2013

Italian
Cyber Security Report

Critical Infrastructure and Other Sensitive Sectors Readiness

Cyber Intelligence
and Information
Security Center

SAPIENZA
Università di Roma

CIS Sapienza

Cyber Intelligence and information Security

2013 Italian Cyber Security Report

Critical Infrastructure and Other Sensitive Sectors Readiness

Research Center of Cyber Intelligence and Information Security
“Sapienza” Università di Roma

December 2013

CASA EDITRICE
UNIVERSITÀ
LA SAPIENZA
2013

List of authors

Marco Angelini

Maria Cristina Arcuri

Roberto Baldoni

Claudio Ciccotelli

Giuseppe Antonio Di Luna

Luca Montanari

Ida Claudia Panetta

Leonardo Querzoni

Nino Vincenzo Verde

with the support of

Gabriella Caramagno

Elizabeth Lee

Casa Editrice Università La Sapienza
Piazzale Aldo Moro, 5 - 00185 Roma

www.editricesapienza.it
editrice.sapienza@uniroma1.it

ISBN 978-88-98533-13-8

Iscrizione Registro Operatori Comunicazione n°11420

Finito di stampare nel mese di novembre 2013 presso

Centro Stampa Università
Università degli Studi di Roma La Sapienza
Piazzale Aldo Moro 5 – 00185 Roma

www.editricesapienza.it

Preface

Every economy of an advanced nation relies on information systems and interconnected networks, thus in order to ensure the prosperity of a nation, making cyberspace a secure place becomes as crucial as securing society from the presence of criminal bands. Cyber security means ensuring the safety of this cyberspace from threats which can take different forms. Stealing secret information from national companies and government institutions, attacking infrastructure vital for the functioning of the nation or attacking the privacy of the single citizen can all be seen as extreme examples of a large spectrum of threats. Additionally, perpetrators of attacks on cyberspace are now professionals working for governments, hacktivist organizations or criminal bands rather than teenagers looking for some short-term celebrity as it was in the old days. Intelligence operations are conducted through cyberspace in order to study the weaknesses of a nation and, to complete the picture, in the military domain cyberspace is now seen as one of the dimensions of the battlefield just like space, sea, ground and air. Understanding the complexity of the picture of making cyberspace a safe place turns out to be a problem which is not only technical but rather a social, legal and economic one. Improving cyber security knowledge, skills and capability of a nation will be essential for supporting an open society and for protecting its vital infrastructures such as telecommunication networks, power grid networks, industries, financial infrastructures etc.

This report gives a break down of the Italian standpoint in the context of the protection of national critical infrastructure and other sensitive sectors from cyber attacks from the legal and technological viewpoints. In particular Chapter 1 discusses the notion of critical infrastructures and cyber security in the US and the EU. It goes on to discuss the evolution and the number of cyber attacks sector by sector reported in the world and in Italy and to provide some numbers related to the cost of cyber crime in Italy. In Chapter 2 the Italian scenario is introduced in terms of the legislative landscape and of regulatory changes in the last decade. The chapter then analyzes the current situation of the Computer Emergency Response Teams (CERT) present in Italy. Chapter 3 gives an overview, from both a legislative and operational perspective, of the level of maturity of some developed countries (namely, France, the UK, Germany and the USA) in protecting their critical infrastructure and other sensitive economic sectors. From this comparison, it seems Italy lags behind other developed countries in terms of implementation of cyber security strategy. Italy still lacks a clear operational directive for the creation of a national CERT which makes difficult, on one hand, assessing the exposure of Italy to cyber attacks and, on the other hand, quick and coordinated deployment of countermeasures, in particular, when advanced persistent threats are discovered.

