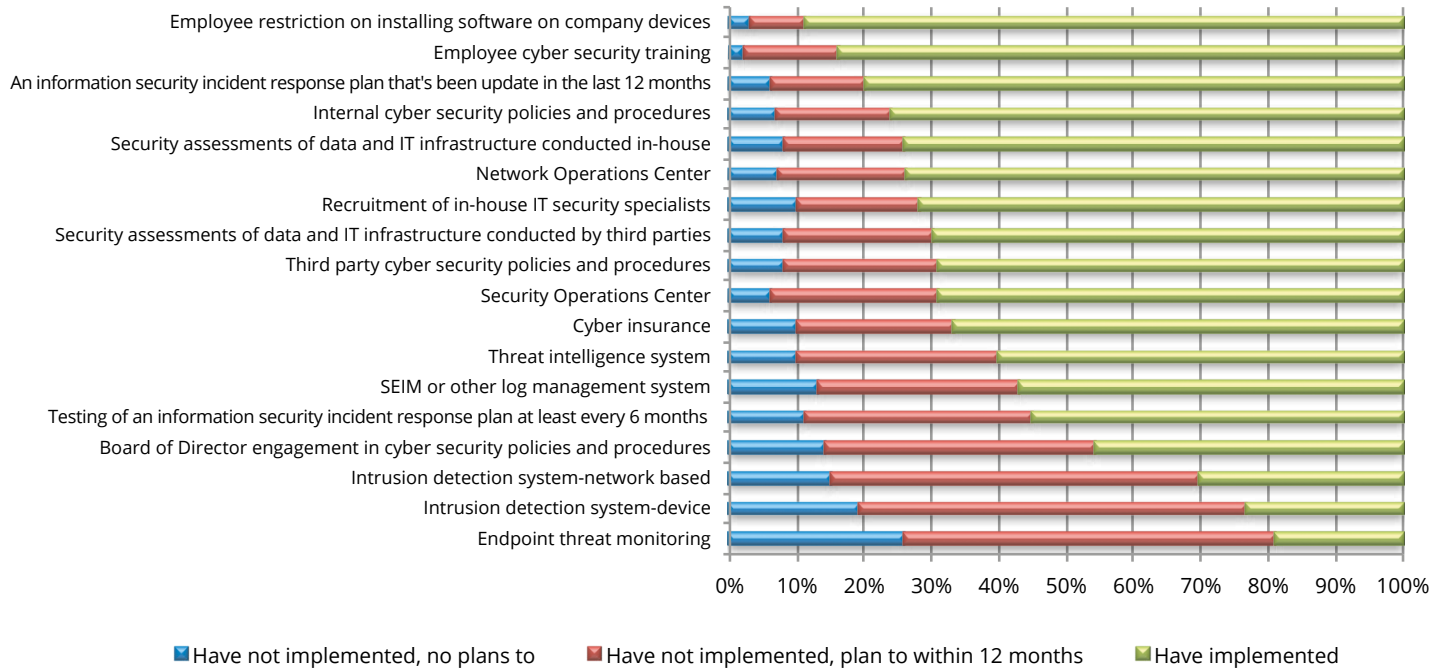
1) training employees to recognize phishing attempts and malicious email;
2) restricting access to key data and information;
3) preparing an incident response plan and identifying key vendors before a cyber event.

In particular, companies should implement training for employees to recognize phishing emails and to follow the company's protocols for handling a suspected phishing email and malicious email.

Moreover, companies should have procedures in place that restrict the number of people who can access key information. They should have identified and classified key data and assets, restricted access to the most important material so that only employees with a specific need can be guaranteed access and created tiers for other data and assets and appropriately restrict access and control rights. Striking a balance between efficient workflow and secure access can be difficult but establishing a coordinated procedure can reduce risk. Finally, in each company, a written incident response

Fig. 3.11 Adoption of cyber risk-mitigation measures by companies (% IT directors interviewed)

Source: Kroll, Global Fraud & Risk Report 2018



plan that identifies key vendors (computer forensics, crisis managers, and legal counsel) should be set up[5].

According to the global survey conducted by Kroll (2018)[6] (already mentioned in paragraph 3.1), the most implemented actions are employee restrictions on installing software (89%) and employee cybersecurity training (83%). Incident response plans (IRPs) also top the list, with 80% of respondents indicating their company already has an IRP in place.

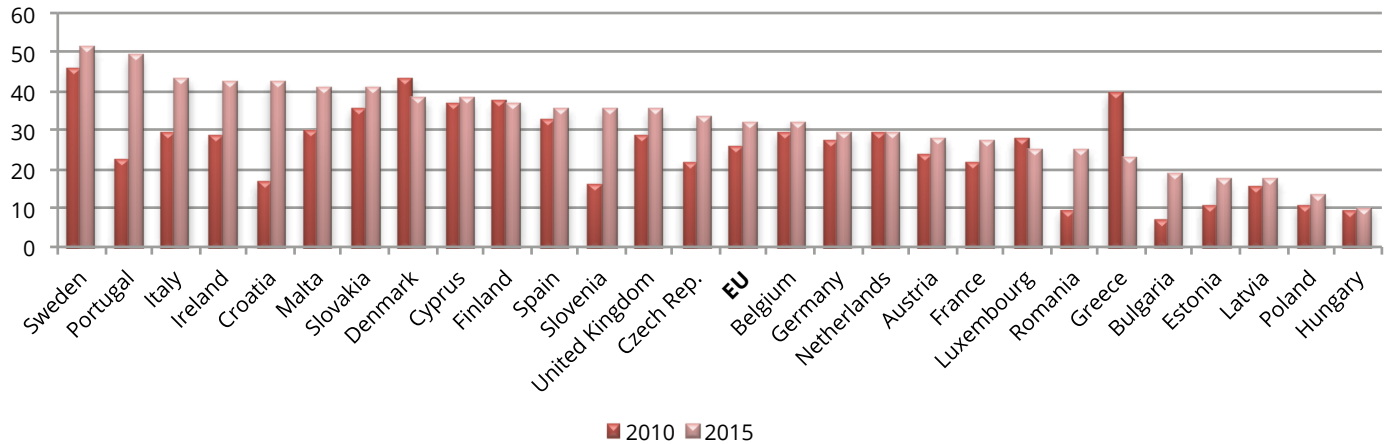
Instead, the top three actions the IT directors expect their company to implement in the next 12 months are device-based intrusion detection systems (57%), endpoint threat monitoring (55%) and network-based intrusion detection systems (54%). While only 46% of respondents currently involve the board of directors in cybersecurity policies and procedures, 40% of those interviewed who did not already have a plan, foresee doing so in the next 12 months (Fig. 3.11).

5 Katherine Henry, Brendan Hogan, *Understanding cyber insurance risks of target companies,* January 2018, downloadable at https://www.themiddlemarket.com/opinion/understanding-risk-management-and-cyber-insurance-risks-of-target-companies

6 Kroll, *Global Fraud & Risk Report*, 2018

Fig. 3.12 Share of enterprises with a ICT security policy (%)

Source: Eurostat



Looking at IT security policies in European enterprises, we can underline that, in 2015, almost one out of three enterprises in the EU-28 had ICT security policies in place. Sweden, Portugal and Italy were the countries with the greatest awareness of the importance of having a security policy (51%, 49%, 43% of companies, respectively). With the spread of the phenomenon of IT risks, the level of alertness among European countries actually increased over the period 2010-2015, with very few exceptions (Denmark and Greece) (Fig. 3.12).

The issue of cybersecurity is particularly felt in large companies and more than 70% of European large companies had an ICT security policy in 2015, compared with less than 1 in 3 SMEs. A similar situation is observed in all Member States (Fig. 3.13).

The destruction or corruption of data due to an attack or some other unexpected incident is the risk mostly addressed by enterprise ICT security policies in Europe[7]. In 2015, 28% of European enterprises defined a security policy to address this risk.

Among the EU countries (Fig. 3.14), Italy had the highest percentage of enterprises with a formally defined ICT security policy addressing the risks of data destruction or corruption (37%) and disclosure of confidential data (32%).

The risk that less worried EU companies in 2015 was the unavailability of ICT services due to an attack from outside (e.g. Denial of Service attack). Only 22% of European enterprises had a formally defined ICT security policy against this cyber threat (Fig. 3.14).

7 Eurostat, *ICT security in enterprises*

Fig. 3.13 Share of enterprises with a ICT security policy, by size class (%, 2015)

Source: Eurostat

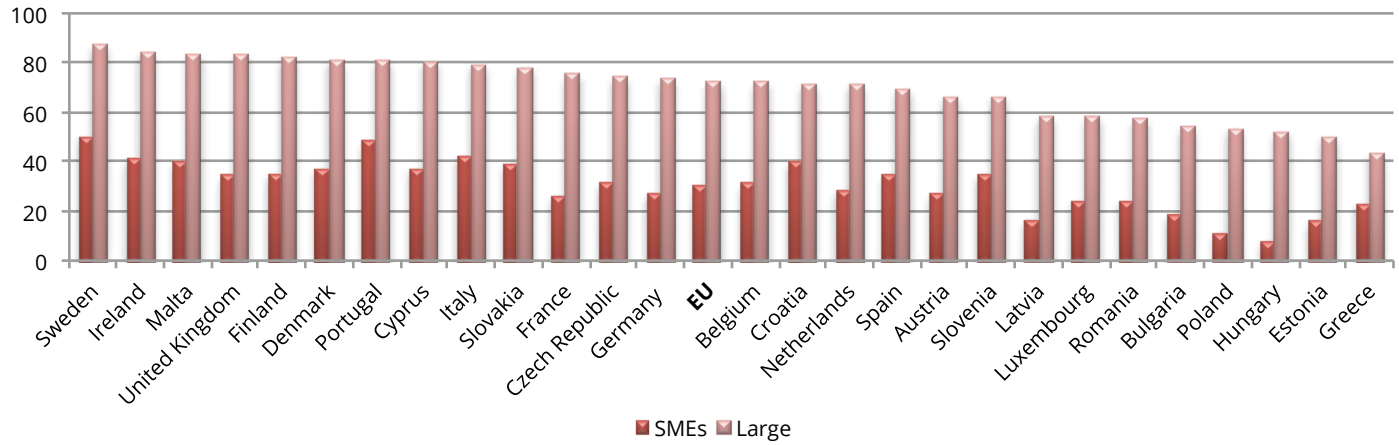


Fig. 3.14 Share of enterprises with a ICT security policy, by type of risk (%, 2015)

Source: Eurostat

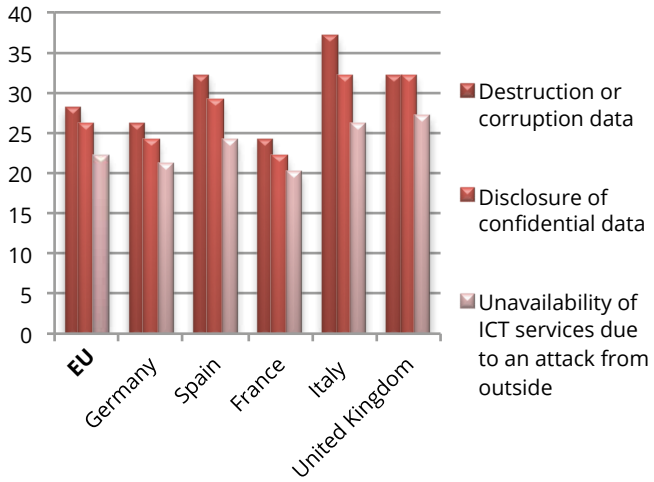


Fig. 3.15 Share of European enterprises with a ICT security policy, by industry (%, 2015)

Source: Eurostat

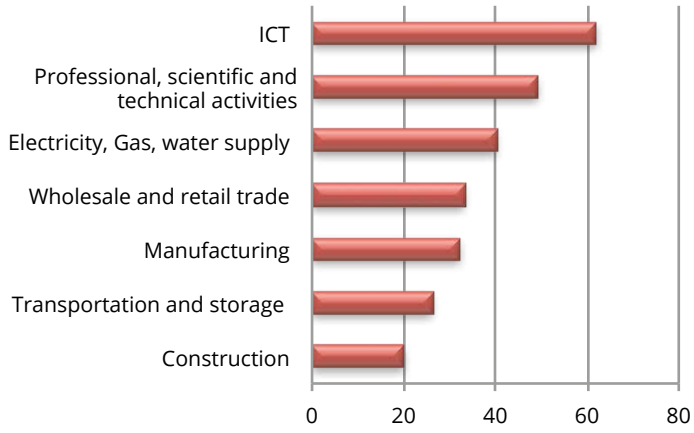
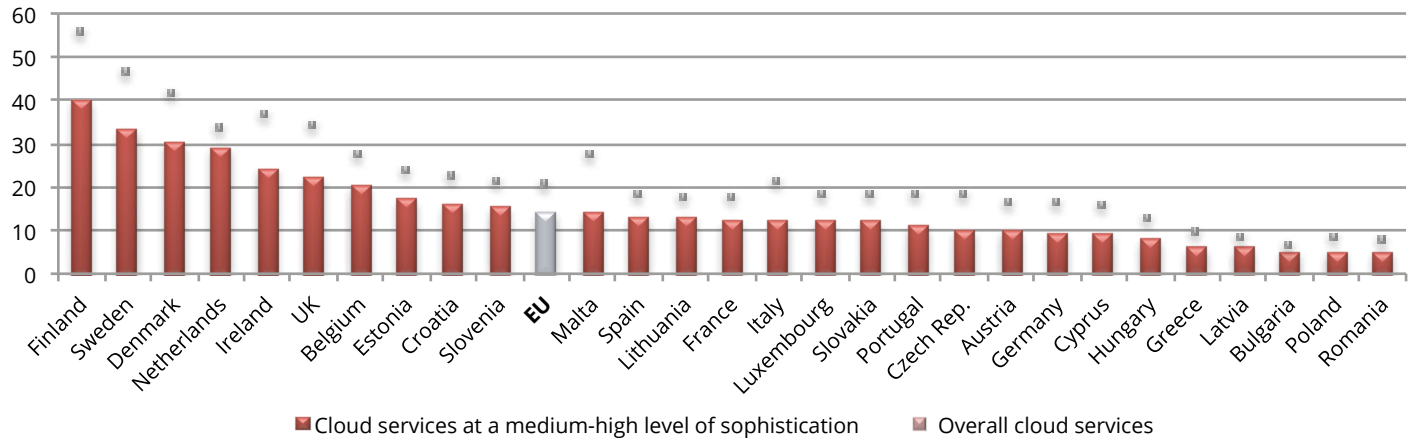


Fig. 3.16 Adoption of cloud services among EU enterprises, by country (%, 2016)

Source: I-Com elaboration on data Eurostat (2016)



Finally, comparing different economic sectors, we can notice that ICT, professional, scientific and technical activities and electricity, gas and water supply were those most prepared to counter cyber attacks with 62%, 49% and 40% of companies, respectively, having defined a ICT security policy (Fig. 3.15).

3.4. THE USE OF CLOUD SERVICES AND CYBERSECURITY IN ENTERPRISES

3.4.1. The use of cloud services: state of the art and future prospects

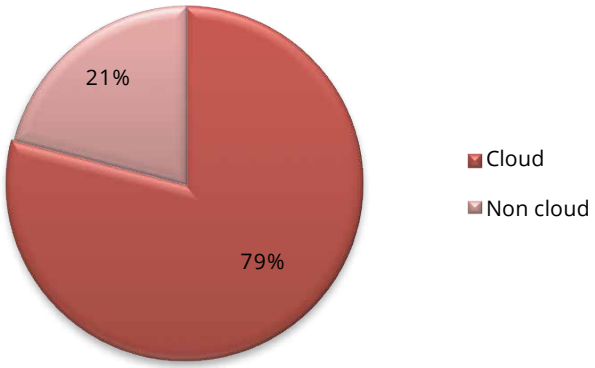
Cloud computing has entered the mainstream of information technology, providing scalability in delivery of enterprise applications and Software as a Service (SaaS). Companies are now migrating their information operations to the cloud. Many cloud providers can allow for data to be either transferred via a traditional Internet connection or via a dedicated direct link.

If we focus on European countries, we can see that just one in five enterprises already use cloud services, with a lower share of those making use of cloud services at a medium-high level of sophistication[8] (14%) and with Northern European countries at the forefront (Fig. 3.16). However, globally, this trend is definitely increasing. From a survey involving 1,002 technical professionals conducted by RightScale, it results that companies interviewed now run 79% of workloads in cloud (Fig. 3.17).

8 According to Eurostat classification, this category includes: hosting of the enterprise's database, accounting software applications, CRM software, computing power.

Fig. 3.17 Workloads

Source: I-Com elaboration on data RightScale 2017 State of the Cloud Report



Cloud computing aims at increasing efficiency in everyday tasks and provides a pathway for massive amounts of data generated by IoT to travel.

The four leading cloud benefits for organizations lie in a faster access to infrastructures (62% of interviewees), greater scalability (61%), higher availability (56%) and faster time-to-market (51%), with the largest increase relative to the previous year being in scalability (58% to 61%) and availability (52% to 56%), while there were decreases in IT staff efficiency (38% to 34%) and cost savings (37% to 35%) (Fig. 3.18).

However, despite the undeniable advantages, the cloud also involves challenges. The greatest one organizations face in implementing cloud platforms and technologies

Fig. 3.18 Cloud benefits

Source: RightScale 2017 State of the Cloud Report

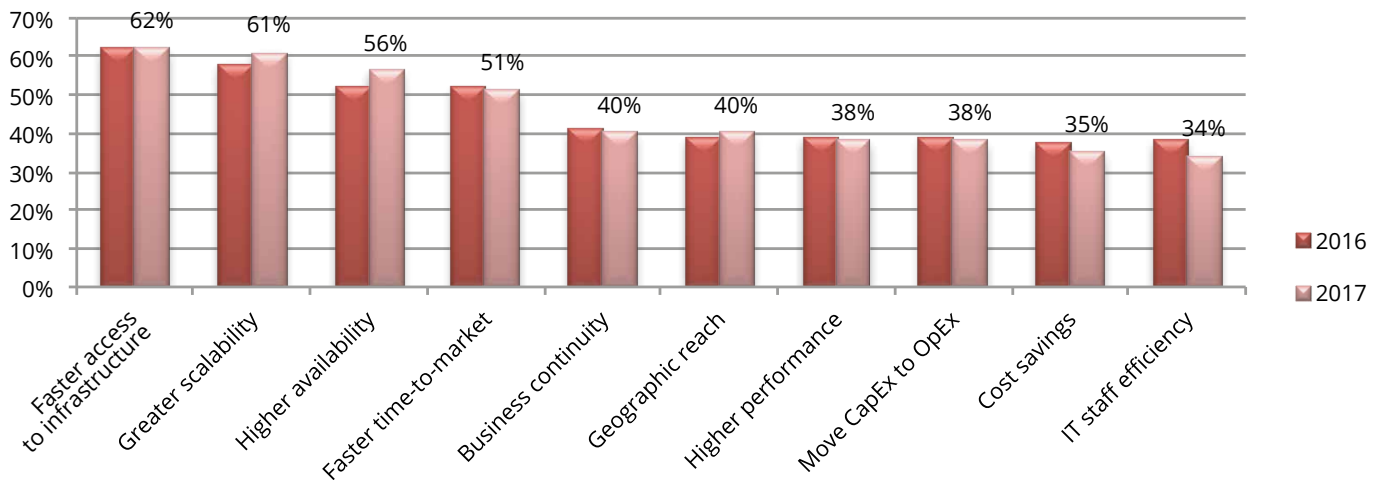
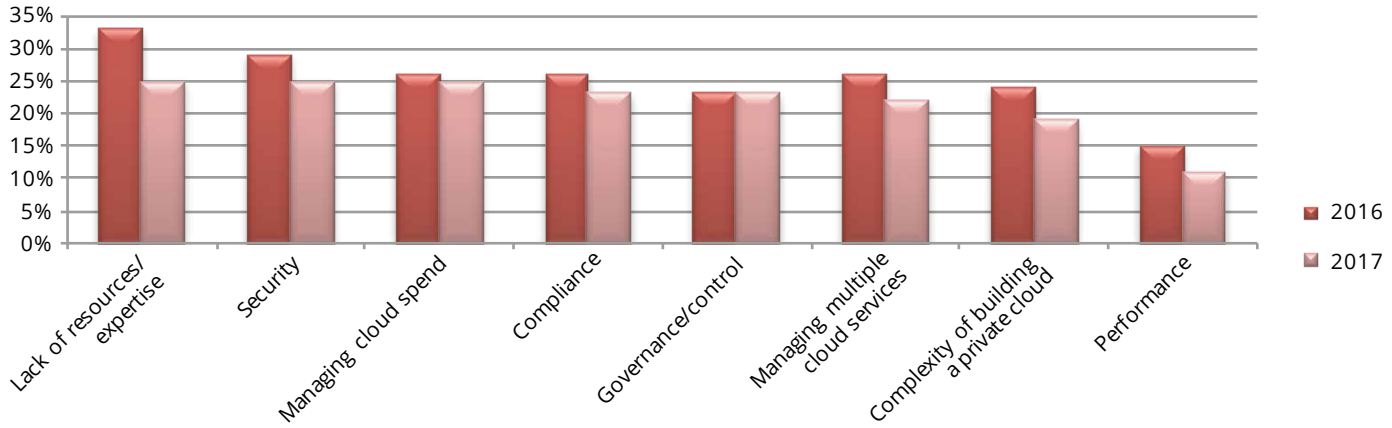


Fig. 3.19 Cloud challenges

Source: RightScale 2017 State of the Cloud Report



include a lack of resources and expertise, security and managing cloud spending (25% of respondents) (Fig. 3.19). Concerns regarding these three aspects, however, dropped in 2017 from 33%, 29% and 26%, respectively, in 2016. Compliance and governance and control follow, representing a limit to cloud adoption for about 23% of the interviewees.

According to the results of a survey[9], the biggest cloud security concerns include unauthorized access (63%) through misuse of employee credentials and improper access controls, hijacking of accounts (61%), and malicious insiders (43%) (Fig. 3.20). Malware, denial of service attacks, and other direct attacks against the cloud provider rank lower on the list of concerns.

9 LinkedIn Group Partner Information Security, *Cloud Security Spotlight Report*, 2015

Security in a cloud environment is, however, quite controversial (this will be further analyzed in 3.4.3.).

3.4.2. The needed transition to the public cloud

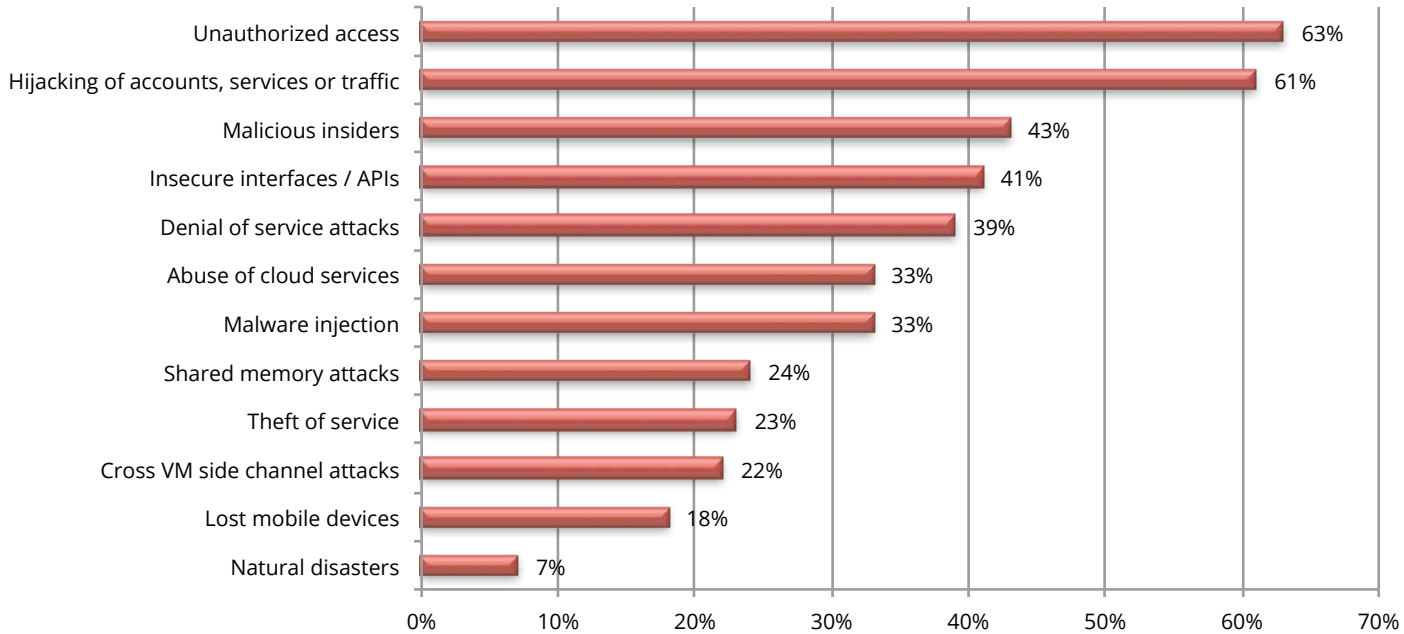
Cloud deployments are typically described in 3 different models: Public, Private or Hybrid.

Private Cloud Service is a secure cloud that only the specified organization can access. This model is usually the first choice for those organizations, including enterprises, that need to store and process private data or carry out sensitive tasks.

Public Cloud Service is like a Private cloud, although in this case resources used to process and store data can be shared with other organizations, and data transferred over a public network such as the Internet. Third party providers will deliver cloud services over the Internet

Fig. 3.20 Security threats in public cloud (2015)

Source: Cloud Security Spotlight Report (2015)



and are normally charged by the CPU cycles, storage, or bandwidth they require. The public cloud offers more technical flexibility and simpler scaling for many workloads and implementation scenarios. In some cases, using the public cloud also reduces IT operating costs.

Hybrid Cloud is a cloud computing environment which uses a mix of private cloud and third party public cloud services. With the hybrid cloud model, IT decision makers have more control over both the private and public components than using a pre-packaged public cloud platform.

While adoption of the public cloud has been limited to date, future prospects seem to be markedly different and, today, many companies are moving towards public cloud solutions. One of the main benefits that comes with using public cloud services is the ease of scalability, implying a high degree of cost-effectiveness. In addition, the public cloud can benefit from a greater reliability. Since the public cloud involves a vast network of servers, even if one data center was to fail entirely, the network would simply redistribute the load among the remaining centers making it highly unlikely that the public cloud would ever fail.

According to the results from a recent study[10], although just 40% of the observed companies have more than 10% of their workloads on public cloud platforms, about 78% are "cloud aspirants" – i.e. they plan to have more than 10% of their workloads in public cloud platforms in three years, or plan to double their cloud penetration –, whereas the remaining 22% are quite skeptical.

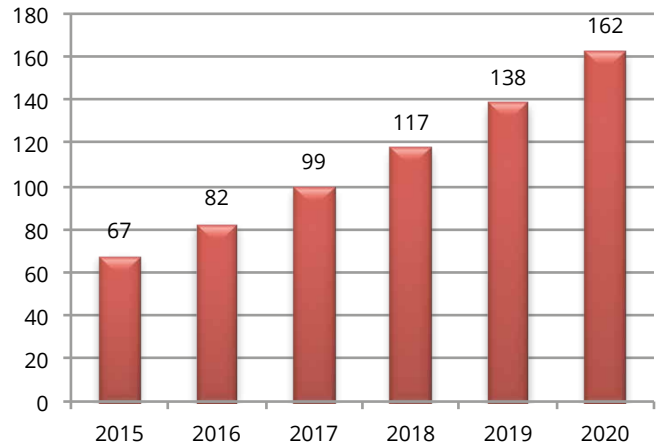
In addition, worldwide spending on the public cloud is expected to grow significantly over the next years, at a 19.3% compound annual growth rate (CAGR), moving from $67 billion in 2015 to $162 billion by 2020 (Fig. 3.21).

According to the data released by Gartner, the worldwide public cloud services market revenue was projected to grow by 18.5 percent in 2017, reaching $260.2 billion, up from $219.6 billion in 2016, and is expected to reach $411.5 billion by 2020, registering a further 12.2% average annual growth rate.

Final data for 2016 shows that software as a service[11] (SaaS) revenue was the second largest share of total revenue in 2016, reaching $48.2 billion. SaaS was also projected to grow by 22% in 2017. The acceleration in SaaS adoption can be explained by providers delivering nearly all application functional extensions and add-ons as a service. This appeals to users

Fig. 3.21 Worldwide spending on public cloud computing (bln $)

Source: IDC (2016)



because SaaS solutions are engineered to be more purpose-built and deliver better business outcomes than traditional software.

Cloud Advertising[12] represents the lion's share of the overall market (over 40%) (Fig. 3.22), whereas the Cloud System Infrastructure Services[13] (IaaS) segment is the fast-growing (+37% in 2017, compared

10 McKinsey Global, *Cloud Cybersecurity Research*, 2017

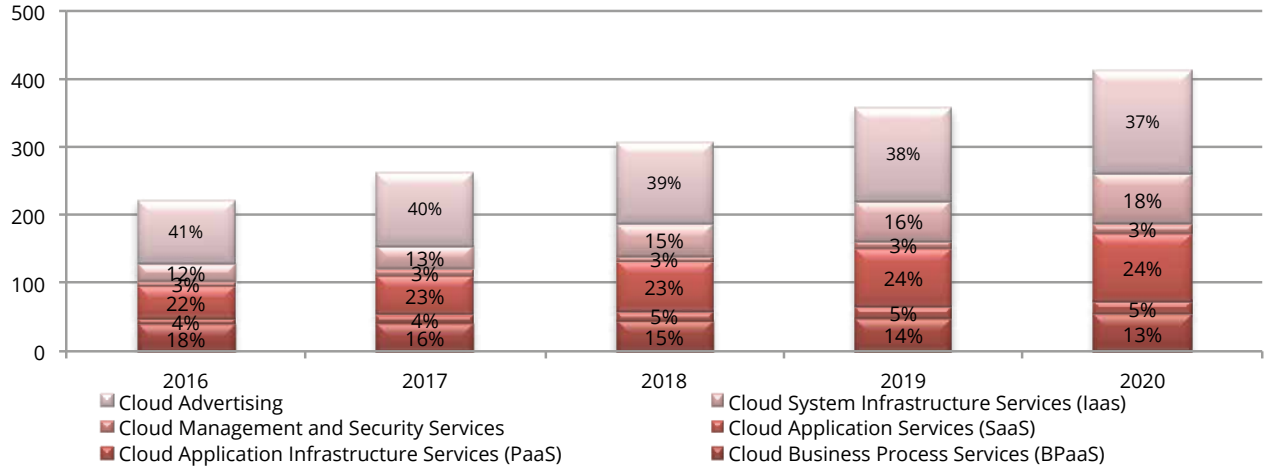
11 SaaS is defined as software that is owned, delivered and managed remotely by one or more providers. The provider delivers software based on one set of common codes and data definitions that is consumed in a one-to-many model by all contracted customers at any time on a pay-for-use basis or as a subscription based on use metrics.

12 Cloud Advertising is defined as cloud-based services that support the selection, transaction and delivery of advertising and ad-related data in which content and price are determined at the time of end-user access, usually by an auction mechanism that matches bidders with advertising impressions as they become available. This applies to search, display, mobile, social and video ad formats.

13 IaaS is defined as a standardized, highly automated offering, where compute resources, complemented by storage and networking capabilities are owned and hosted by a service provider and offered to customers on-demand. Customers are able to self-provide this infrastructure, using a Web-based graphical user interface that serves as an IT operations management console for the overall environment. API access to the infrastructure may also be offered as an option.

Fig. 3.22 Predictions on public cloud service revenues (bln $)

Source: I-Com elaboration on Gartner data

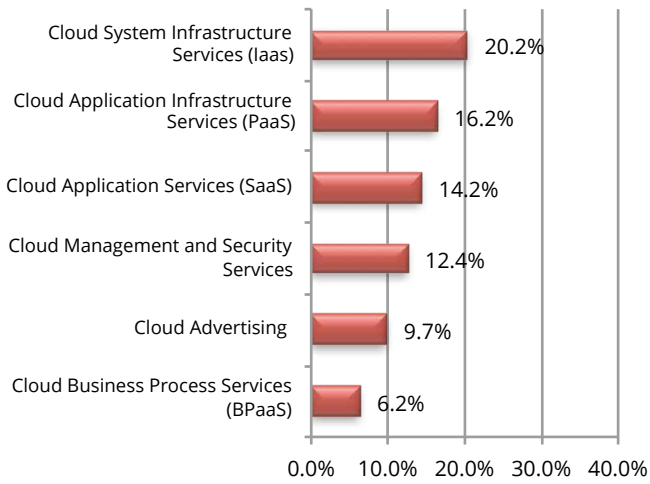


to 2016, with an average 20.2% annual growth over the next three years) (Fig. 3.23).

Strategic adoption of a platform as a service[14] (PaaS) offering is also outperforming previous expectations, as enterprise-scale organizations are increasingly confident that PaaS will be their primary form of application development platform in the future. This accounts for the remainder of the increase in the Gartner public cloud services revenue forecast. It is the second fastest growing segment, expected to increase on an average of 16.2% over next years and to reach $21 billion.

Fig. 3.23 Expected growth in public cloud service revenues (CAGR 2017-2020)

Source: I-Com elaboration on Gartner data



14 PaaS, usually depicted in all-cloud diagrams between the SaaS layer above it and the IaaS layer below, is defined as a broad collection of application infrastructure (middleware) services (including application platform, integration, business process management and database services).

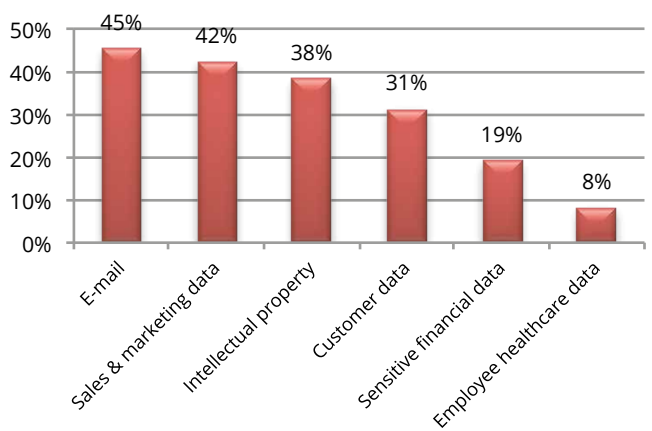
3.4.3. The cloud security challenge: a cloud-centric cybersecurity model to make the transition secure

As enterprises scale up their use of the public cloud, they must rethink how they can protect data and applications. However, using the public cloud disrupts traditional cybersecurity models that many companies have built up over the years. As a result, as companies make use of the public cloud, they need to dramatically evolve their cybersecurity practices in order to consume public cloud services in a way that enables them both to protect critical data and to fully exploit the speed and agility that these services provide.

Companies mainly worry that they will have less control over sensitive corporate data when it is stored in remote interlinked computers. Indeed, most sensitive data, such as financial or employee healthcare data, tends to be stored less in the cloud (Fig. 3.24).

Fig. 3.24 Information stored in the cloud (2015)

Source: Cloud Security Spotlight Report (2015)



Cloud models can be mainly segmented into Software as a Service (SaaS), Platform as a Service (PaaS) and Integration as a Service (IaaS), with different consequences in terms of security.

The SaaS model is focused on managing access to applications. In this case, the security officer needs to focus on establishing controls regarding user access to applications.

The PaaS model is focused on protecting data. This is especially important in the case of storage as a service. The security operation needs to consider providing for the ability to load balance across providers to ensure fail over of services in the event of an outage. Another key consideration should be the ability to encrypt the data whilst stored on a third-party platform and to be aware of the regulatory issues that may apply to data availability in different places. The IaaS model is focused on managing virtual machines. The Chief Security Officer's (CSOs) priority is to overlay a governance framework to enable the organization to put controls in place regarding how virtual machines are created and spun down, thus avoiding uncontrolled access and potential costly wastage.

According to the results reported in the Cloud Security Spotlight Report[15], SaaS solutions are the most used solutions (60% of respondents), followed by IaaS (47%) and PaaS (33%). Nonetheless, although there

15 Cfr. footnote 2

are core security implications that are common across IaaS and PaaS, an important difference is the shared responsibility for security in the PaaS model. Where a customer of IaaS will be responsible for securing operating systems and specifying authorizations for users, when working with PaaS, more responsibility is shifted to the PaaS provider who will provide physical security and implement access controls. In addition, a PaaS offering provides continual security updates for individual components as they are issued.

Companies are increasingly building both new applications and analytics capabilities in the cloud and starting to migrate existing workloads and technology stacks onto public cloud platforms. However, despite the benefits of public cloud platforms, persistent concerns about cybersecurity for the public cloud have deterred companies from accelerating the migration of their workloads to the cloud. Security is often cited as one of the top barriers to cloud migration, along with the complexity of managing change and the difficulty of making a compelling business case for cloud adoption. Obviously, companies need a proactive, systematic approach to adapting their cybersecurity capabilities for the public cloud.