In order to conduct a deep analysis of the Italian cyber security situation, an anonymous questionnaire was sent to the four main sectors of the Italian economy i.e. public administration, utilities, large industries - sensitive to intellectual property theft - and the financial sector. Chapter 4 discusses the results of this exercise. Among other observations, the study points out that some sectors are not fully aware of being a sensitive sector for cyber attack and that a breach in its information system could cause an economic/technical problem at national or EU level, that the defense measures (already employed) neglect advanced persistent threats, but that organizations have, on average, good recovery capability. The report also proposes a cyber security readiness index which is computed through four indexes, namely the awareness index, the policy index, the defense index and the external independence index. Each of these indexes is computed by aggregating several answers to the questions proposed in the questionnaire. Results are reported in a radar chart showing cyber security readiness proportional to the area covered by the radar chart. According to the results, the utility sector exhibits better readiness than other sectors while the public administration sector has definitely got the smallest readiness index. Considering the results of the questionnaire, the experiences of other countries and the Italian legislative landscape, Chapter 5 presents a set of recommendations for a national cyber security strategy. These recommendations span all the phases of the risk management process. In this preface it is worthwhile highlighting that the following are considered priorities: the realization of a national CERT (with a clear role and mission), cooperation among operators in the same sector and with the best sectors of academia, the conceivability of a national cyber security agency that embeds necessary capabilities and skills for an efficient strategy implementation and a nationwide methodology for classifying threats and adapt the dimension of the response. The interested reader can go through the complete recommendation list for details.

Securing the national cyberspace and protecting the critical infrastructure can also be seen as a giant national economic opportunity for growth in terms of industrial capability and research. At the time of writing, Italy has a very good worldwide standing in the cyber security sector with the presence of key sector players, high-tech small-medium enterprises and highly reputed research centers. This makes Italy a breeding ground for cyber security initiatives that could be a source of employment for the current and next generations. All other developed countries are investing huge amount of resources in this sector to make their cyberspace a safe place for their citizens to visit and for businesses to operate whilst Italy is investing zero resources. Considering the pervasiveness of cyberspace and its relevance in any form of economy for the present and the future, the security that a nation will be able to provide for its cyberspace will be a measure of its independence, of its economic strength and of its capability to maintain its wealth for the following generations. This is why in the future the study will, hopefully, be extended to small-to-medium sized businesses, that are the heart of Italian economy, to assess their awareness of the cyber threats that can steal their intangible assets.

Let me finally thank all the authors of this report, Gabriella Caramagno, Elizabeth Lee, Reto Haeni, Carlo Iantorno, Luisa Franchina, Pier Luigi Dal Pino, Marina Brogi, Luigi Vincenzo Mancini, Fabrizio d'Amore, Giuseppe Ateniese and the Italian Presidency of the Council of Ministers. We are expecially grateful to the respondents to the questionnaire. We really hope that this report will help us in gaining trust in order to increase the number of respondents for the next editions. The work has been partially supported by the MIUR PRIN TENACE project and by Microsoft.

Roberto Baldoni
Cyber Intelligence and Information Security
Research Center Director
Università degli Studi di Roma La Sapienza

Rome, 15 November 2013

Contents

List of Figures

List of Tables

List of Boxes

List of recommendations

CHAPTER

1 Critical Infrastructures, Sensitive Organizations and Cyber Threats

In order to understand how Italy is facing the delicate issue of critical cyber infrastructure in terms of governance, it is necessary to briefly examine the definition of the scope of the analysis, i.e. what critical infrastructures are, which organizations can be considered sensitive due to their role in society and what cyber security is: the combination of these concepts allows for the identification of the economic sectors that are sensitive to cyber attacks. With reference to the critical infrastructure (CI), despite the numerous attempts made, there is still no universally recognized definition, or at least a definition that provides a classification suiting the characteristics of each nation. It is often identified as the infrastructures whose incorrect functioning, even for a limited time period, may negatively affect the economy of individual subjects or groups, involving economic losses and/or even expose people and things to a safety and security risk [6]. Box I reports the definitions of critical infrastructure that can be found in US and EU formal documents.