Above all, for an approach to public cloud cybersecurity to be effective and consistent, it requires developing a cloud-centric cybersecurity model. This implies, firstly, not using the controls it already has for on-premises systems, since these – even if reconfigured – will never provide visibility and protection across all workloads and cloud platforms. On the contrary, what needs to be done is to reassess the company's cybersecurity model, accounting for how the network perimeter is defined – so as to define the boundaries for the cloud-cybersecurity model – and whether application architectures need to be altered for the public cloud – that is, whether security controls need to be incorporated within the applications. Regarding the first issue, 3 models are emerging across companies[16]:

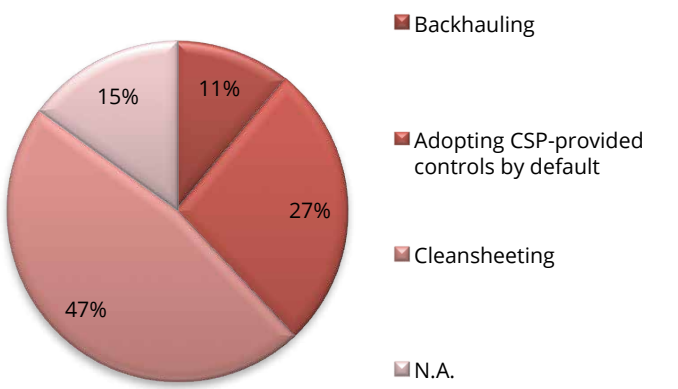
1. **Backhauling**, where all public cloud access is through private infrastructures with external gateways, which allow the company to continue using the on-premise security tools that they already know well;
2. **Adopting CSP (Cloud Solution Provider) controls by default**, maintaining separate private security controls and CSP controls for the public cloud only. This solution may be more cost-effective but makes it more complex to secure a multicloud environment;
3. **Cleansheeting**, that is, best-of-breed security controls for the public cloud and private cloud. This solution involves developing cloud-specific controls from solutions offered by various external providers and it represents the best perimeter-security solution. However, a lot of in-house cybersecurity expertise is needed to select vendors and integrate their solutions, which may slow the migration of workloads into the cloud.

Backhauling is now the most popular model for perimeter security among the cloud aspirants considered in the survey conducted by McKinsey. However, enterprises

16 McKinsey & Company, "Making a secure transition to the public cloud", January 2018

Fig. 3.25 Expected distribution of cloud security models by 2020

Source: I-Com elaboration on data McKinsey



are increasingly moving toward a virtual-perimeter model (cleansheeting), that is likely to become the most popular model by 2020 (Fig. 3.25).

The second choice to assure an appropriate cloud-centric cybersecurity model is to decide whether to rearchitect applications in the public cloud, by rewriting codes or altering application architectures (or both). Deciding to do this is one way to ensure stronger security within the organization with changes like tamper detection using hash, memory deallocation, and encrypting data flows between calls, and with other benefits like superior performance, lower operating costs (because app-level security protections reduce the need for a company to choose best-of-breed security solutions) as well as compatibility with all CSPs.

Developing a cloud-centric cybersecurity model is, however, just the first step towards a proper cybersecurity policy. Then, companies need to:

- redesign the full set of cybersecurity controls for the public cloud – that is, for each individual control, they need to determine who should provide it and how rigorous they need to be;
- clarify internal responsibilities for cybersecurity, compared to what providers will do – when enterprises migrate applications and data to the public cloud, they must depend on CSPs and third-party providers for some security controls but they should not depend on them to provide all necessary controls. Collaboration between companies and their CSPs appears to be especially important in four main areas: transparency in controls and procedures; regulatory compliance support; integrated operations monitoring and response; and multicloud IAM (Identity and Access Management) capabilities;
- apply developers to cybersecurity – that is, companies need to make highly automated security services available to developers via APIs (Application Programming Interfaces), just as they are doing for infrastructure services, in order to prevent the possible delay of the security team in signing off on a configuration from attenuating the value of the public cloud's agility.

In addition, a model of Security as a Service is recently emerging. It is an outsourcing model for security management. Typically, Security as a Service does not require on-premise hardware, avoiding substantial capital outlays. These security services often include

authentication, anti-virus, anti-malware/spyware, intrusion detection, penetration testing and security event management, among others.

The benefits of this model are at least five:

1. Constant virus definition updates that are not reliant on user compliance;
2. Greater security expertise than that typically available within an organization;
3. Faster user provisioning;
4. Outsourcing of administrative tasks, such as log management, to save time and money and allow an organization to devote more time to its core competencies;
5. A web interface that allows in-house administration of some tasks as well as a view of the security environment and on-going activities.

Two key factors for protecting cloud environments that appear to be common to the different models are security consistency with other IT infrastructure and continuous protection.

The real matter is that applications and data maintained in the cloud can be more secure than data held in on-premise corporate systems because moving to the right kind of advanced cloud system represents a more dynamic approach to risk. Cybersecurity is integrated with marketing, customer service and logistics, developing a single way of tracking the behavior of everyone who interacts with the company. In other words, with this type of system, the more attacks the cloud faces, the stronger it becomes.

As companies digitize more and more aspects of their internal operations and external contacts with the outside world, the standard approach to protecting on-site corporate networks from cyber-attacks involving the use of IT systems to detect and prevent unwanted efforts to gain entry is no longer truly effective. The problem calls for an entirely different type of solution. Here, the cloud may offer several benefits:

- almost unlimited **low-cost computational power**, which is often needed to identify the kinds of suspicious activity that indicate the movements of hackers and who they might be. Without the cloud platform and its analytical power, it would be almost impossible to detect such patterns, especially when monitoring huge volumes of data, highly complex and interconnected applications, and time intervals as long as months or years. Because cloud software is independent of particular hardware platforms, it is innately "virtual" — codes run on other codes, not on devices;
- **simplicity**, by reducing the number of points of vulnerability and making it easier to keep up with technological advances, since companies can now rely on their CSPs to build the cloud infrastructure, hardware, software, and services required;
- companies are able to **scale up** their systems as needed, to a degree not possible with on-premise computing;
- vast improvements in a company's ability to **counter cyber-threats** because of the way it responds to intrusion. By the time a cyber-attack is detected in a typical computer system on someone's premises, the security technologies have already failed. The standard

defense against such attacks is limited to remediation and repair and, since many on-premise IT technologies are not designed to work with one another, it's highly difficult to learn from this experience. In the cloud, by contrast, security technologies are merged together into an analytics platform, which is maintained across a wide variety of computer hardware systems. In real time, the system logs and analyzes all activities taking place on the computers. An advanced cloud service continually checks the integrity of the security controls in place and evaluates the critical entry points of the system and what alternatives might exist if they had to be shut down. The moment a new threat is identified, the operational data about it is injected into the analytics platform and analyzed against the entire body of the accumulated security technology information. At the same time, any threatened applications and their associated data are immediately respawned in a new software-defined network beyond the reach of the attackers and the vulnerability is immediately patched. Finally, the strength of the cloud-based system lies in its ability to combine authentication and analytics from multiple sources. As cyber attacks become an increasingly shared problem among companies and governments, it will be important to openly exchange information about the attackers' identities and the nature of the threats they pose. With a cloud-based system, this can be done without compromising anyone's secure data, and it can be set up in a way that benefits the entire knowledge base shared by cloud participants.

PART 4

CYBERSECURITY IN VERTICAL SECTORS: MANUFACTURING, ENERGY AND AUTOMOTIVE

4. CYBERSECURITY IN VERTICAL SECTORS: MANUFACTURING, ENERGY AND AUTOMOTIVE

4.1. CYBERSECURITY IN THE MANUFACTURING SECTOR

4.1.1. Trends in manufacturing and the intake of digital in EU industry

Consumer expectations and the advent of connected devices and platforms are driving the ongoing digitization of manufacturing. The sector continues to evolve in response to the challenge of ensuring the right products are delivered at the right price to the right person through a process of improved sophistication.

At the center of the industrial transformation there is the IoT because of the revolutionary ways this connected technology has streamlined and simplified various manufacturing processes.

Traditionally, robots have been used to perform tedious, repetitive tasks on the assembly line. Nowadays, however, robots are capable of mimicking more human traits such as dexterity and memory, which make them more useful in industries like manufacturing. They are also providing safer working environments for humans by switching places with them in dangerous or unsuitable situations. Finally, robots equipped with sensors – smart machines that "talk" to the control board, quickly identifying and fixing mechanical problems – also provide valuable feedback and data, thus allowing companies to make necessary adjustments more accurately.

Within the EU, Germany is the country with the largest sales of robots (Fig. 4.1), with over 20,000 units in 2016, 36% of

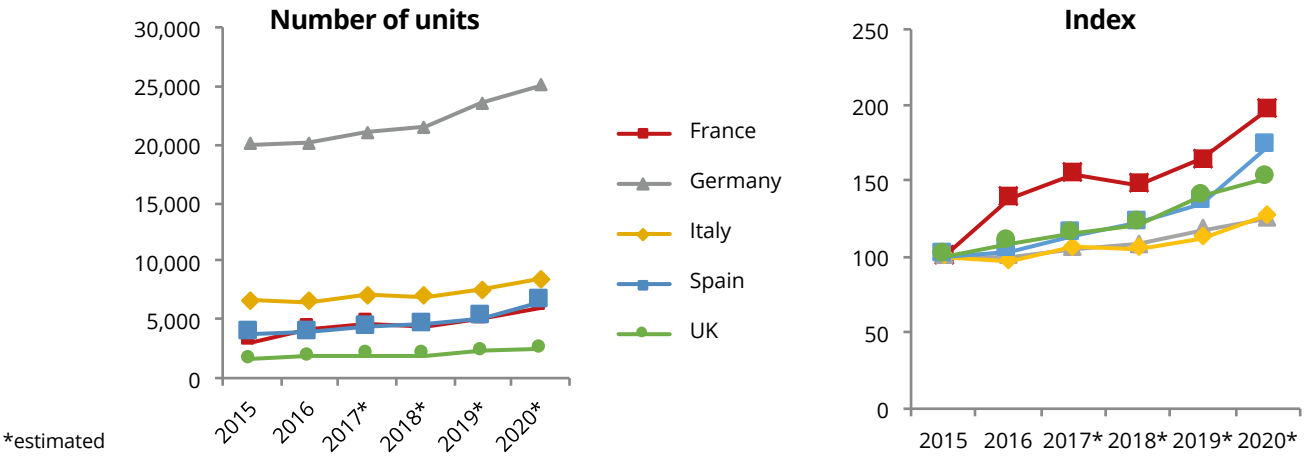
Fig. 4.1 European Robot Market, by country

Source: I-Com elaboration on data IFR (2017)

*estimated

Fig. 4.2 Estimated annual shipments of multipurpose industrial robots in Europe

Source: I-Com elaboration on data IFR (2017)



*estimated

the total European market. The second largest market[1] is Italy, with a share of 11% (more or less 6,500 units sold), that is expected to remain stable to 2020, differently from Germany whose share will decline. The Italian robot market is projected to reach 8,500 units by 2020.

France is the market that will grow the most, at a 42% compound annual growth rate, starting from 2015 until 2020, almost doubling its sales – about 6,000 units compared to 3,045 in 2015 (Fig. 4.2). The Italian market, as well as the German one, starting from higher values, have registered lower growth rates – on average an annual 31% and 25%, respectively – resulting in only a 28% and 25% increase in the five-year period. Nonetheless, by 2020 they are projected to remain the two largest markets in the European market, reaching approximately 82,600 units (from slightly more than 56,000 units in 2016), 2.7% of the global market.

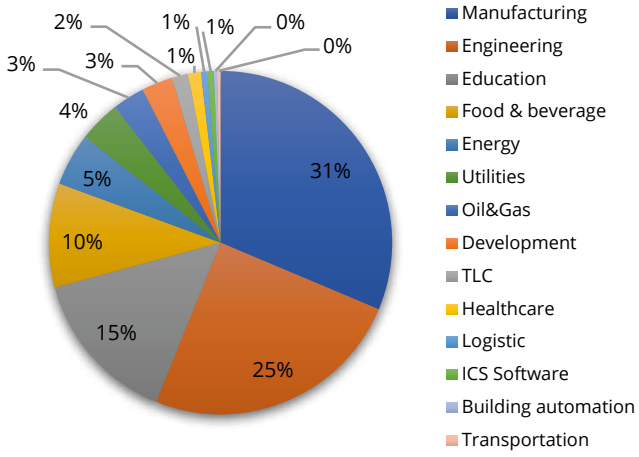
Robots and other automated technology are also integral in improving speed and efficiency, allowing manufacturing companies to "optimize production workflows, inventory, Work in Progress, and value chain decisions." By integrating their IT systems, teams across the platform in various geographical locations can access relevant data, facilitating a quicker, more collaborative and transparent communication.

In such a context, data plays a key role, in order to derive any form of value from sensors, IoT-enabled devices and other "things", also in manufacturing. Manufacturers acquire data regarding their assets but also regarding

1 And 7th at a global level, following China, Korea, United States, Japan, Germany and Taiwan.

Fig. 4.3 Percentage of attacked industrial control systems (ICS) users (June 2017)

Source: I-Com elaboration on Kasperby Lab data



customers and the hundreds of millions of connecting devices they dispose of. Information about things like supply, delivery, customer support used to be difficult to find or cumbersome to work with. In the digital era, that data is streamlined and collaboration-friendly, increasing accessibility for all stakeholders.

4.1.2. The main cyber threats in the manufacturing industry

As manufacturers innovate, integrating cutting-edge technologies into products, automating the shop floor, connecting supply chains, and increasingly investing in valuable intellectual property (IP), the industry is also likely to experience an acceleration in the velocity and sophistication of associated cyber threats as cyber risk and innovation are closely linked.

According to a report from Kaspersky Lab[2], in the first half of 2017 the manufacturing industry was the most susceptible sector to cyber threats – with the industrial control systems (ICS) computers of manufacturing companies accounting for almost one third of all attacks (Fig. 4.3).

According to the results of a study from Deloitte and the Manufacturers Alliance for Productivity and Innovation (MAPI)[3], nearly 40% of surveyed manufacturing companies were affected by cyber incidents last year. 38% of those impacted indicated cyber breaches resulted in damages in excess of $1 million, in addition to harder to quantify repercussions regarding brand and reputation damage which are time consuming and costly to repair.

Top threats, damaging about one third of the interviewed enterprises, include IP theft (34%) and phishing/pharming (32%) (Fig. 4.4). The former is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers; the latter being the fraudulent practice of directing Internet users to a bogus website that mimics the appearance of a legitimate one, in order to obtain personal information such as passwords, account numbers, etc.

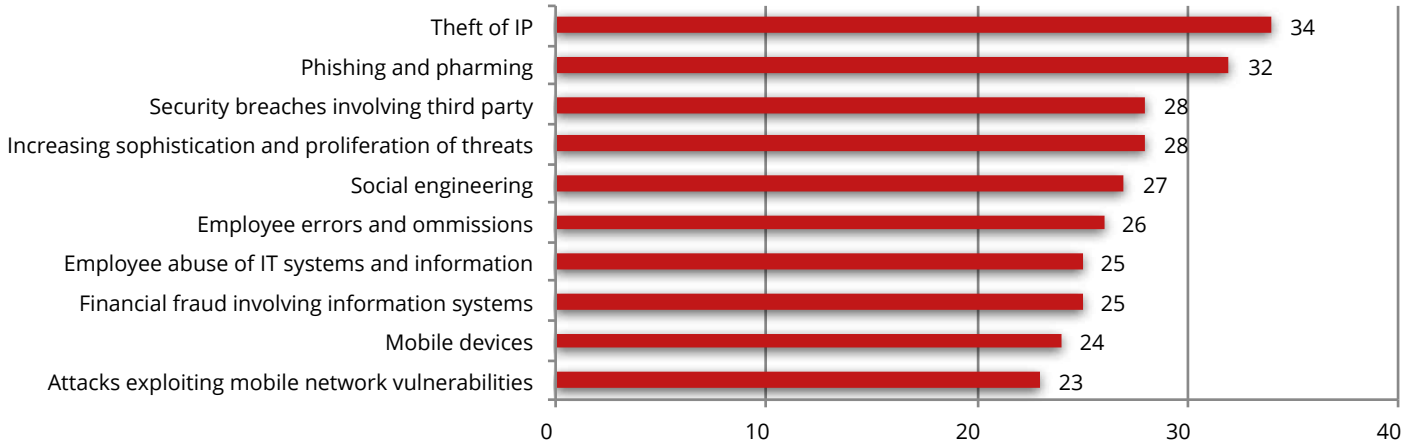
In addition, increasing dependence on technology-enabled connected products brings a new set of risks

2 Kaspersky Lab, *Threat Landscape for Industrial Automation Systems in H1 2017*, 2016

3 Deloitte and MAPI, *Cyber risk in advanced manufacturing*, 2016

Fig. 4.4 Top 10 cyber threats facing manufacturing (2016)

Source: Deloitte and MAPI, 2016



to manufacturers. Indeed, attacks involving mobile devices or mobile networks concern about one in four surveyed companies.

For cyber risk to be adequately addressed in the age of Industry 4.0, cybersecurity strategies should be secure, vigilant and resilient, as well as fully integrated into an organizational and information technology strategy from the start.

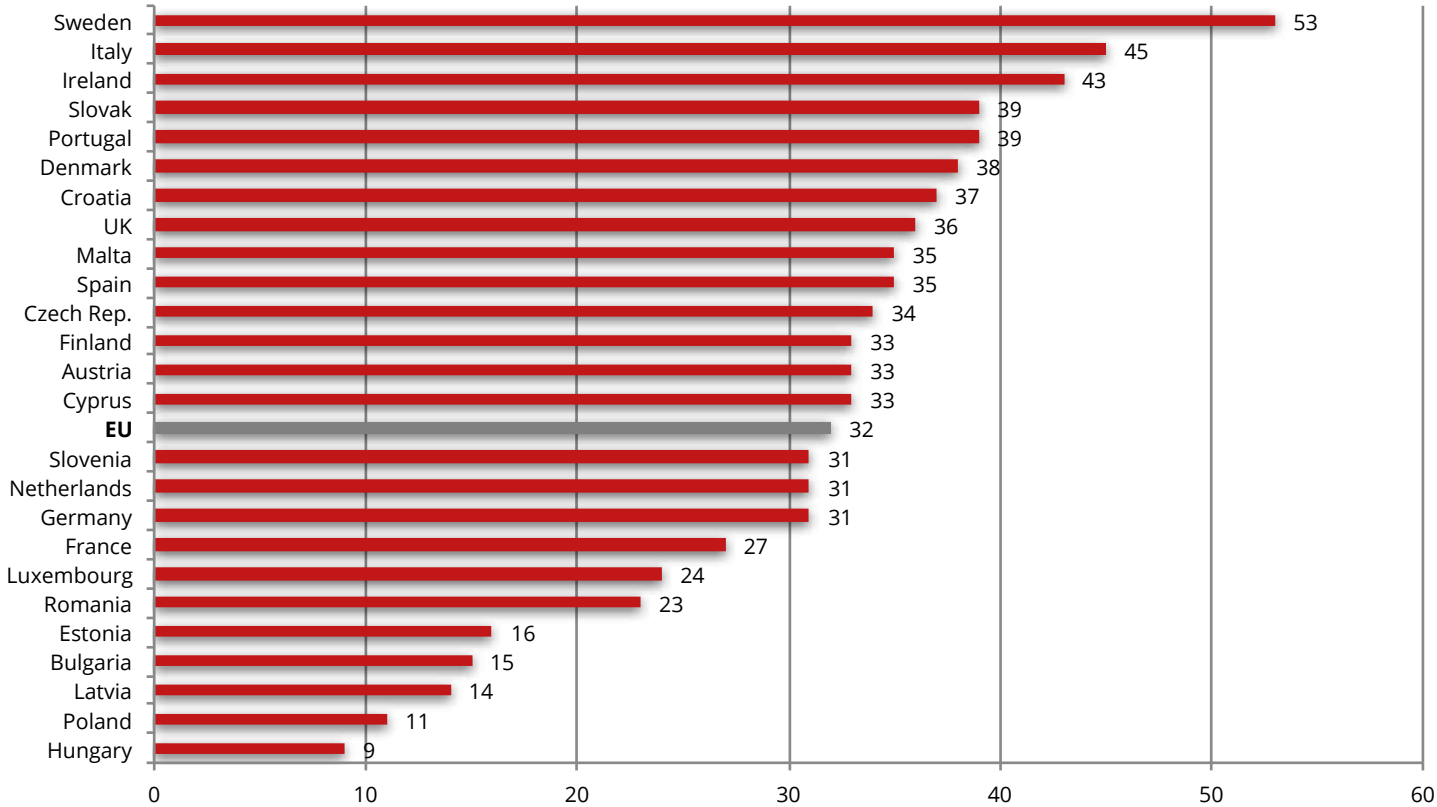
4.1.3. How companies are addressing cyber risks

The challenge of implementing a secure, vigilant, and resilient cyber risk strategy is different in the age of Industry 4.0. When supply chains, factories, customers and operations are connected, the risks posed by cyber threats become far reaching. One major problem is that many factories are today more than 20 years old, which raises concerns as to whether they are equipped with updated defenses. Because machinery is often phased in over time, unlike office systems, unknown vulnerabilities may have been dormant for years and are now just coming to life. As manufacturers add connected devices to these outdated machines, security professionals raise concerns that attackers may find the combination ripe for exploitation.

Vulnerable systems could lead to factory floor downtime, another key worry for automation professionals. Manufacturers want to avoid unplanned downtime at all costs, as well as product quality problems that could be caused by compromised machines not working properly. For manufacturing security professionals, the challenge is upgrading aging systems to prevent easy intrusions by attackers, as well as integrating technologies like IoT systems.

Fig. 4.5 Manufacturing companies with a formal ICT security policy (%, 2015)

Source: I-Com elaboration on Eurostat data



Cybersecurity should become an integral part of the strategy, design and operations, considered from the beginning of any new connected Industry 4.0 – driven initiative. The process to improve security should be viewed as a gradual one, rather than addressing all threats at once. For example, a written security policy can provide a framework for improvements, yet according to a study conducted by Cisco[4], 40 % of manufacturing security professionals said they do not have a formal security strategy, nor do they follow standardized information security policy practices.

If we look at only EU countries (Fig. 4.5), in 2015, only one

4 Cisco, *2017 Midyear Cybersecurity Report*, 2017

in three manufacturing companies had formally defined a written security policy. Sweden ranks first among the EU countries with 53% of manufacturing companies equipped in this sense, followed by Italy (45%).

However, undoubtedly, there is room for improvement by spreading best practices.

One major problem is the multitude of products and vendors in manufacturing settings, that creates a confusing picture for security experts. 46% of the manufacturing security professionals said they use six or more security vendors and 20% said they use more than 10 vendors. Asked specifically about products, 63% of security professionals said they use six or more products, while 30% said they use more than 10 products[5]. The complexity speaks for the need for both IT and OT teams to narrow their focus on security threats – for example, using only those products that can address the most immediate concerns. In addition, security is often outsourced, especially among small and medium enterprises (SMEs). In Italy, for instance, as well as in France and Germany, the most outsourced service among SMEs is incident response (Fig. 4.6), that is, the process by which an organization handles a data breach or cyber attack. This also includes the way the organization attempts to manage the consequences of the attack or breach, so as to limit the damage and minimize both recovery time and costs, as well as collateral damage such as brand reputation. In this case, as in any other case, except for audit services, 61%, 54% and 45% of SMEs, respectively, in the three countries use outsourced incident response services, compared with 42% in Italy and France, and 41%, in Germany, of overall enterprises. Only a small share of SMEs (less than 10%) declare not to outsource any of the considered security services.

On the one hand, the composition of security teams may be a hurdle to overcome in terms of protecting assets on the manufacturing floor. Nearly 60% of the manufacturing organizations said they have fewer than 30 employees dedicated to security. In addition, 25% said that a lack of trained personnel is a major obstacle to adopting advanced security processes and technology. On the other hand, manufacturers also need their IT and OT departments to share knowledge, so as to reduce to a minimum the consequences of one's processes or downtimes on others.

Given the aging systems in use in the industry, manufacturers are conscious of the need to improve and upgrade them not only for security reasons, but to boost their competitive advantage. According to a study by the Global Center for Digital Business Transformation[6], four out of 10 manufacturers will suffer market disruption over the next 5 years, in part because they do not modernize to meet offers from more advanced competitors. Security plays a key role in competitive advantage because it can help maintain brand reputation and avoid revenue and customer losses.

5 Ibidem

6 Global Center for Digital Business Transformation, *Life in the Digital Vortex: The State of Digital Disruption in 2017*, 2017

Fig. 4.6 Percentage of SMEs outsourcing security services, in selected EU countries (2017)

Source: I-Com elaboration on Cisco data

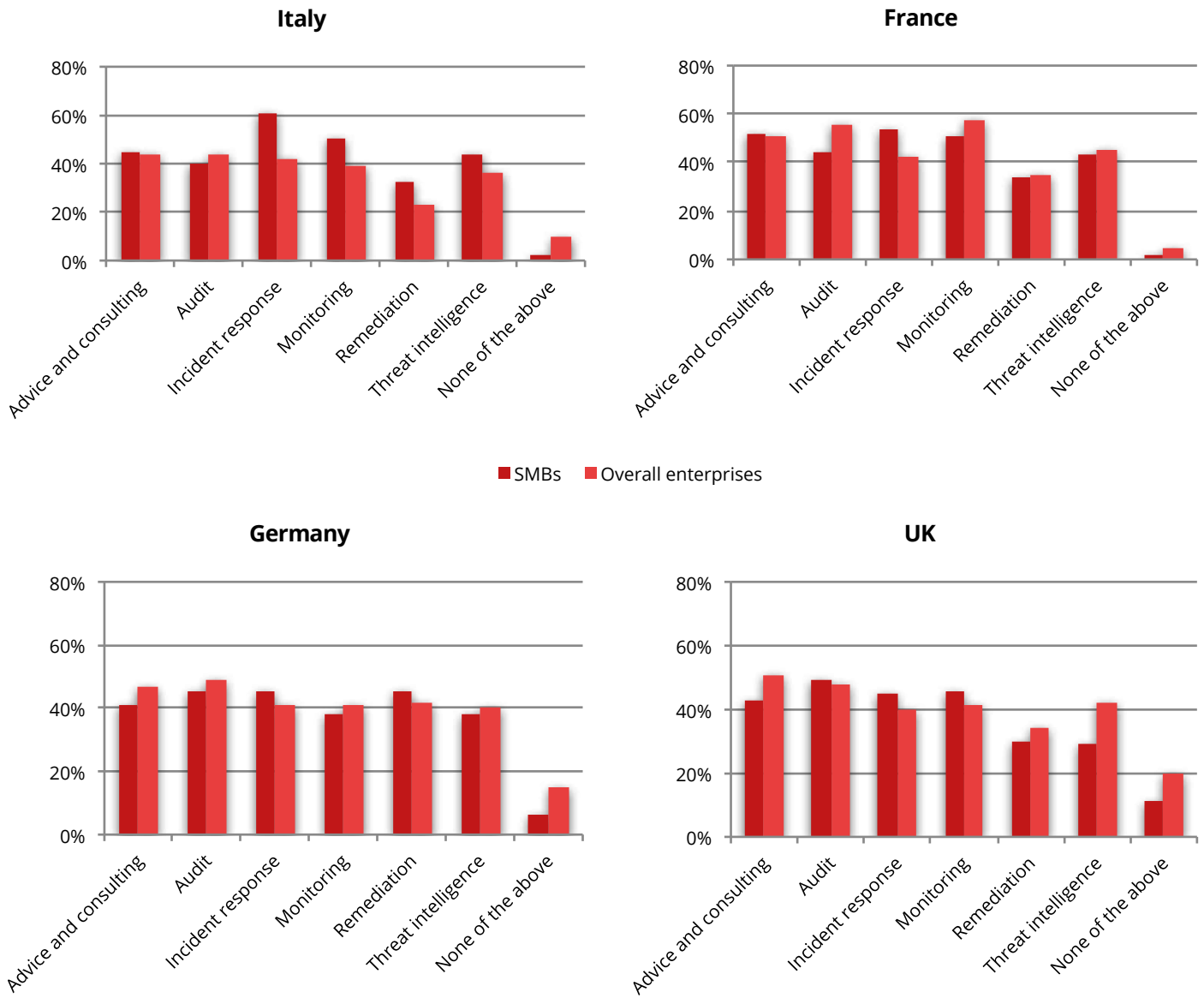
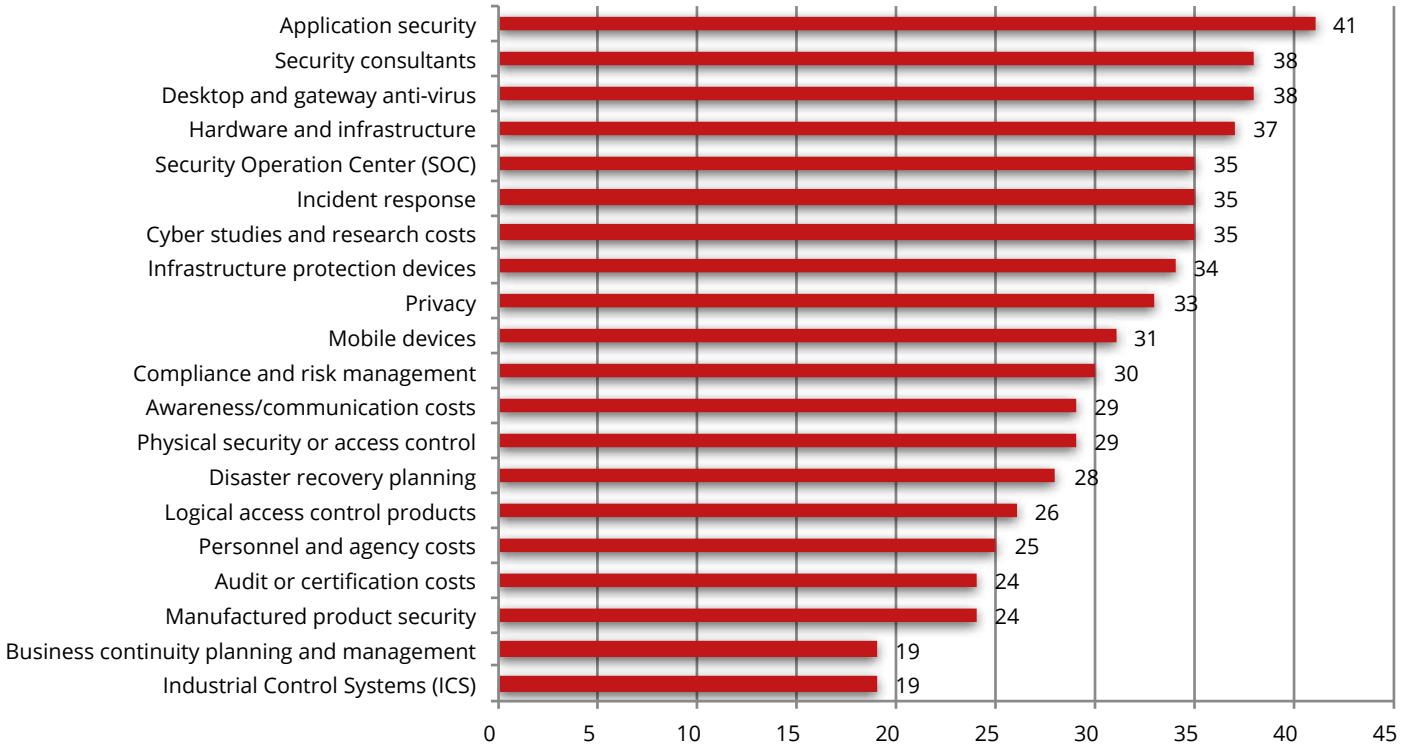


Fig. 4.7 Top initiatives funded in cyber budgets (%)

Source: Cyber risk in advanced manufacturing, Deloitte and MAPI (2016)



Meanwhile, increasing prioritization of cyber risk at the highest levels of the organization has led some companies to review compliance requirements for established cybersecurity regulations. According to a survey conducted by Deloitte[7], while only one in four manufacturers are reviewing the National Institute of Standards and Technology (NIST) framework, more than half of companies surveyed review and update their policies to be compliant with relevant cybersecurity laws and regulations. What companies mainly focus on is application security (Fig. 4.7), that is, the use of software, hardware, and procedural methods to protect applications from external threats (41% of interviewed companies). Secondly, they turn to security consultants (38%) or make use of anti-viruses (38%). 35% of them are attentive to incident response.

7 Deloitte and MAPI, *Cyber risk in advanced manufacturing*, 2016

4.1.4. The role of cloud computing

Cloud-computing applications will impact virtually every aspect of modern manufacturing companies. For companies, cloud computing will impact how they manage their operations, from enterprise resource planning (ERP) and financial management to data analytics and workforce training. The cloud will also prove integral to how manufacturers integrate into industrial supply chains. At the manufactured-product level, cloud computing will transform everything from how products themselves are researched, designed, and developed, to how they are fabricated, manufactured and used by customers in the field.

Moreover, cloud computing will play a key role towards enabling and democratizing new manufacturing production systems such as 3D printing (i.e., additive manufacturing), generative design, and the Industrial Internet of Things. Currently, digital services such as cloud computing provide at least 25 percent of the total input that go into finished manufactured products[8].

Cloud computing helps manufacturers manage their businesses with better intelligence, which is made possible through the expanded use of data analytics. The cloud is rapidly becoming the central venue for data storage, analytics and intelligence for most manufacturers. Cloud computing also empowers manufacturing operations, making them more productive, cost- and energy-efficient, safe and streamlined. Cloud-based systems can be scaled up or down to manage shifting project workloads, an especially important requirement for manufacturing firms. Moreover, it gives manufacturers the ability to leverage infinitely scalable computational resources on an on-demand, pay-as-you-go basis, so that they can readily access the computational resources they require without having to purchase expensive IT equipment up-front when they may only need it intermittently, which is especially important for small and medium-sized enterprises (SMEs) that lack the financial resources to purchase expensive IT equipment. Another key way cloud computing will impact modern manufacturing is by facilitating integration — whether of widespread supply chains or of the data streaming from IoT-enabled production equipment on the factory floor.

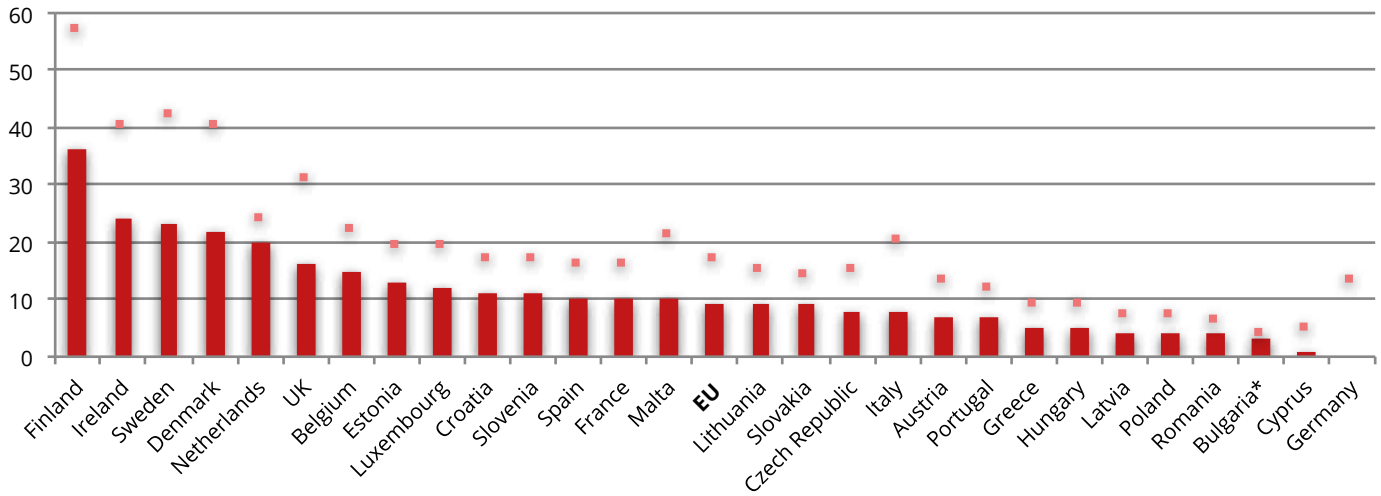
Thus, whether it's how manufacturing enterprises operate, how they integrate into supply chains, or how products are designed, fabricated, and used by customers, cloud computing is helping manufacturers innovate, reduce costs, and increase their competitiveness. Cloud computing allows manufacturers to use many forms of new production systems, from 3D printing and high-performance computing (HPC) to the Internet of Things (IoT) and industrial robots. Moreover, it democratizes access to and use of these technologies by small manufacturers.

The security aspects are very important when cloud computing is used given that the security strategies that have been developed since the 80's are not applicable. The prime reason for this increased importance of security is that the servers' part of the cloud is not in the same

8 Sherry M. Stephenson, *The Linkage Between Services and Manufacturing in the U.S. Economy*, 2017

Fig. 4.8 Use of cloud computing services among EU manufacturing enterprises (2016)

Source: I-Com elaboration on data Eurostat



*2015 ■ Enterprises purchasing cloud computing services of medium-high sophistication level ■ Enterprises buying CC services

domain, i.e. the data owner and cloud computing servers are normally in two different domains. Many private users, as well as organizations, hesitate over the adaptation of cloud computing and its services because of the risks related to the security and privacy of these services.

The degree of adoption of cloud computing services – especially those of medium and high level of sophistication[9] – is, in fact, still quite low across EU manufacturing enterprises (17% and 9%, respectively) (Fig. 4.8), though with much higher shares in certain countries, especially the Northern ones. Finland leads where 57% of manufacturing companies make use of cloud computing services and more than one third of them use at least one of the cloud computing services of medium or high sophistication level.