Even though there is some difference, in essence both the above definitions look at identifying potential threats like human error, occasional accidents, terrorist attacks that can lead to a malfunction or onset of the crisis of the CI under observation. Moreover, the European Commission highlights that if an accident occurred in a member state, it could have an impact on other states, as a result of increased interdependencies between infrastructures relating to various member states. These infrastructures are, thus, considered European Critical Infrastructures (ECI). The designation to ECI is the result of a complex technical-political process that arises from the potential impact that can be caused by a failure and/or destruction of an infrastructure in terms of sectoral and inter-sectoral relevance. The inter-sectoral evaluation criteria relate to:

a) potential victims, in terms of number of fatalities or injuries;

b) potential economic effects, in terms of financial losses, deterioration of products or services and environmental effects/damages;

c) potential effects on population, in terms of loss of public confidence, physical suffering and disruption of daily life, including the loss of essential services.

Briefly, EU directive 114/2008 lays down rules for the owners and/or operators concerning the security of their infrastructure to prevent, or at least mitigate, consequences on other nations. In other words, given the pan-European role played by such large infrastructure, security levels must conform to a high qualitative standard and, thus, the rules to be adopted are not defined only by the member state in which an infrastructure is located but, to some extent, they are imposed at European level.

An essential component of the European Programme for Critical Infrastructure Protection (EPCIP)[1] is the Critical Infrastructure Warning Information Network (CIWIN), a protected public Internet-based information and communication system that allows subjects involved in Critical Infrastructure Protection (CIP) to share CIP-related information and good practices (Box II reports the first initiatives in this field).
In Italy, according to the Working Group on CIP(Gruppo di Lavoro sulla Protezione delle Infrastrutture Critiche) established by the Department of Innovation and Technology (Dipartimento per l'innovazione e le tecnologie) within the Presidency of the Council of Ministers, critical infrastructure is identified as:

[1] EPCIP is the 2004 European program dedicated to the identification and protection of ECI.

Definition of critical infrastructure in the United States

The term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters [45].

As early as 1998, US legislation had revealed that ownership/management of critical infrastructure is mostly private. It is a complex system that synergistically produces and distributes a continuous flow of essential goods and services [43].

Definition of critical infrastructure in the European Union

1. Critical Infrastructure (CI) means an asset, system or part thereof located in member states which is essential for the maintenance of vital society functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a member state as a result of the failure to maintain those functions.
2. European Critical Infrastructure (ECI) means critical infrastructure located in member states to which the disruption or destruction would have a significant impact on at least two member states. The significance of the impact will be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure [20].

Box I: Some definitions of Critical Infrastructure.

The United States was the first, in 1996, to perceive the importance of the issue of CIP, beginning a series of analysis and studies that took shape in 1998 with President Clinton issuing Presidential Decision Directives 62 and 63.

At the European level, only in June 2004 did the European Council call for a comprehensive strategy for the protection of critical infrastructure and in October of the same year, the European Commission proposed measures to strengthen the European Union's (EU) prevention, preparedness and response to terrorist attacks on critical infrastructure, with a series of proposals to enhance prevention, preparedness and response to terrorist attacks [14].

Box II: The first measures in the field of CIP.

> "the combination of networks and systems including industry, institutions, and distribution facilities that operate in synergy and produce a continuous flow of essential goods and services for the organization, functionality and economic stability of a modern industrialized country, whose destruction or temporary unavailability can cause a debilitating impact on the economy, daily life or the ability of a country to defend itself"[32].

This definition highlights the systemic and network aspect of critical infrastructure, emphasizing that the criticality is not so much in the value of the single component, but rather in its systemic relevance.

Focusing on the concept of network and systemic nature to define critical infrastructure, the presence of interdependencies is relevant. On the one hand, the phenomenon of integration brings benefits in terms of efficiency, quality of service and cost reduction, but on the other hand, it determines an intrinsic vulnerability and new types and forms of threats. It is possible to analyze the interdependencies by considering six different dimensions[39]:

1. *Environment:* it is influenced by the operating state and condition of each infrastructure, and it in turn exerts pressures on the individual infrastructures.
2. *Types of interdependencies:* we can define the following four principal classes of interdependencies: physical, cyber, geographic, and logical. Two infrastructures are physically interdependent if the state of each one is dependent on the material output of the other. An infrastructure has a cyber interdependency if its state depends on information transmitted through cyberspace. Infrastructures are geographically interdependent if a local environmental event can determine changes in their state. Finally,

two infrastructures are logically interdependent if the state of each one depends on the state of the other via a mechanism that is not a physical, cyber, or geographic connection.