Nonetheless, some argue that one benefit associated with cloud computing is, among others (scalability, operational efficiency, application and partner integration, data storage, management, and analytics), that it can actually make manufacturing IT systems more secure[10]. This is because cloud-computing providers employ best-of-breed cybersecurity practices that are often far more

9 They include: hosting of the enterprise's database, accounting software applications, CRM software, computing power.

10 American Enterprise Institute, *How cloud computing enables modern manufacturing*, 2017

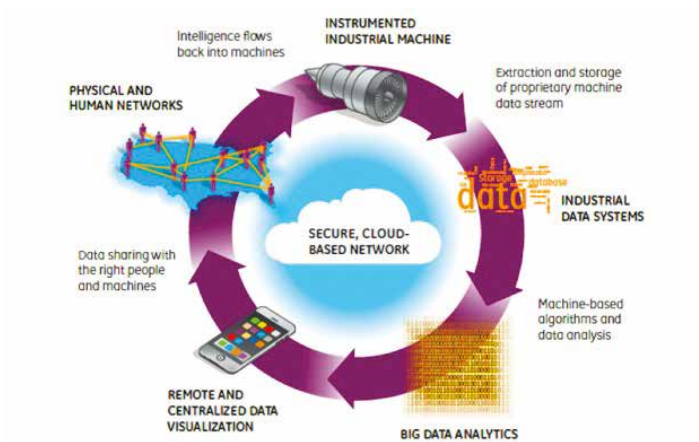
sophisticated than what individual companies can achieve by themselves on a one-off basis. Cloud computing providers are able to develop expertise in secure computing that other companies cannot easily match. While cloud computing does not guarantee security, and organizations should investigate the terms of service and security practices of any particular service provider, the net result of a shift toward greater use of cloud computing will likely be a decrease in the overall security risk profile of those companies. This is particularly true for SMEs that lack the required resources and expertise to implement strong security programs. Cloud computing represents an opportunity for these organizations to have better data security at affordable prices. In addition, the use of a single set of infrastructures versus multiple, older data centers actually boosts security, because consolidation means less complexity, and less complex infrastructure is easier to lock down.

On the other hand, as The Industrial Internet Data Loop represented in Figure 4.9 shows, a secure, cloud-based network computing is essential since it acts as the central hub for modern industrial production systems. The cloud, indeed, connects instrumented industrial machines to industrial data systems, making possible both big data analytics and data virtualization while facilitating engagement with physical and human networks. This leads to a virtuous cycle of continuous improvement, as the data being generated by industrial machines are fed through machine-based algorithms and data-analysis strategies to generate value-added insights that are then fed back into the machine and applied to the broader industrial system.

Clearly, the development of globally interoperable technical standards, as well as a common terminology, to define data will be vital if cloud computing is going to serve as the platform for integrating data from production equipment, devices and sensors made by vendors from throughout the world. Currently, there exists insufficient interoperability to pass data from design and product definition through to production equipment and processes. For example, it's often difficult to pass product-definition data from the controller on the machine tool to the coordinate-measuring machine that is going to inspect it. This is a challenge exacerbated when machines are made by different manufacturers, even worse, when involving different manufacturers from different countries.

Fig. 4.9 The Industrial Internet Data Loop

Source: American Enterprise Institute



4.2. CYBERSECURITY IN THE ENERGY SECTOR

Digitalization enables the growing use of renewable resources, storage, e-mobility, micro grids and distributed generation in the energy sector. However, this means, on the one hand, the continuous introduction of intelligent components that communicate in much more advanced ways (two-way communications with wired and wireless communications) than in the past. On the other hand, digitalization involves a raised exposure to cyber attacks due to the addition to the energy networks of devices (based on standardized components) with common vulnerabilities.

With the increasing digitalization of the energy sector, new technology advances and trends have emerged, such as integration of Internet of Things (IoT) in devices, cloud services, analytics to effectively manage digital devices using big data, expansion of the telecommunication infrastructures and networks, and applications with close demand and response integration.

The increased complexity of the energy networks is reflected in the way energy and energy related information and data are used, shared, processed and controlled as well as communicated. Digital utilities are becoming increasingly data driven and big data analytics will become part of their primary processes. In this changing context, adding new technologies and services to a network requires prioritizing cybersecurity risks and the relative competences.

4.2.1. The ongoing change in the energy sector

Among other critical infrastructures, energy infrastructures are some of the most complex and strategic because all everyday life sectors (telecommunications, finance, health, transport, etc.) depend on them to deliver their services. Indeed, a lack of energy supply has a huge impact on the economy. According to a 2015 Lloyd's study, a potential power interruption for a long period could affect society, industry and trade, with a tangible risk of impact on GDP (Gross Domestic Product).

The energy sector is evolving in a new system where digital technologies are playing an increasingly important role, allowing the establishment of a new paradigm. A smarter energy system can perform power generation, transmission, network management and market related tasks with better precision. It can also give a faster response than a human dependent system, optimizing energy management, prioritizing usage, and setting policies for quick response to outages.

Energy control systems are used to monitor and control operations that in case of energy transport and distribution networks are widely dispersed (SCADA – Supervisory Control and Data Acquisition) or for single facilities or small geographical areas (DCS – Distributed Control Systems). These systems are connected to remote components such as remote terminal units (RTU) and programmable logic controllers (PLC) that monitor system data and initiate programmed control activities in response to input data and alerts.

Currently, new technologies are introducing new intelligent components (e.g. electricity or gas smart meters, digital valves or pumps) to the energy infrastructures that communicate in advanced ways.

These new components are based on information and communication technology (ICT) that can be interconnected to local networks.

The increased efficiency in supply services has brought an increased exposure to cyber incidents and attacks. Indeed, the digitalization of the energy sector raises the concern on how to address the risks and threats of cyber incidents and attacks affecting personal data and strategic energy infrastructure data, which can be crucial for the security of the energy supply.

In the energy sector, two high-level objectives were defined by EECSP (Energy Expert Cybersecurity Platform):

- a secure energy system that provides essential services to EU society;
- data protection in the energy systems and the privacy of EU citizens.

The energy market is changing, both significantly and rapidly. The increasing shift towards renewable energy and the above-mentioned digitalization technologies have allowed for the appearance of market players using applications with a high demand and supply integration, e.g. virtual power plants.

European citizens have become energy producers that can be virtually managed by new operators through the cloud and new market players have emerged (as aggregators and third parties managing demand and supply).

As well, utilities and operators use demand response as a resource for balancing grid supply and demand. These programs can lower the cost of electricity in wholesale markets, and lead to lower retail rates. Demand response programs could be increasingly valuable options in grid management. Moreover, the spread of renewable resources leads to a more dynamic pricing of electricity products. All these changes in the market are enabled with more digitalization and more interaction among market participants.

However, with the growing use of digital devices and more advanced communication systems, the overall cyber risk has increased. The focus of cybersecurity in the energy sector is to support the sector's reliability and resilience even in the event of a cyber attack.

The three main protection goals for cybersecurity have been defined – Confidentiality, Integrity and Availability (CIA). In the energy sector, the priority objective depends on the specific position in the supply chain.

For example, in generation and transmission, availability and integrity are the most important as altered or delayed data could result in misconfiguration of devices that eventually could affect system reliability. Instead, for the advanced metering infrastructure, confidentiality of customer personal data is the most critical objective.

For nuclear energy, the protection goals must prevent cyber acts that could (directly or indirectly) lead to unauthorized removal of radioactive material, sabotaging nuclear material or nuclear facilities or theft of nuclear sensitive information.

Regardless of the source of a cybersecurity incident, the potential impact on the energy sector is similar, e.g. brownout, blackout or misconfiguration of control systems.

The described changes in the energy sector have highlighted the cybersecurity need to keep pace with increasingly sophisticated cyber threats.

4.2.2. Cybersecurity concerns and available answers

In 2016, with the adoption of the Directive on Security of Network and Information Systems (EU Directive 2016/1148) and the General Data Protection Regulation (EU Regulation 2016/679), the European Commission has begun to define a cross-sectorial approach to cybersecurity.

Due to the absence of a sectorial differentiation in the framework of NIS Directive and GDPR, DG Energy[11] has entrusted the EECSP-Expert Group[12] with the task to analyze if the energy sector is sufficiently covered by the existing legislation or if there is a need for more action to achieve effective cybersecurity.

The EECSP-Expert Group identified the strategic areas and the gaps not covered by the existing legislation. Although most energy subsectors already have some measures in place, this should be supported by a formalized and effective threat and risk management system at EU level. According to the EECSP-Expert Group, a structured and comprehensive way to identify operators of essential services for the energy sector at EU level should be pursued. Moreover, a shared governance on cybersecurity and a secure, controlled disclosure of information should be established.

The second strategic priority is to establish an effective response framework that allows a rapid and coherent response in emergencies related to cybersecurity. To achieve this, a cyber response coordination framework focused on the energy sector, taking into consideration the central role of energy in modern society needs to be defined and implemented at a regional level.

The third priority is related to energy sector protection through the improvement of cybersecurity resilience. It is important to work on the establishment of a European cybersecurity framework, specifically designed for energy. Europe should promote internal coordination and pursue international cooperation, in order to involve all EU actors in cybersecurity for energy. The final goal should be the sharing of information and best practices.

The last identified priority is the availability of adequate energy cybersecurity skills and competences. The lack of specialized resources and specific skills can be addressed through personnel training. Furthermore, promoting research can create the right conditions fulfilling this last strategic priority in the near future.

Clearly, a key role will be played by the ability and willingness of different stakeholders to cooperate and collaborate in a common goal. However, it is important to take into consideration that the continuous "smart" evolution of the energy sector is increasingly linked to the digital world and its further evolution.

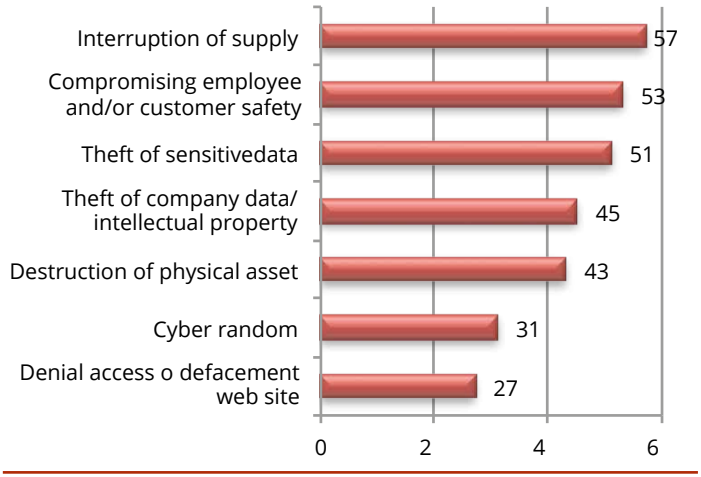
To date, cybersecurity efforts in the energy sector have focused on the transmission networks. However, also distribution grids address the risks of cyber attack, that could result in blackouts, disrupting industry as well as other services such as transportation and health.

According to a 2017 Accenture survey, the main utilities' concerns on cybersecurity are related to the interruption of supply (57%) and employee and customer safety (53%).

11 European Directorate General for Energy.
12 Energy Expert Cybersecurity Platform.

Fig. 4.10 Utilities' cybersecurity concerns (%, 2017)

Source: Accenture



A less troubling concern appears to be the denial of access to a company website or its defacement (27%) (Fig. 4.10). Utilities recognize cyber criminals and governments or their agents as the main types of attackers, – 29% and 24%, respectively (Fig. 4.11). The most rapidly spreading threats in recent years have been cyber crime – organized groups of hackers that carry out criminal acts for profit – and cyber espionage – nation-state directed or inspired attacks, including own-government.

A Marsh 2017 survey showed that 61% of interviewed energy organizations placed cybersecurity in the top five risks faced by their organizations. Companies play a key role in promoting cybersecurity. In 2015, only 40% of European energy enterprises had formally adopted an ICT security policy (Fig. 4.12). The best performer was

Fig. 4.11 Types of cybersecurity attackers (2017)

Source: Accenture

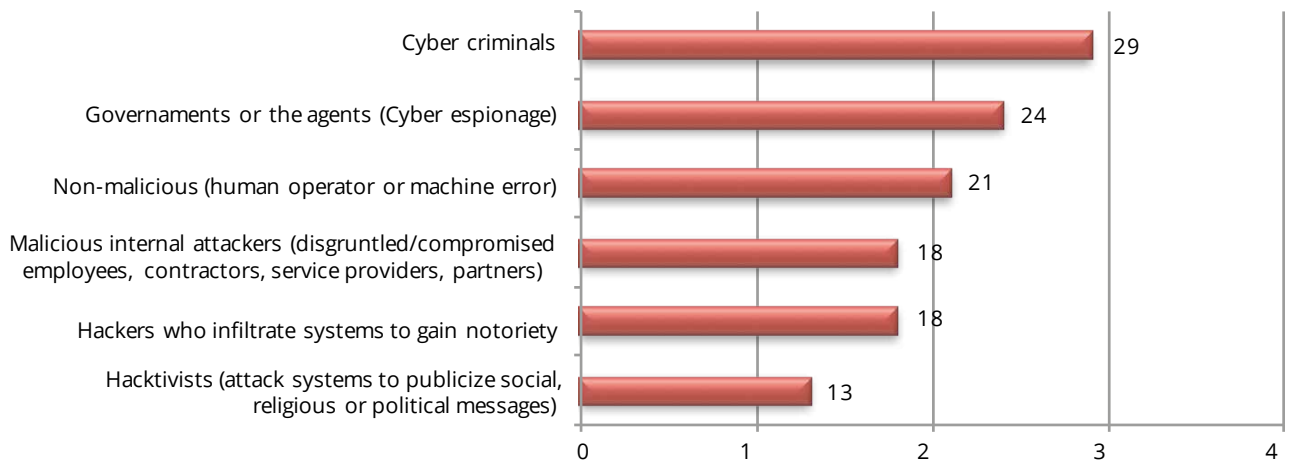


Fig. 4.12 Energy enterprises with a formal ITC security policy (%, 2015)

Source: Eurostat

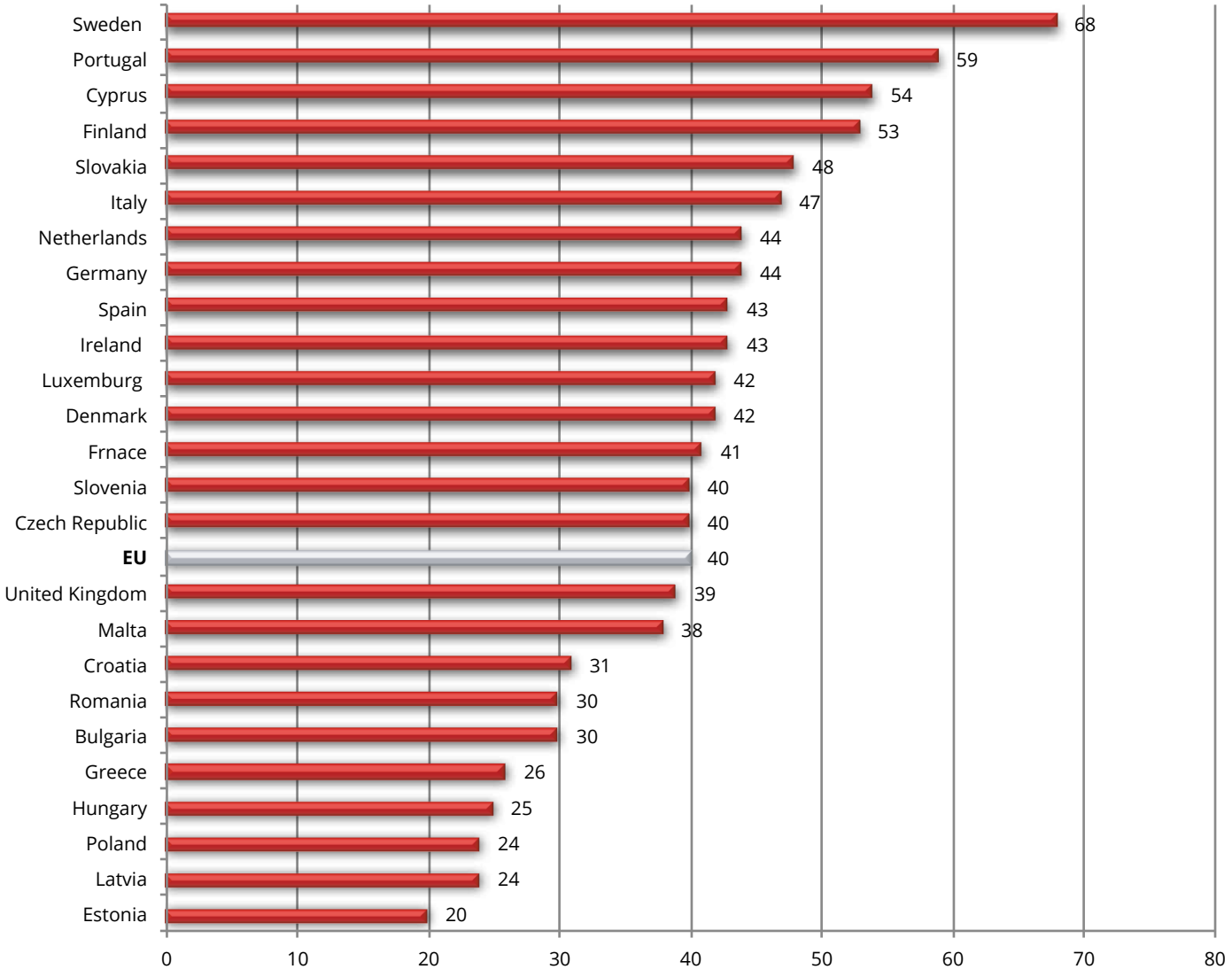
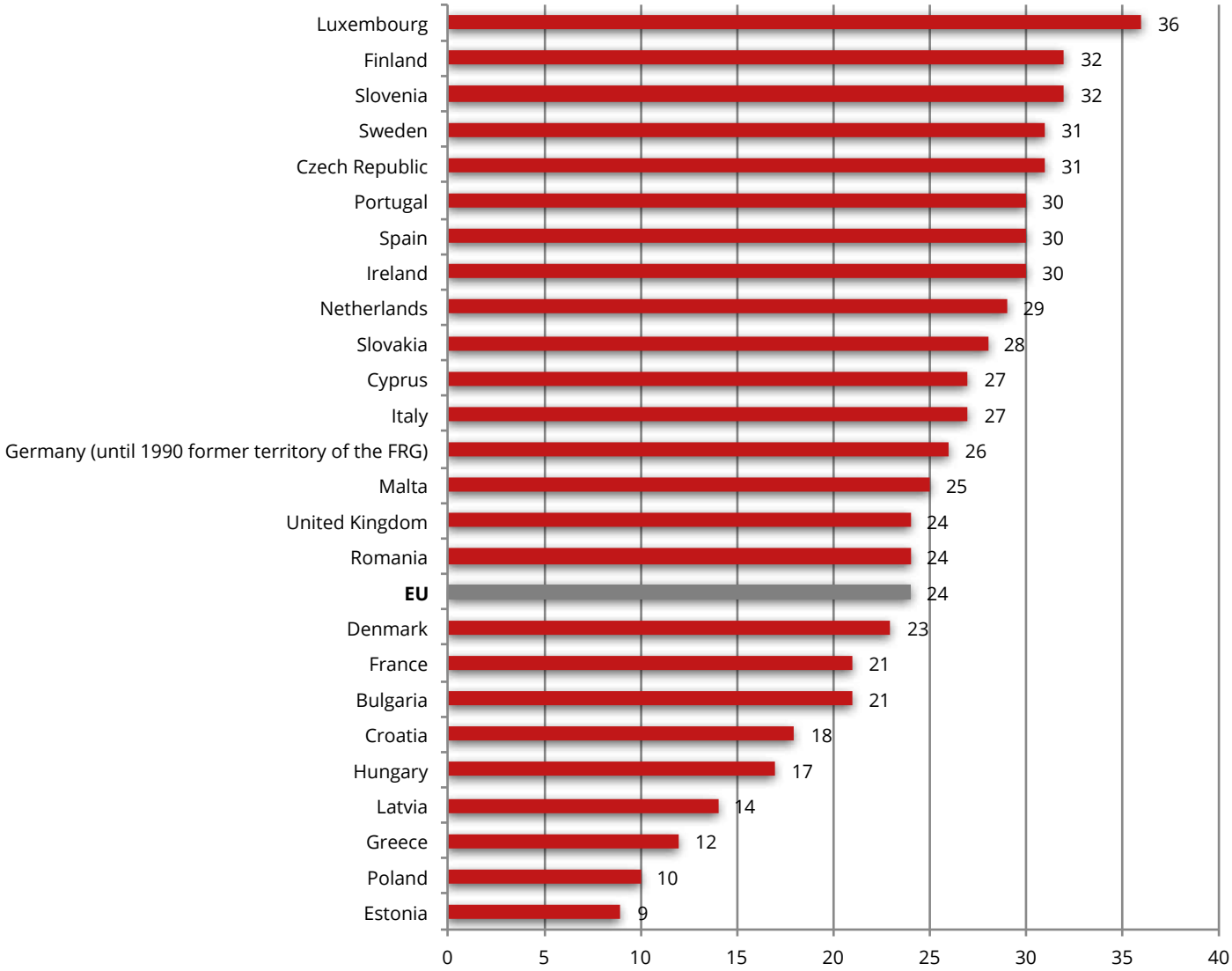