3. *State of operation:* the state of operation of an infrastructure has to be considered as a continuum that exhibits different behaviors during normal operating conditions, during times of disruption, or during times when repair activities are under way.
4. *Infrastructure characteristics*.
5. *Type of failures:* interdependencies could increase the risk of failure or disruption in infrastructures.
6. *Degree of coupling:* the propagation time and the transmitted intensity of a possible malfunction vary in function of the degree of coupling.

Information systems are fundamental to the organizational structure and the mechanisms of operation of business, industry and government institutions. However, such systems, especially with reference to critical infrastructure, are vulnerable to growing violations due to interconnectivity [22]. Types of interdependence among infrastructures became more important, so increasing the cyber risk exposure for the private sector and the public sector in a national and an international context. The importance of cyber risk is due to its potential disastrous effects, especially when you consider that one criteria defining the critical infrastructure is the analysis of the impact of any damage to the same infrastructure. It is worth pointing out that only some of the damage resulting from a cyber risk can be evaluated in economic terms (production losses, damage to property, theft of cash, etc.), while others are less obvious [7].

Interference with information systems could result in loss of consumer and shareholders' confidence, resulting in a negative reputation and, therefore, in value destruction [5]. If attention is focused on the aspects associated with the presence of cyberspace relating to CIP, it is referred to as Critical Information Infrastructure Protection (CIIP). The boundary between CIP and CIIP is very weak, because of the tight inter-relationships between the physical world and the virtual world. Literature often considers the two terms as interchangeable, and some authors have suggested the use of the acronym CI(I)P. Considering the peculiar traits due to the digital domain, the cyber threat for CIIP in the cyberspace domain raises urgent and complex challenges in the field of protection and security.

Box III provides definitions of cyberspace and cyber security. It can be seen as the notion of cyber security includes (but it is not limited to) critical infrastructure protection from cyber attacks. Cyber security includes also the protection of other economic sectors that are sensitive to cyber attacks.

Cyberspace

Cyberspace is a set of interconnected computing infrastructures, including hardware, software, data and users as well as the logical relationships between them. It includes, among other things, the Internet, communication networks, process actuators systems and mobile devices equipped with a network connection.

Cyber Security

Cyber security is the condition in which cyberspace is protected with respect to voluntary or accidental events, consisting in the acquisition and transfer of data, in their modification or unlawful destruction or the blocking of information systems, thanks to appropriate security measures. These measures include safety audits, management of security updates (patches), authentication procedures, access management, risk analysis, detection and response to incidents/attacks, mitigation of impacts, recovery of components subject to attack, training and education the personal, and verification and enhancement of the physical security of the premises where information and communication systems are placed.

Box III: Cyberspace and cyber security definitions [31].

It is important to understand the differences among the following expressions: cyber security, cyber crime and cyber terrorism. Cyber crime is identified as the set of offenses ranging from identity theft to scams via Internet banking and cyber ransom. Therefore, cyber crime concerns the civil area. Cyber terrorism concerns the military area: it consists, in fact, in the set of actions that organizations or groups accomplish in cyberspace for subversive purposes. For both areas, civil and military, cyber security is critical. Cyber security is "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets" [51]. This sector is characterized by an evolving and not fully completed regulatory framework and a complexity coming from the combination of Information and Communication Technology (ICT) with other systems essential to the sustainability of the key features of modern societies. Therefore, cyber security is a very interesting issue for both academics and professionals [1, 9, 40]. In Europe two main priorities have been identified:

1. protection of infrastructures based on ICT identified as critical infrastructure;
2. protection from cyber crime.

In 2009, the European Commission outlined a plan of immediate action to strengthen the security and resilience[2] of Critical Information Infrastructures (CIIs). The activities of this plan are carried out within and in parallel with the EPCIP program, concerning the critical infrastructure protection. The action plan is organized in five pillars (see table 1.1, first column). In 2011, the European Commission published the results achieved following the implementation of the action plan for the protection of CII, in each of the five areas. These results are summarized in the table 1.1.

Table 1.1: The five pillars established in Action Plan 2009 with their results.

The five pillars established in Action Plan 2009	**Results achieved (Report 2011)**
Preparedness and prevention: for the definition of common standards and the establishment of adequately prepared national Computer Emergency Response Teams (CERTs).	In 2009, ENISA (European Network and Information Security Agency) and the national CERTs established and approved CERTs minimum skills and services, in order to operate properly in support of pan-European cooperation. In the same year the European Forum of Member States (EFMS) was established to facilitate the communication and exchange of information between authorities of the member states. In addition, the European Commission adopted the European Public-Private Partnership for Resilience (EP3R) to foster cooperation between the public sector and the private sector on security and resilience of ICT systems.
Detection and response: for the adoption of a European Information Sharing and Alert System EISAS.	ENISA developed a roadmap for the development, by 2013, of EISAS.
Mitigation and recovery: for the elaboration of national emergency plans and the organization of national and pan-European exercises on the response and the disaster recovery as a result of security incidents on large-scale networks.	ENISA has developed a good practice guide for exercises at national level and strategic recommendations for the development of national strategies. On November 4, 2010 the first pan-European exercise related to security incidents on communication networks (Cyber Europe 2010) was held.
International cooperation: for promoting European priorities in terms of safety, at the international level and to participate in exercises at the global level.	Principles and European guidelines for the resilience and Internet stability were formulated on the basis of the EFMS' work.
Criteria for European Critical Infrastructure in the ICT sector: for implementing the identification and protection plan of ECI imposed by Directive 114/08.	A first draft of the criteria for identifying European Critical Infrastructure in the ICT sector was produced, with special focus on fixed and mobile communications and the Internet.

More recently (in February 2013), the European Commission published a European strategy for cyber security [16] defining the principles that should guide the EU cyber security policy. Although member states are primarily responsible for security in cyberspace within the national borders, the European strategy proposes actions to improve the overall EU performance. These actions, both short and long term, involve EU organizations, the member states and the private sector. In particular, the EU Strategy is structured into the following five strategic priorities:

[2] The ability of a system to return to its original state after an unexpected event.

1. Achieving cyber resilience. The legislative proposal concerning the European strategy for cyber security plans:
    - To establish common minimum requirements of Network and Information Security (NIS) at the national level by requiring member states to appoint specialist national authorities in the field of NIS, to establish well-functioning national CERTs, and to adopt a NIS strategy and a national cooperation plan. A European CERT (CERT-EU) was established in 2012.
    - To foster cooperation and information sharing between the specialist national authorities, to respond to cyber incidents with an international dimension. EFMS favors communication between the specialist authorities of the member states.
    - To improve the readiness and the involvement of the private sector. The majority of computer systems and telecommunications networks are in the private sector, thus it is essential to improve the involvement of the private sector in the context of cyber security.
2. Drastically reducing cyber crime. Cooperation between the member states is important for responding to the growing threat of cyber crime. The European Cybercrime Centre (EC3), formed in 2013 within Europol, is the European reference point for the fight against cyber crime. EC3 facilitates collaboration and information sharing between the authorities of the member states, the private sector and other stakeholders.
3. Developing cyber defense policy and capabilities related to the Common Security and Defence Policy (CSDP). Cyber defense focused on the detection, response and recovery against cyber threats is essential to increase the resilience of systems in the NIS. In this context, the European strategy involves strengthening the synergy of the civil and military sector for the protection of critical information infrastructures. This effort should be supported by research, development and collaboration between the governments of the member states, the private sector and the academic sector.
4. Developing the industrial and technological resources for cyber security. Many global leaders offering innovative ICT products and services are located outside the EU. The risk for Europe is to depend too much on non-EU ICT and security solutions. Research and development provide the EU with the opportunity to promote a reliable European ICT sector, boost the internal market and reduce Europe's dependence on foreign technology. The European Commission intends to use Horizon 2020 to promote research and development in the field of security and privacy in the ICT sector, and the development of tools to combat criminal and terrorist activities involving cyberspace.
5. Establishing a coherent international cyberspace policy for the European Union and promoting core EU values: the EU strategy is aimed at maintaining an open, free and secure cyberspace. The European Commission intends to develop a coherent international policy in the field of cyberspace aimed at increasing engagement with key partners and key international organizations and improve the coordination, promoting the fundamental values of the EU. This policy encourages the efforts for the development of standards of behavior and enforcement of international laws in cyberspace. It also promotes the Budapest Convention to combat cyber crime.