Fig. 4.13 Energy enterprises with a formally defined ICT security policy – new or reviewed over the last 12 months (%, 2015)

Source: Eurostat



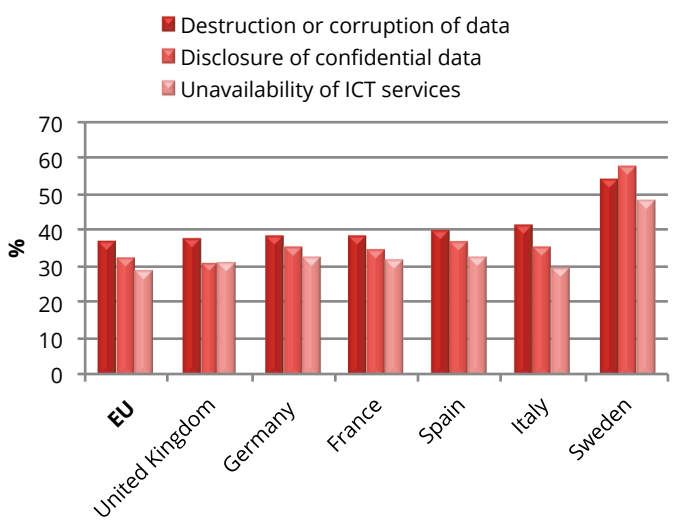
Sweden (68%), followed by Portugal (59%), Cyprus (54%), Finland (53%), Slovakia and Italy (48% and 47%).

In the same year, on average, 24% of EU energy enterprises formally defined (or reviewed) an energy security policy in the previous 12 months (Fig. 4.13). Luxemburg topped the ranking (36%), followed by Finland and Slovenia (32%).

EU energy companies were less worried by the unavailability of ICT services due to an attack from outside (e.g. Denial of Service attack) and only 29% of enterprises had a formally defined ICT security policy against this cyber threat. While 37% were concerned about data destruction or corruption resulting from an attack or unexpected incident (Fig. 4.14). Swedish concerns about disclosure of confidential data almost doubled in the European average (58% vs. 33%).

Fig. 4.14 Share of energy enterprises with an ICT security policy, by type of risk (%, 2015)

Source: Eurostat



4.2.3. The role of cloud computing

The future of modern energy is based on connecting a large amount of decentralized local producers and operators of energy storage systems, as well as electricity producers and consumers, all working together through remote control and monitoring as virtual power plants. The key components of the ongoing transformation in the changing energy sector are: energy efficiency, distributed energy sources, demand response, storage, advanced hardware/software and energy cloud.

Deriving from cloud computing, the energy cloud represents a clear evolution in the traditional relationship between utilities and stakeholders. More specifically, the energy cloud represents the evolution of old generation models, combining the large-scale economy with the flexibility of distributed energy sources. Supported by technological progress, energy cloud includes platforms to enable the matching of traditional market players and customers.

With regard to security issues, many cloud experts believe that trusted cloud data centers have better security than in-house data centers, so security is contingent upon the reliability of the provider. Although the main reason for adopting cloud was originally not to do with security, this could become a key success factor for cloud computing companies.

In analyzing the use of cloud computing in Europe it emerged that 19% of European energy enterprises used at least one of the cloud computing services in 2016.

Fig. 4.15 Energy enterprises using cloud computing (%, 2016)

Source: Eurostat

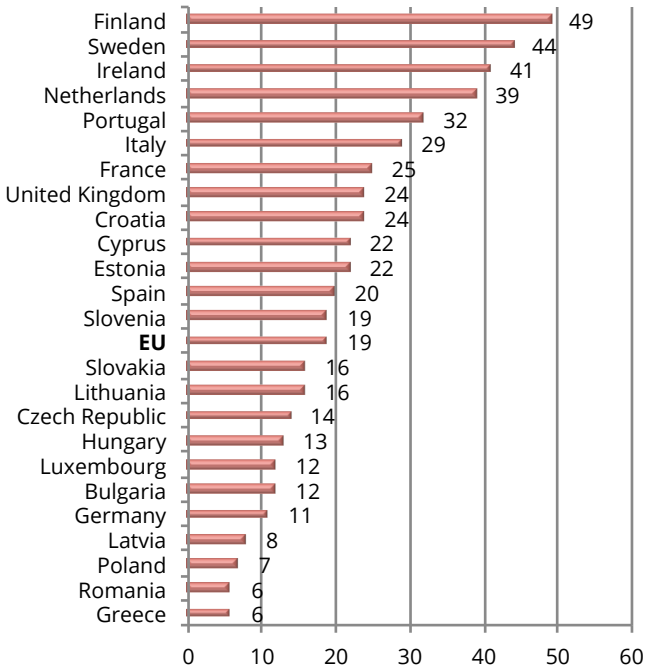
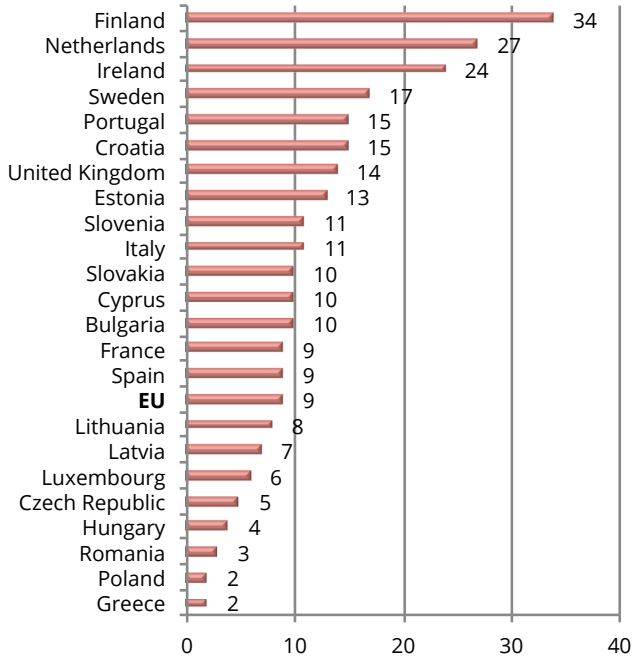


Fig. 4.16 Energy enterprises using high cloud computing services (%, 2016)

Source: Eurostat



Finland was the best performer, with almost half of energy enterprises using the cloud, followed by Sweden (44%) and Ireland (41%) (Fig. 4.15).

Nordic countries emerged as the main users of the cloud. Concerning high cloud computing services[13], Finland was the first with 34% of energy companies subscribing to them, while the EU28 average was only 9% (Fig. 4.16), while Sweden topped the ranking in both low and medium cloud services (15% and 27%, respectively).

4.2.4. Examples of security breaches

Cyber attacks in the energy sector could have an impact on all economic activities. Cyber risks are growing in terms of both the sophistication and frequency of attacks. The economic and physical repercussions on energy infrastructures could be serious, making it an

13 According to the Eurostat ranking, there are three levels of services: *Low*: email, office software, storage of files; *Medium*: email, office software, storage of files, hosting of the enterprise's database; *High*: accounting software applications, CRM software, computing power.

attractive target.

To improve the protection of energy systems and limit any possible domino effect, the energy sector should take a systemic approach and assess cyber risks across the entire energy supply chain. However, measures that require supply chain compliance or cross-border cooperation are more difficult to implement and require increased cooperation across sectors and states.

Companies should implement measures to prevent, detect and respond to cyber threats. These include both technical measures of resilience (e.g. security measures for software and hardware, measures for managing physical structures), and human resilience measures built on developing a strong cyber awareness culture within organizations.

Working across sectors, collaborating with governmental and private sector institutions help companies to better understand the nature of cyber risk impacts. Although information on breaches is quite confidential, energy cyber attacks are becoming much more widespread. Disseminating information about incidents, sharing best practices and introducing international cybersecurity standards are key elements for addressing the challenge.

One of the most recently publicized cybersecurity breaches within the electricity sector was the Ukraine power grid cyber attack on December 23, 2015. This well-planned hack on three power distribution companies caused outages for 80,000 energy customers. It is the first known hack to cause a power outage. and began with a spear-phishing campaign. It is classifiable as a combination of hacking and human error.

As well, there have been other important attacks.

In 2012, the whole Saudi Arabia economy was affected by the Shamoon virus, which infected 30,000 computers belonging to Saudi Aramco, the world's largest oil and gas producer. Some systems were offline for 10 days, and 85% of the company's hardware was destroyed.

In 2013, a computer virus attacked a turbine control system at a US power company after a technician inserted an infected USB drive into a computer on the network. The incident kept a plant off-line for three weeks.

In 2014, South Korea reported a cyber attack against the operator of its nuclear power plants. The attackers released sensitive and confidential information online, including the designs and manuals for the plant's equipment.

In 2015, hackers attacked the Maitland office of the Department of Resources and Energy in New South Wales (Australia). The hackers may have been interested in the department's current projects or may have viewed it as a weak link to access more highly classified government information.

In 2016, in Israel an employee of the Electricity Authority was the victim of a phishing attack, which infected a number of computers on the network with malware. The power grid was not affected, but it took two days for the Authority to resume normal operations.

These examples highlight the large variety of potential attacks. If we consider that these events were a tiny subsection of the real number of incidents that have occurred recently, the scale and complexity of the risk becomes apparent.

4.2.5. Smart grid opportunities and risks

Smart grids are the two sides of the same coin, representing both a risk and an opportunity. On the one hand, the increased connectivity of industrial control systems is leading (and increasingly in the future) to significant benefits in terms of safety, productivity, improvement of quality service and operational efficiency. On the other hand, such increased connectivity increases the risk of exposure to cyber attacks and damages. The integration of IT technologies, operational technologies (OT) and IoT solutions for consumers opens up the possibility of new attacks on industrial control systems. It is therefore important to set up an adequate security system, so as to avoid information carried by the digital network being manipulated prompting malfunctions and interruptions in the supply of electricity with heavy consequences on an entire country.

Digitization has quickly changed the electricity sector and its dynamics. If, until a few years ago, the risk related to electrical infrastructures was mainly technical, today, this has markedly changed and the network must address (also) many other risks. Many utility control systems work on old or vulnerable operating systems with limited or no end point protection.

In the same way, mobile technology allows for greater efficiency and cost reductions through remote access to devices and systems, but makes (cyber) security critical[14]. Smart grids could be seen as an opportunity for distribution businesses, boosting high-level protection to previously vulnerable assets. For instance, to meet the security goal, the smart grid must integrate consolidated, end-to-end IT/OT and physical security into its design. This should be achieved through certificate-based, device-level authentication (where feasible), network protocols that support encryption, application security, network segmentation, security monitoring, incident response and a hardening process to confirm vulnerabilities are managed in a timely fashion (Accenture, 2017).

As mentioned above, the whole supply chain in the energy sector requires far greater scrutiny. Suppliers of hardware or services can have their solutions accidentally compromised by third parties, providing an easy route into the heart of a distribution business (e.g. a technician might inadvertently download malware while updating software through misdirection to an alternative site).

A successful attack could undermine consumer trust in utilities and raise security questions along the value chain. Hence, developing effective strategies to protect smart grids from potential IT breaches is becoming essential and urgent. Smart grids must be equipped with sophisticated protection mechanisms that can evolve rapidly and adapt to the continuous development of malware.

The need for cybersecurity is now a reality. It must become a core industry capability that protects the entire value chain right up to end users. Distribution grids have some specific challenges to address and smart grids provide the visibility and control to improve grid robustness. Utilities can work towards compliance with local security standards, or on developing security as a core business capability.

14 Requiring effective identity and access management policies and the use of additional measures (e.g. as multi-factor authentication to prevent stolen employee credentials from being used to access systems).

Although there is no single path forward, some steps should be considered by any distribution business to strengthen resilience and response to cyber attacks such as:

- investigating a platform approach to security in order to pool resources or define platform based models and technology solutions, which could help in addressing cybersecurity issues;
- integrating resilience into asset and process design. Cybersecurity should be considered in new distribution systems in order to make them more resilient;
- sharing threat information, an essential activity that could create awareness of the latest threat landscape and how to prepare accordingly;
- developing security and emergency management governance models that reflect the prevailing corporate culture. Each distribution business needs to consider its organizational and operational framework in order to choose the most effective approach;
- developing relationships with regional security officials and cyber response experts will be critical to an effective, efficient response.

4.2.6. Challenges in the energy sector

In the energy sector, cybersecurity is focused on supporting the system's reliability and resilience even in the event of a cyber attack. Unlike IT systems, a control system in the energy sector that is under attack cannot be easily disconnected from the network as this could potentially result in safety issues, brownouts or even blackouts. According to the EECSP, specific challenges for the energy sector are the following:

- **grid stability in a cross-border interconnected energy network**. This is related to electricity, gas and nuclear energy, due to the strong interconnection of the grids and pipelines across Europe, and the potential cascading impact across the regions of the "weakest link" problem;
- **protection concepts** reflecting current threats and risks is relevant for the entire energy sector. Protection concepts have to develop continuously into a changing threat environment. If only a few years ago, ICT technologies supported power systems, today these technologies are increasingly critical to guaranteeing the appropriate level of reliability and resilience in the whole sector. ICT has modernized the energy sector, but it has also added complexity and introduced new inter-dependencies and potential vulnerabilities;
- **handling of cyber attacks** within the EU is relevant to all energy sectors. An EU level approach is needed, due to the cross-border dimension of cyber attacks. There are several issues to take into consideration in handling cyber attacks – the ability to identify, detect, respond and recover from a cyber attack; the threat agents (e.g. state actors, organized crime, terrorism etc.); different levels of handling (e.g. operator, Member State, EU, military etc.); crisis management and cyber response abilities;
- **effects resulting from cyber attacks** not fully considered in the design rules of an existing power grid or nuclear facility. This challenge mainly impacts on the electricity sector, including nuclear energy.

The energy sector was designed and implemented to ensure reliability, including redundancy and fallback mechanisms, to meet n-1 reliability criteria. Protection mechanisms used in the past were mainly built against physical attacks, with design rules not anticipating cybersecurity;

- **introduction of new highly interconnected technologies and services** mainly impacts on the electricity sector, but also on the gas sector due to increased facility automation and interconnection. For nuclear energy, this challenge is not important, because the use of new technologies in the sector is strictly controlled, verified and authorized by competent authorities;
- **outsourcing of infrastructures and services** is relevant to electricity, gas and nuclear sectors. In the energy sector the demand for data services (e.g. cloud based) and dedicated telecommunication networks has grown. Consequently, the reliability of the energy sector is becoming dependent on other sectors with lower requirements in terms of availability and integrity. Outsourcing of infrastructures and services requires appropriate consideration and rules to manage the risks;
- **integrity of components used in energy systems** is relevant to electricity, gas and nuclear energy. The protection against corrupted components, which might have hidden functions or access (backdoor) capabilities included, is another important issue. Reliable security does only exist if trustful components are used and a trustful supply chain exists. Security encompasses the evaluation of appropriate encryption technologies as well as other protection technologies, the capability to identify and detect malicious activities;
- **increased interdependency among market players** is mainly relevant to the electricity sector. The energy market has changed tremendously and led to an interdependency among market players. Today, energy network stability is no longer uni-directional and mainly controlled by the TSOs. Due to the increased use of automation technologies to maintain network stability, the security of supply risks has grown, and potential interruption could be caused directly (DSO – distribution system operator) or indirectly (VPP – virtual power plant operator) by connected market players;
- **availability of human resources and their competences** is key to the entire energy sector. Resources with a broader set of skills, (e.g. ICT engineering and information security skills and sector specific engineering skills) are needed in all subsectors of the energy sector and nuclear energy;
- **constraints** imposed by cybersecurity measures in contrast to real-time/availability
- **requirements**. This challenge is relevant to electricity, gas and nuclear energy. Cybersecurity requirements cannot impact on the system operation. It is important that security controls and available measures be optimized to the real-time and availability requirements as needed in the electricity and gas subsector and in nuclear energy.

Tab 4.1 Challenges in the energy sector

Source: EECSP, 2017

CHALLENGE	ELECTRICITY	OIL	GAS	NUCLEAR
Grid stability in a cross-border interconnected energy network	X		X	X
Protection concepts reflecting current threats and risks	X	X	X	X
Handling of cyber attacks within the EU	X	X	X	X
Effects of cyber attacks not fully considered in the design rules of an existing power grid or nuclear facility	X			X
Introduction of new highly interconnected technologies and services	X		X	
Outsourcing of infrastructures and services	X		X	X
Integrity of components used in energy systems	X		X	X
Increased interdependency among market players	X			
Availability of human resources and their competences	X	X	X	X
Constraints imposed by cybersecurity measures in contrast to real-time/ availability requirements	X		X	X

As shown in Table 4.1, all of the challenges identified concern the electricity subsector, but not always the other sub-sectors (nuclear, oil and gas).

4.3. CYBERSECURITY IN THE AUTOMOTIVE SECTOR

4.3.1. Digitalization in the automotive industry

The digital revolution has already defined a new concept of mobility, which goes towards a more efficient, cleaner, safer and smarter future for all.

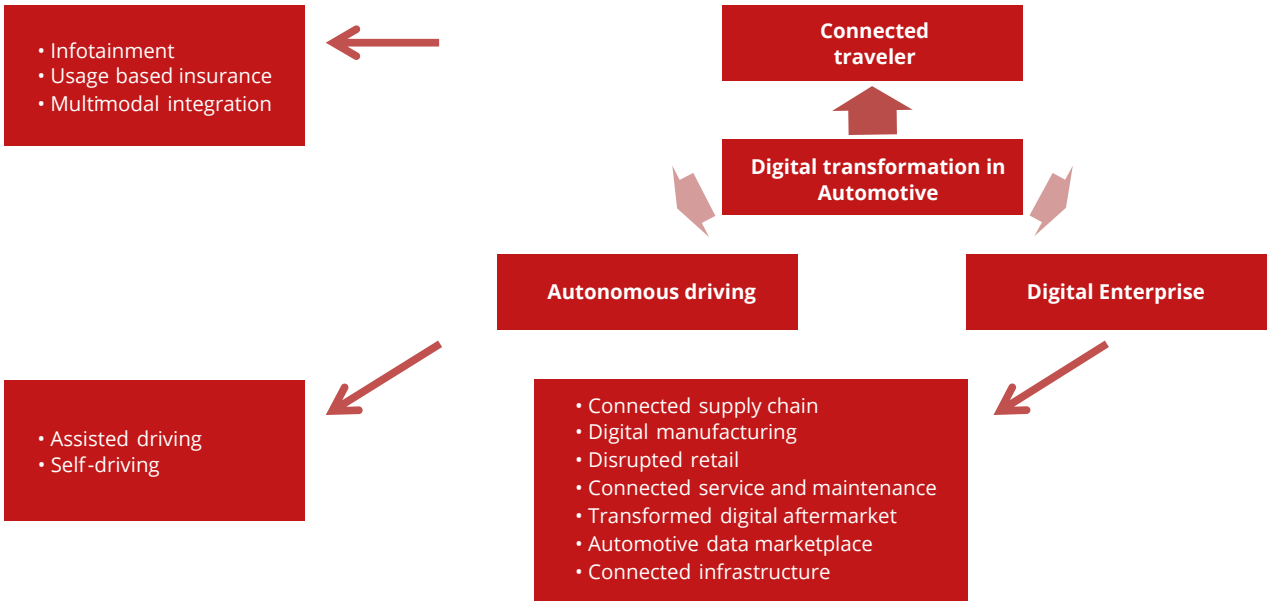
According to a joint WEF and Accenture paper[15], there are three key areas for the digital transformation in the automotive industry: Connected traveler; Autonomous driving; Digitizing the enterprise and ecosystem (Fig. 4.17). Therefore, the future trend is that every aspect of vehicular transportation will be controlled by telematics and information technology. In truth, connected vehicles already offer services relating to navigation, security, emergency and multimedia and service diagnostics. Therefore, assisted driving is already a reality and self-driving vehicles are already used in proof-of-concept testing around the world. However, the sheer scale and number of legislative, infrastructural and technological barriers will slow the rate of its adoption.

The rise of connected vehicle services across various functions will unleash an expanding flood of data – each with different levels of customer perceived privacy sensitivity – that needs to be captured, stored, analyzed and turned into intelligence to underpin services and revenues (Table

15 World Economic Forum and Accenture, *Digital Transformation of Industries. Automotive Industry*, White Paper, 2016

Fig. 4.17 Digital transformation in the automotive industry

Source: World Economic Forum and Accenture, 2016



4.2). The opportunities (driver safety, customer experience, quality and reliability, location-based services, dealer services, infotainment) from analyzing connected car data are numerous[16] and in the future will certainly increase.

Companies in all industries are seeking to understand what data they have and can potentially collect, what data others might have, and how they can use all this information to better serve customers and constituents. This is especially true in the automotive industry, which is one of the most data generation intensive industries in the world. The commercial promise of more precisely targeted customer offers, new business models and increased efficiency from data and analytics make these new businesses a veritable gold mine for automotive players[17].

As the new generation cars are real mobile devices connected to the Internet, car manufacturers are anxiously awaiting the 5G that will enable more efficient, fast and reliable connections among vehicles and between vehicles and infrastructures, improving road safety, enabling unmanned driving and the most advanced smart city services, such as traffic management. 5G, together with the Internet of Things, could

16 SAS, *The Connected Vehicle: Big Data, Big Opportunities*, 2015

17 World Economic Forum and Accenture, *Digital Transformation of Industries. Automotive Industry*, White Paper, 2016

Tab 4.2 Data generated by connected cars and the main use cases

Source: McKinsey & Company, Monetizing car data. New service business opportunities to create new customer benefits, 2016

Perceived privacy sensivity	CAR-RELATED USE CASE EXAMPLES		
	Macro-category	**Today**	**2020-2025**
Low	**External road and enviromental conditions** (e.g., ice warning on the road from ESP, fog from camera/sensors' feed	Real-time maps	Preventive safety car adaptation; Live road conditions reports
	Technical status of the vehicle (e.g., oil temperature, airbag, deployment, technical malfunctions report)	Car repair diagnostics; Automatic emergency call (e-call)	Predictive, remote service booking
	Vehicle usage (e.g., speed, location, average load weight in the trunk)	PAYD insurance; Toll/road tax payment	Reduce engineering costs; Trunk delivery
	Personal data and preferences (e.g., driver/passengers' identity, preferred radio station, use patterns of applications)	Vehicle settings "memory" based on key presence at entry	E-commerce in the car; Targeted advertisements
High	**Direct communications from the vehicle** (e.g., calendar, telephone, SMS, e-mail)	Speech control of messaging and e-mail	Proactive navigation and services; Virtual assistant/ concierge services

actually be the technology platform that connects cars and cities, hospitals and homes, and people to everything around them more meaningfully and this will completely revolutionize the way that we will travel in our daily lives. Moreover, 5G will provide new opportunities for business for companies operating in the automotive sector.

4.3.2. The current status and trends of the smart car market

The number of connected vehicles in the world is increasing considerably. According to some estimates, connected vehicle installations in China, North

Fig. 4.18 Connected vehicle installations from 2013 to 2018, by region (in mill. units installed)

Source: Statista, 2018

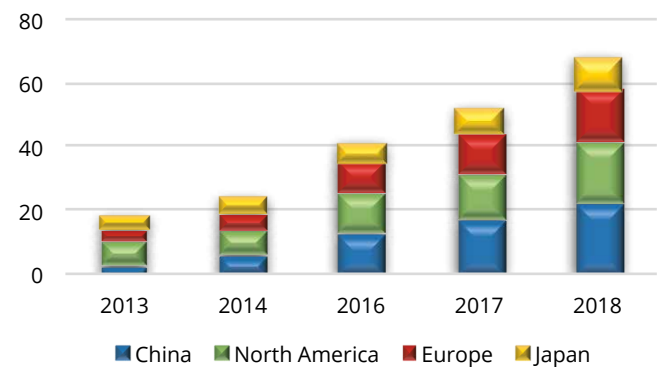


Fig. 4.19 Number of connected cars in 2025 and 2030 (mill. units installed, estimates)

Source: PwC, 2017

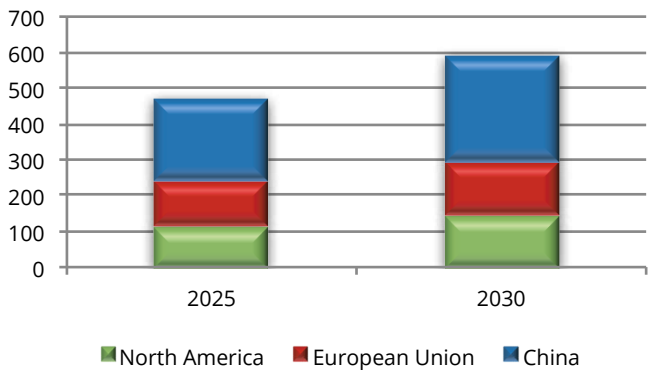
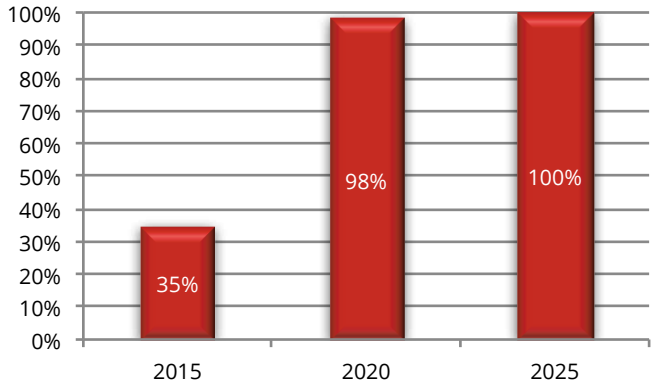


Fig. 4.20 Share of new cars sold connected to the Internet worldwide: 2015-2025 (estimates)

Source: Statista, 2018



America, Europe and Japan should reach 68 million by the end of 2018, an increase of 278% compared to 2013 (Fig. 4.18). Other estimates[18] even forecast a population of about 470 million connected cars in North America, China and the European Union by 2025, reaching 592.7 million installations by 2030. The largest market will be China, followed by the European Union and North America (Fig. 4.19).

Furthermore, some analysts are even more optimistic, predicting that 100% of new cars sold in the world will be connected to the Internet in 2025 (Fig. 4.20).

For autonomous vehicles, before showing their market trends, a distinction must be made among the various types of driving automation. There are 5 main different levels of driving automation:

a) Level Zero: No Automation

At Level 0, the driver performs all operating tasks like steering, braking, accelerating or slowing down, and so forth.

b) Level One: Driver Assistance

At this level, the vehicle can assist with some functions, but the driver still handles all accelerating, braking and monitoring of the surrounding environment. Think of a car that brakes a little extra when you get too close to another car on the highway.

c) Level Two: Partial Automation

Most automakers are currently developing vehicles at this level, where the vehicle can assist with steering or acceleration functions and allow the driver to disengage from some of their tasks. The driver must always be ready to take control of the vehicle and is still responsible for most safety-critical functions and all monitoring of the environment.

18 PwC, The 2017 Strategy & Digital Auto Report, September 2017

d) Level Three: Conditional Automation

Starting at Level 3, the vehicle itself controls all monitoring of the environment (using sensors like LiDAR). The driver's attention is still critical at this level but can disengage from "safety critical" functions like braking, leaving it to technology when conditions are safe.

e) Level Four: High Automation

The vehicle is capable of steering, braking, accelerating, monitoring the vehicle and roadway, as well as responding to events, determining when to change lanes, turn, and use signals. At Level 4, the autonomous driving system would first notify the driver when conditions are safe and, only then, does the driver switch the vehicle into this mode. It cannot determine between more dynamic driving situations like traffic jams or merging onto a highway.

Fig. 4.21 New autonomous car sales (mill., estimates)

Source: PwC, 2017

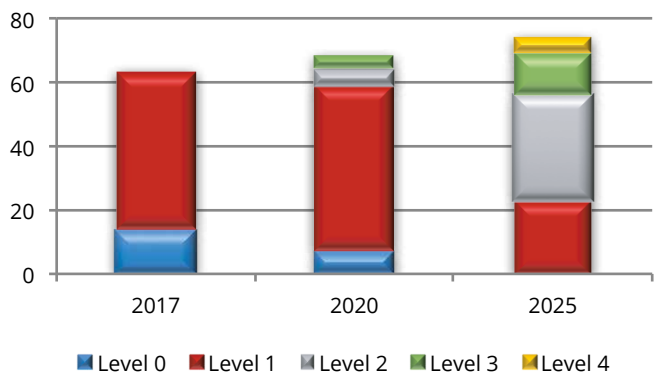
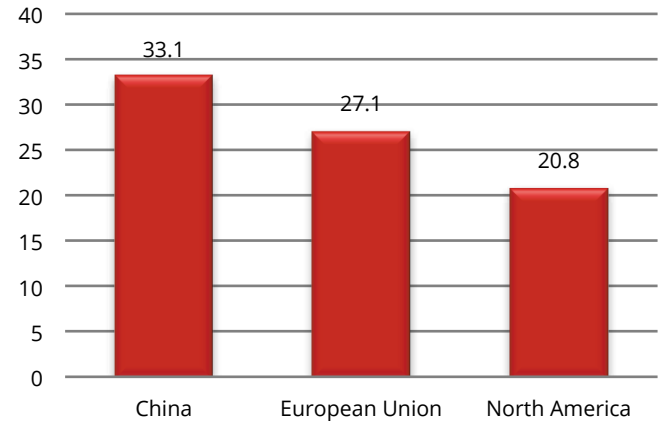


Fig. 4.22 Number of autonomous cars sold in 2030 (mill. units installed, estimates)

Source: PwC, 2017



f) Level Five: Complete Automation

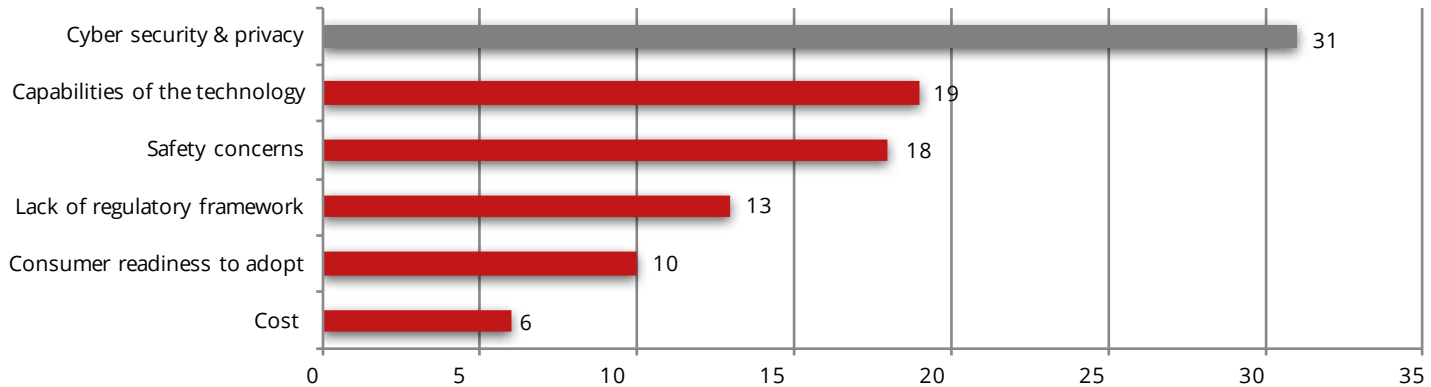
This level of autonomous driving is human attention free. There is no need for pedals, brakes or a steering wheel, as the autonomous vehicle system controls all critical tasks, monitoring the environment and identifying driving conditions like traffic jams.

According to some estimates[19], in 2017 only vehicles of levels 0 and 1 were available on the market in China, North America and the EU. Starting from 2020, level 2 and 3 vehicles will also be available, while from 2025 level 0 vehicles will disappear and level 4 will start being sold (Fig. 4.21). Autonomous level 4 and 5 will start to become mainstream after 2028 and the analysts forecast about 80 million level 4 and 5

19 PwC, *The 2017 Strategy & Digital Auto Report*, September 2017

Fig. 4.23 Main obstacles to the growth of connected cars (% of respondents)

Source: Foley, 2017



autonomous cars in China, North America and the EU by 2030. The first market will be China, followed by the EU and North America (Fig. 4.22).

4.3.3. The challenge of cybersecurity in the age of connected and autonomous vehicles

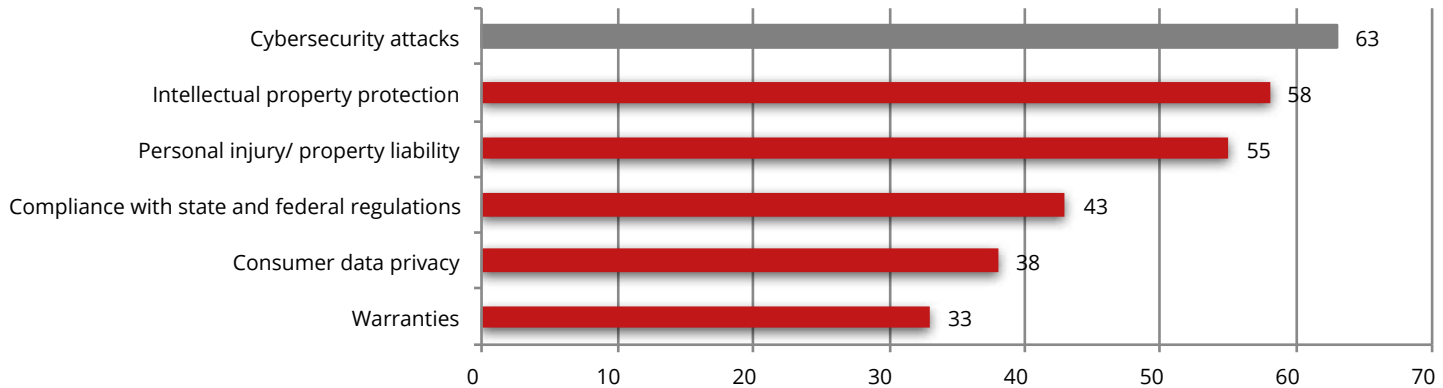
Computers and digitalization have made significant contributions to vehicle safety, value, and functionality – from stability control to electronic fuel injection, navigation, and theft prevention. They have also increased connectivity, adding many functions common to smartphones, such as cellular data and voice functionality, web browsers, online games, and entertainment. However, increases in the use of shared information and in-vehicle connectivity have made cars vulnerable to cyber attacks. Each electronic control unit (ECU) and the increasing array of sensors they work with must be secured in some form, whether it is via cooperating or co-processors, code verification, protection of data at rest and in transit, or other capabilities that have become common in Internet security[20].

Experts have proved that hackers can remotely access and control vehicle components or tap into private customer data collected by the on-board system. For instance, a hacker can access the internal network of the car and control the safety critical ECUs such as braking and engine start/stop operations. Undeniably, remote car hacking will become a dangerous threat for connected and autonomous cars[21].

20 McAfee, *Automotive Security Best Practices*, White Paper, June 2016.
21 Frost & Sullivan and Irdeto, *Cybersecurity for the Automotive Industry*, White Paper, 2017.

Fig. 4.24 Main legal issues to be addressed before the development of connected and autonomous cars (% of respondents)

Source: Foley, 2017



The cybersecurity risk for connected cars is of particular importance because external access to a car's network not only compromises the privacy of a driver's data, but also the cybersecurity threat to connected cars can become a matter of life and death, threatening the industry's road map towards autonomous and connected vehicles[22].

According to the results of a survey[23] conducted in the third quarter of 2017 on 83 automotive and technology executives between America and Asia, IT security and privacy – selected by 31% of respondents – are an important concern for connected cars and the main obstacle to their development (Fig. 4.23). In addition, cybersecurity attacks emerged as the top legal issue for 63% of respondents to be addressed in developing technology for connected cars and/or autonomous vehicles (Fig. 4.24).

Not only companies but also consumers are worried about cybersecurity for connected cars. Consumers are aware that a connected vehicle has the potential to be targeted by a cyber attack.

The Irdeto Global Consumer Connected Car Survey examined consumer awareness of cyber attacks targeting connected cars and autonomous vehicles in six countries – Canada, China, Germany, Japan, the UK and the US. According to this survey, 85% of global consumers indicated that they believe any connected car has the potential to be targeted by a cyber attack (Fig. 4.25).

In addition, the survey found that 59% of connected car owners are concerned that their vehicle could be targeted by a cyber attack (Fig. 4.26).