1.1 Critical infrastructures and sensitive organizations subject to cyber attacks

In 2006, the European Commission defined network and information security as "the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems" [12]. CII is thus crucial both because it is critical itself and because it serves other critical infrastructure as well. CIP includes "the programs and activities of infrastructure owners, operators, manufacturers, users, and regulatory authorities which aim at keeping the performance of critical information infrastructures in case of failures, attacks or accidents above a defined minimum level of services and aim at minimizing the recovery time and damage"[12]. As regards cyber crime, there is still no single definition, mainly because of the differences in the legislation of the various member states. The European Commission, in a communication of 2007 [13], said, in general, that it includes "the criminal acts committed against electronic communications networks and information systems or by means of such networks and systems".

Over the years, governments have drafted lists identifying the areas in which critical infrastructure operates. Table 1.2 shows the sectors pointed out as critical by the US government, in the recent Presidential Policy Directive 21 [44], and the European Commission, as stated in the proposal, Directive on European Critical Infrastructure in 2006 [11].

Table 1.2: Economic sectors of critical infrastructure.

Critical Sectors - American Government	**Critical Sectors - European Commission Proposal**
Food And Agriculture	Food
Water and Wastewater Systems	Water
Dams	Research Facilities
Healthcare and Public Health	Health
Nuclear Reactors, Materials and Waste	Nuclear Industry
Emergency Services	Space
Information Technology	Information, Communication Technology (ICT)
Energy	Energy*
Transportation systems	Transport*
Financial Services	Financial
Chemical	Chemical Industry
Communications	
Defence Industrial Base	
Commercial Facilities	
Critical Manufacturing	
Government Facilities	

*Critical sectors that have transitioned in the final version of the European Commission Directive [20].

Direct correspondences exist between some American and European critical areas, e.g. the financial services and the energy sector. The banking and financial services play a vital role in the economy of each country, so that a violation would be a huge risk for the entire system (see Box IV). Also the energy sector is critical. Electrical energy has various features, including the ease of conversion into other forms of energy (mechanical, light, thermal, etc.), the ease and flexibility of transport, the possibility of a widespread distribution and, at the same time, it is storable, only in limited quantities. This means that, at any time, the demand must be balanced by the production of energy. The need to use ICT technologies exposes the mentioned areas to the risk of computer breaches. The American and European classifications of critical sectors show, also, some differences. First, the list provided by the US government is more detailed, for example, it pays attention to activities concerning public services, such as heritage preservation, emergency services, government activities. Moreover, agriculture is considered a critical sector. This is due to the fundamental mission that the government attaches to this sector: the ability to provide safe and nutritious food, hence the need to protect it from possible attacks, which would represent a serious threat to public health, safety, welfare, and thus the national economy. The European ICT sector may correspond to the union of the two critical areas of American information technology and communications. Another difference concerns the water sector identified by the European Commission which should correspond to the union of the two sectors water and dams listed by the US government. Finally, in the European list there are two separate entries, space and research facilities, which do not have a direct correspondence in the US list, although the former may fall within the communications sector and the second may fall in government facilities. The EU directive proposal constitutes a first milestone in a step-by-step approach to identify and designate ECIs and assess that need to improve their protection. As such, the final version of this Directive [20] solely concentrates on the energy and transport sectors, paving the way to future reviews in order to include other sectors within its scope.

In the financial sector, operational risk has wide-ranging systemic implications given the increasingly large size, interconnectedness, and complexity of financial institutions which increase the possibility of errors and fraud. Disruptions to the flow of financial services because of impairment of all or part of the financial system may give rise to systemic risk and possible spillover effects to the real economy. The magnitude of such disruptions depends on asymmetric information and network externalities. System and process failures are particularly dangerous if they occur in the clearing and settling of financial transactions as well as in the trading and pricing of financial instruments. Financial Market Infrastructures (FMIs) which facilitate the clearing, settlement, and recording of monetary and other financial transactions can strengthen the markets they serve and play a critical role in fostering financial stability. However, if not properly managed, they can pose significant risks to the financial system and be a potential source of contagion, particularly in periods of market stress. An FMI is defined as a multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions ("Principles for financial market infrastructures", BIS and OICV-IOSCO, April 2012). Financial institutions in general are connected directly and indirectly to their customers, to other financial institutions, and to their service and utility providers; accordingly, operational risk may be imported from connected entities. The fallout from the recent financial crisis has illustrated that many sources of systemic risk were triggered or at least propagated by vulnerabilities in operational risk management of market and payment infrastructures. As a consequence, global leaders recognized a greater role of operational risk. The policy resolutions of the Group of Twenty (G-20) Summit in Pittsburgh, Pennsylvania, in September 2009 mark a shift of financial sector regulation from internal controls and sound risk management practices to macro prudential regulation for systemic risk and contingency planning. For banking supervisors, operational risk is inherent in all banking products, activities, processes, and systems, and the effective management of operational risk has always been a fundamental element of a bank's risk management program. In order to implement in our system the EBA's Guidelines on Internal Governance (27 September 2011), the circular no. 263 - New regulations for the prudential supervision of banks was emended in July 2013 (15th amendment). Among others, the most important innovations are related to:

- The discipline of information systems, taking into account the main developments which emerged on the international scene and setting the main constituents of governance and organization of the information system, IT risk management, all the requirements to ensure the security and the system management of data. The provisions also provide that the definition of principals security for access to critical systems and services through the Internet channel are applicable Recommendations of the ECB in the field of security of online payments.
- The Business continuity discipline, by reorganizing provisions presently contained in different regulation sources. Among others a process of rapid escalation by accident in emergency was defined so as to ensure that the declaration of a state of crisis happened in the shortest possible time from the detection the accident. The total time for recovery will not exceed four hours, including times for the stages of analysis , decision-making , technical assistance and verification.
- The formalization of the role of the CODISE Working Group (the business continuity working group set up in 2002) as the structure responsible for the coordination of crisis management operating in the Italian financial system. The group is coordinated by the Banca d'Italia in agreement with the CONSOB (the Italian stock exchange commission) and consists of representatives of the leading banking groups and the companies that manage infrastructures essential to the orderly working of the financial system.

The problem of cyber threat in the financial sector has been investigated in [3] and [2] where a complex event processing infrastructure supporting an information sharing system has been introduced to face cyber attacks and frauds happening at distinct organizations.

Box IV: Vulnerabilities, threats and operational risks in financial systems.

1.2 Italian critical IT infrastructure

In Italy, attacks on computer security have had an exponential growth in recent years. Assinform[3] estimated that 40% of attacks require at least 4 days to be solved. In 90% of cases the attack is successful due to incorrect configuration of the security system and the lack of specific skills. The costs incurred by the private sector and the government to protect themselves are high: Gartner[4] quantifies them at $55 billion in 2011, $60 billion in 2012 and an expected $86 billion in 2016. These data show the increased importance of cyber security, as evidenced by the annual reports of the "Sistema di Informazione per la Sicurezza della Repubblica"[5]. The 2010 report is very important because for the first time cyber security was included in the category of Growing Challenges and deemed a matter of national security [27]. Moreover, the 2012 report highlights that the threat landscape is changing, also regarding the use of advanced technologies, "able to have a profound effect on the continuity of functions and vital interests of the country...". From here, the role of information policy for security is an essential component of the safeguarding of main national interests.