22 McKinsey & Company, *Shifting gears in cybersecurity for connected cars*, 2017.

23 Foley, *Connected Cars & Autonomous Vehicles Survey*, 2017.

Fig. 4.25 Share of consumers who think any connected car has the potential to be targeted by a cyber attack (%)

Source: Irdeto, 2017

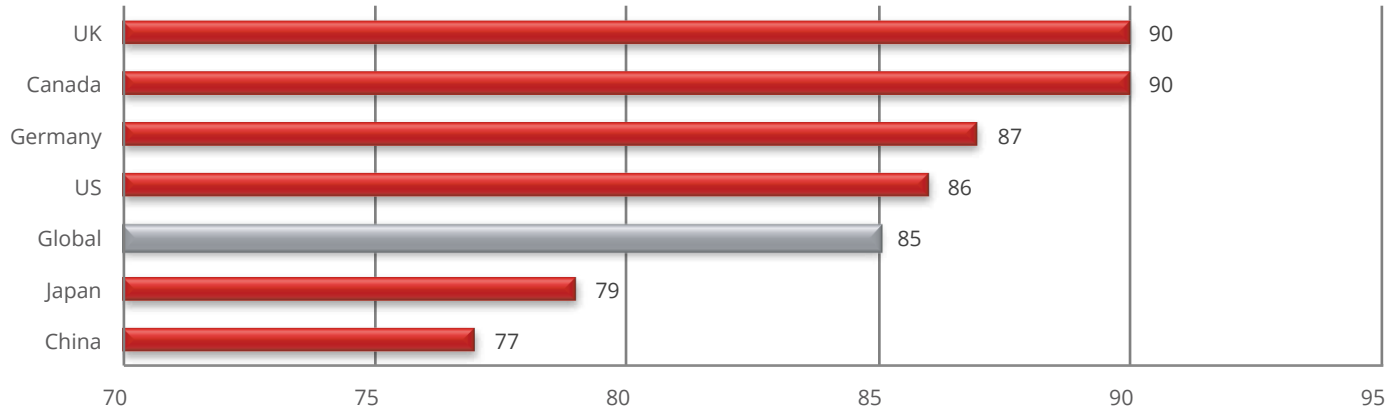
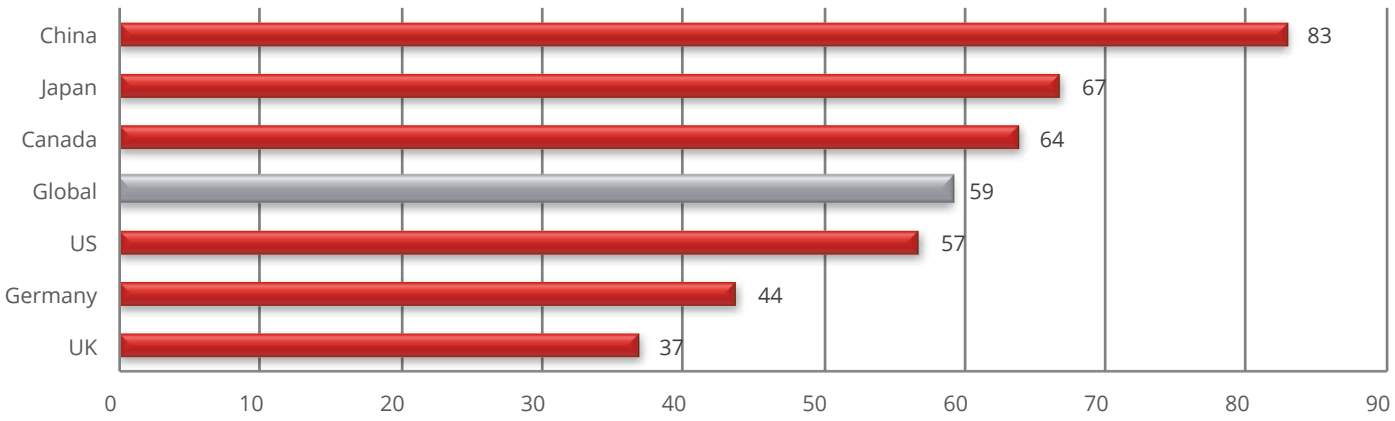


Fig. 4.26 Share of connected car owners who are concerned that their vehicle could be targeted by a cyber attack (%)

Source: Irdeto, 2017



Therefore, with vehicles already connecting, the risk has increased, and the core challenges will be establishing and maintaining trust, consumer confidence and vehicle safety. Certainly, companies have an important role to play in promoting and guaranteeing cybersecurity in the automotive sector.

4.3.4. Main cyber threats for smart cars

Remote fault diagnostics, telematics and connected infotainment significantly enhance driver safety and enjoyment, but they also present new challenges for the automotive sector as they turn vehicles into prime targets for cyber attacks. The growing risk of a vehicle's systems being infiltrated or having its safety, privacy and financial elements compromised, requires manufacturers to understand and apply IT security[24].

Cyber threats can have significant consequences for smart cars. Some of the most common ones include[25]:

- **Driving Safety Hazards**

The victimized vehicle can cause driver distractions such as arbitrarily turning on the in-car audio and turning up its volume. A more aggressive form of attack occurs when vehicle safety functions are disabled, thereby jeopardizing human life and public safety.

- **Cyber Ransom**

Cyber criminals have established an ecosystem in which they target connected vehicles with ransomware, which can lock users out of their cars until ransom is paid to the hackers.

- **Risks to Data Privacy and Integrity**

Gaining unauthorized access to data through interfaces such as USB, Wi-Fi, Bluetooth and mobile 4G/5G is becoming a relatively easy task, allowing hackers to delete or modify files on vehicles and on user devices. Every link is a potential point of weakness that attackers will be quick to seize on. An attacker only needs to find one insecure opening, whether that is peripheral such as bluetooth or a music download system, for example, and from there they may be able to take control of safety-critical electrical components like the brakes or engine and wreak havoc.

- **Physical Abuse**

Consuming memory space and squandering CPU cycles are just a couple of forms of physical abuse on connected vehicles. A more aggressive example is draining a vehicle's battery by turning on the headlight for a drawn-out period.

- **Stepping-stone Attacks**

A compromised vehicle may be used as a sort of stepping stone for sending bogus data to others or to penetrate the home environment.

4.3.5. The role of cloud computing

Gartner predicts a quarter-billion cloud-connected cars on the road by 2020. Cloud-based services offer new navigation system to drivers and passengers, such as the use of map data to determine the most optimal use of fuel during the car's route or vehicle-to vehicle (V2V) communication to help avoid accidents. Cloud connectivity is also changing infotainment and supporting the evolution of autonomous driving.

24 Kaspersky Lab, *Threat Predictions for 2018*, 2017
25 Trend Micro, *Cybersecurity Solutions for Connected Vehicles*, 2017

Moreover, the cloud can help automotive companies redefine and personalize customer relationships, transform and optimize operations, improve governance and transparency, and expand business agility and capability.

As cloud adoption by automotive companies matures, other benefits will also accrue. Business users will be able to design and prototype applications quickly. Organizations can benefit from new user-driven, mobile and cloud-centric information technology. The cloud is expected to support the transformation of enterprise IT functions, roles and responsibilities.

As well, business managers will increasingly use the cloud for application development to enhance agility[26]. Automotive companies are leveraging modern cloud-computing platforms for creating Cloud native Applications, Operating Systems, the Internet of Things (IoT), devising a comprehensive software development methodology. All of this has the potential to literally transform it into a global powerhouse.

Moreover, with cloud computing, you have round the clock support from skilled staff ready to manage the systems and its security. As well as the risk of failures, hacks and any type of technical breakdowns can also be reduced with cloud services. Cloud systems also ensure that cutting edge technologies improve the cloud's performance in terms of cybersecurity through platforms able to hinder any cyber attack attempt. Furthermore, for cybersecurity, there are a number of ways bad actors can compromise connected vehicle components and technologies, ranging from curious hackers attempting to demonstrate weaknesses, to malicious entities attempting to cause harm, on both small and large scales. Only through the thoughtful use of disruptive technologies such as big data, machine learning, artificial intelligence and use of cloud computing can we help build a better, safer and more secure connected vehicle ecosystem.

The use of cloud computing also ensures security during natural disasters. Imagine a situation – if all the important data of an organization is stored in the company's network of hardware or servers, and if a cyclone, storm or earthquake hits the area, there is a possibility that all the data could be destroyed. Cloud computing is a fit solution to avoid this. Even during a natural disaster, your data stays safe and intact in the cloud[27].

In conclusion, with the cloud platform, companies are creating smaller consoles and centers to reduce costs, lower risks, increase security and dramatically improve vehicular engineering.

26 IBM, *Cloud for automotive*, 2015

27 *How cloud computing helps to improve the automotive business?*, 2016. https://www.quora.com/How-cloud-computing-helps-to-improve-the-automotive-business

CONCLUSIONS AND POLICY RECOMMENDATIONS

1. DIGITAL SERVICE PENETRATION IN EUROPE

The economic growth connected to digitization and the creation of a digital single market in Europe foresees the massive penetration of digital services. In a context characterized by a widening development of telecommunication infrastructures and digital service penetration, it becomes important to:

- continue to urge investments in infrastructures and, in particular, in optical fiber and 5G that will result in an important technological evolution, and in the promotion of research activities to develop new generation technologies and services;
- stimulate the growth of demand in the less advanced countries and regions in order to reduce the digital divide, if necessary by providing EU and national incentive policies to acquire digital skills and access to enabling technologies;
- foster the digitalization of businesses, with a particular focus on SMEs. In this maturation process a strong contribution can be offered by the PA;
- launch awareness campaigns aimed at making businesses and citizens / consumers aware of the enormous opportunities related to digitization and at highlighting the new risks related to the digital revolution underway and, consequently, the available protection tools.

2. CYBERSECURITY

2.1. GENERAL POLICIES

Digitalization offers enormous opportunities for growth and simplification, but it also carries new challenges. In this difficult fight against cybercrime, the EU and individual Member States need to join forces for:

- a strong and unconditional support for the common European cyber-defense policy, also through the sharing of the best experiences from the Member States and the know-how of the relative research centers;
- a benchmarking of the implementation of the NIS Directive and National Cybersecurity Plans should be produced and released online by the EU institutions (EU Commission or ENISA);
- the strengthening of the provisional budget and human resources allocated to ENISA in order to allow the agency to fulfil its mandate;
- the European Union and its Member States to increase investments and bring together different EU funds, national funds and private sector investments towards strategic objectives, in the framework of a stronger cooperation between the public and private sectors;a ninth Framework Program (FP9) including more funds for cybersecurity R&D, enhancing the cooperation between the public and private sectors and between larger companies and SMEs;
- the creation of a solid cybersecurity skills base of

professionals and the increase in the awareness of citizens, particularly focusing on the youngest and the more elderly, and businesses, targeting SMEs.

2.2. MANUFACTURING

A new approach to security is a must for those who want to benefit from the added value potential of smart industry solutions in the future. As the complexity of the supply chain increases, so do the possible risks. Cybersecurity is no longer simply an end in itself as it has now become a key factor behind companies retaining their competitive edge in the age of digital transformation. Manufacturing in the future will be data-driven, networked and transparent. Threat levels today are completely different from a few years ago and production system security has increasingly become a topic for public debate.

One major issue when dealing with cybersecurity is that it has altered what used to be geographic borders into digital frontiers. Governments cannot face this alone. They should work with industry in a **public-private partnership** using economic tools to encourage, on the one hand, investment beyond ordinary levels of commercial cybersecurity spending and, on the other hand, the development of industry-led voluntary standards and best practices related to issues such as interoperability, privacy and security itself.

Cybersecurity in manufacturing usually deals with IoT security.

The following recommendations could be carried out[1]:

- given the lack of knowledge present within industries, **security education and training** should be established, if absent, or significantly enhanced. Among incentives devoted to Industry 4.0 such as tax credits, a part should go to training and hiring programs to improve cybersecurity skills within organizations, with a special focus on SMEs;
- encouraging the use of **open interoperability frameworks** that incorporate security and provide the necessary transparency;
- clarify **liability among IoT stakeholders**, filling possible gaps in the European and national legislation.

2.3. ENERGY

Over the last years, cybersecurity has become a critical cross-sectorial and cross-border issue for all stakeholders, companies and Member States. Global commitment to climate change and a low carbon economy have made the spread of smart energy a priority in the development of critical infrastructures. A cost effective low carbon energy system across EU requires a more distributed energy structure and a greater inter-connection and cooperation across national boundaries.

Cyber threats are increasing in the energy sector and

1 They are partly taken from ENISA, *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*, November 2017

Member States varyin their levels of readiness in terms of the status of existing assets, infrastructures, technical capabilities and economic situations.

Although the NIS has triggered important progress in the cyber- security framework, providing a multi-sectorial approach, the energy sector should now move forward in a clearer and more coordinated direction.

The energy system has become a potential target for cyber-attacks, also because the more **distributed model** offers hackers different opportunities. On the one hand, a distributed energy system has, unquestionably, a **higher number of potential vulnerabilities** and access points, on the other hand, the **effects** and the **impacts** of possible attacks **can be reduced and isolated to one part of the system**.

Among other general **non-legislative requirements** (e.g. harmonization of the security and resiliency standards, promotion of consumer awareness and engagement, the establishment of a stakeholder proactive and empowered network, and common smart energy communication systems), some policy recommendations have been made in order to set up an EU energy cyber- security strategy, which, however, require **legislative implementation. This involves**:

- **Designation of a central authority**. The definition of a responsible institution with an executive role for energy cyber- security. It will focus on cooperation in information sharing, incident reporting and other critical elements of energy cybersecurity;
- **Incident reporting**. The incident reporting and sharing of relevant information by Member States and all energy stakeholders should be encouraged;
- **Information sharing**. The standardization of information sharing should be a priority;
- **Alignment of cybersecurity activities**. All activities should be aligned and fully integrated with national cybersecurity and critical information infrastructure protection (CIIP) strategies and operations.
- **Security standards**. A set of minimum security requirements for communication and control devices applied to a smart energy network should be developed (e.g. mandatory security risk assessment, compliance standards and regulatory sanctions for non-compliance);
- **Certification board**. A certification board made up of public and private stakeholders to coordinate smart grid/energy cybersecurity certification and compliance activities should be created.

2.4. AUTOMOTIVE

The automotive industry is rapidly evolving and automakers are recognizing opportunities to use digital, connected and cognitive technologies to deliver superior customer experiences. The advanced technologies, that enable the production of connected and autonomous cars, have created new opportunities but also challenges related to cybersecurity. These challenges are not only threatening passenger privacy, but also the safety and reliability of automobiles.

Determining how to implement and maintain

cybersecurity principles in a complex vehicle development cycle is not an easy task and for this reason it necessary to provide a support (e.g. best practices or guidelines) for automakers who play a fundamental role in ensuring security and safety.

The best practices and guidelines for starting up a responsible vehicle cybersecurity management are described below[2]:

- **vehicle security by design.** Engineers and suppliers should build in security and privacy protection throughout the design of each vehicle. It is necessary to incorporate security into the vehicle development process, including the designing of security features into the hardware as protective functions for the vehicle control system and communications-based functions like navigation satellite radio, and telematics; and to use "threat modeling" as a design process to test systems for vulnerabilities and simulate attacks on security and design controls. Defenses obtained through security by design are intended to stop cyber-attacks before they impact a system;
- **risk assessment and management.** Risk assessment and management strategies can help assess the potential impact of identified cybersecurity risks and discovered vulnerabilities and assist in the development of protective measures. A cross functional team should be empowered with providing oversights and the enforcement of a company's cybersecurity program. Responsibilities should include secure product development requirements, threat management, responding to incidents, training and developing strategies for future threats;
- **create data governance protection**. Vehicle and consumer data security should be a top consideration when developing a data governance strategy. Security and compliance requirements should be put in place to address how data is stored, encrypted, accessed and shared. Privacy experts should help determine how the car collects and uses data and whether it complies with federal and state regulations;
- **contribute to industry security standards**. Automakers should proactively become involved in establishing regulations for vehicle security. Staying involved with industry networks and working with government agencies will help define where the industry is headed;
- **collaboration with and engagement of appropriate third parties and experts to address cyber risk**. Cybersecurity and regulatory risks cannot be managed alone and, for this reason, it is important to collaborate with experts who can ensure the appropriate utilization of cybersecurity measures and maintaining clear communication channels.

2 Some of these have been developed by the members of the Alliance of Automobile Manufacturers and the Association of Global Automakers that have collaboratively developed the Framework for Automotive Cybersecurity Best Practices, which is intended to support the ongoing efforts of the automobile industry on cybersecurity matters.
https://mse238blog.stanford.edu/2017/07/ramdev10/automotive-cyber-security-threat-guidelines-and-challenges/

2.5. DEVELOPING CLOUD COMPUTING IN A SAFE ENVIRONMENT

The development of cloud computing, which has the potential to revolutionize how organizations work (public and private), is slowed down by the fact that cloud computing providers face considerable regulatory uncertainties.

However, the greatest challenge facing cloud computing providers is **security and privacy**. In addition to the business concerns that are raised by these issues, privacy- and security-related mandates vary widely across jurisdictions. The variability of these requirements subjects end users to different types of potential liability depending on where their data is hosted. There is also a problem in the lack of **security skills** that, by contributing to the increase in the so-called "shadow IT activities" (that is, all those IT systems and solutions built and used inside organizations without explicit organizational approval), is interfering with their ability to keep the cloud safe and secure. Thus, there arises the need to urgently address this problem.

Cloud computing changes the **location of data processing** or, more correctly, makes the location of data processing irrelevant. Using the cloud model, applications can be run, and data stored, anywhere within the global cloud environment, which may encompass many data centers in multiple physical locations.

Even more commitment is needed when it comes to cloud computing deployment in the manufacturing sector. In particular, the EU, and not only, should consider both "domestic" and "international" policies to support greater penetration of cloud-enabled manufacturing among their industrial sectors. However, there is no need to create cloud-specific regulations. Cloud computing does not actually reduce an organization's responsibility for protecting its data or for ensuring the privacy of its customers' data. Thus, what governments really need to do is to **create cloud-neutral technology policies**.

What is needed is to both **support the development of globally interoperable, industry-led standards** and **negotiate**, at a global level, **trade agreements that prohibit the use of data localization policies**. The latter is especially important as the premise of cloud computing benefits lies in the ability of data to move seamlessly over the Internet. As a consequence, the proliferation of data-localization policies throughout the world would threaten to inhibit manufacturer integrated global production chains, all connected through the cloud. As well, policymakers should avoid launching data localization policies or imposing measures banning the transfer of data or requiring the local storage or processing of data. They should, on the contrary, pursue trade agreements adopting those norms which protect the movement, transfer and exchange of data.

i-com digital

PARTNERS

enel Google

I-Com – Istituto per la Competitività
Rome
Piazza dei Santi Apostoli 66
00187 Rome, Italy
Phone +39 06 4740746
info@i-com.it
www.i-com.it

I-Com – Institute for Competitiveness
Bruxelles
Rond Point Schuman 6
1040 Bruxelles, Belgium
Phone +32 (0) 22347882
www.i-comEU.eu