In January 2008, the Minister for the Interior issued a decree on"the identification of critical IT infrastructure of national interest" [28], which in art. 1 states:

"The critical information infrastructures of national interest are the systems and computer services supporting the institutional functions of:

a) *Ministries, agencies and supervised authorities, operating in the fields of international relations, security, justice, defence, finance, communications, transport, energy, environment, health;*

b) *Bank of Italy and independent authorities;*

c) *State-owned companies, regions and metropolitan areas covering at least 500,000 people, operating in the fields of communications, transport, energy, health and water conservation;*

d) *Any other institution, administrative office, authority, public or private legal person whose business is considered of national interest because of public order or security, by the Minister for the Interior or at the proposal of the prefects - provincial authorities, public security".*

1.3 Critical economic sectors targeted by this report

This report considers the below list of economic sectors sensitive to cyber threats that include the ones in the EU directive n.124 [20] (European Critical Infrastructure) and the ones in a decree issued by the Italian Ministry for the Interior Decree n.101 of 2008[28]. Additionally, following a recent trend that considers the defense of the intellectual property of national industries as a priority for the economy of the nation, we put in the list the industries that are subject to intellectual property theft.

- plants and energy networks, e.g. power plants, oil and gas plants, depots and refineries, transmission and distribution systems;
- communication systems and information technology and computer networks, e.g. telecommunications, broadcasting services, software, hardware and networks, including the Internet;
- the financial system: banks; financial infrastructures that facilitate the clearing, settlement and recording of monetary and other financial transactions; financial institutions directly connected with their customers, to other financial institution and to their service and utility providers;
- the health care system, e.g. hospitals, pharmaceutical industry, rescue and emergency;
- food supply (food industry, hygiene safety systems, manufacturing and wholesale distribution);
- water supply, e.g. reservoirs, storage and treatment of water supplies;
- transportation;

[3] Assinform is the National Association of Leading Information Technology Companies operating in Italy.

[4] Gartner is a world leader in consulting and research in the field of information technology.

[5] The "Sistema di Informazione per la Sicurezza della Repubblica" is the set of institutions and national agencies responsible for intelligence activities `http://www.sicurezzanazionale.gov.it`.

- the production, storage and transportation of hazardous substances, such as chemical or biological materials;
- the delivery of public services (facilities, information networks, cultural and natural heritage);
- high-tech industry subject to intellectual property theft.

1.4 The cyber threat: current situation and future trends

The critical infrastructure of every country, ranging from oil pipelines to the electricity grid, from gas to water, from transportation, to financial/banking systems, to public services, is increasingly electronically managed. The progressive introduction of network, monitoring and control systems, as well as the interdependence that has arisen, has certainly improved the performance level of such infrastructure, but it has also allowed access to cyber criminals, with consequent cyber attacks and the increasing risk of a domino effect.

Therefore, the scenario has became more and more complex in recent years, as the introduction of advanced technology added new sources of potential risk alongside the traditional threats. An effective infrastructure protection includes threat identification, vulnerability reduction and attack source identification. This activity aims at service downtime minimization and damage limitation.

The expression cyber threat denotes the set of behaviors that can be carried out in and through cyberspace. It consists in cyber attacks: actions of individuals, states or organizations, aimed at destroying, damaging or interfering with the proper functioning of the systems and networks and/or systems actuators process controlled by them, or violating integrity and confidentiality of data/information. Depending on the actors and purposes, we have:

- cyber crime: all the activities with criminal purposes (such as, for example, fraud or wire fraud, identity theft, the misappropriation of information or creative and intellectual property);
- cyber espionage: wrongful acquisition of sensitive property or classified data or information;
- cyber terrorism: the set of ideologically motivated actions, aimed at influencing a country or an international organization.

This categorization has a merely descriptive value, it being understood that the contraindicated action has often no peculiar characterization: an intrusion into a computer system, for example, can be instrumental in data theft for profit intent (criminal matrix), espionage or terrorism and even, in activities of so called hacktivism or cyber agitation (the use of computers and related systems, with or without the use of techniques of hacking as a form of ideologically motivated protest).

Box V: Cyber threat definition [31].

Typically, a cyber attack is launched:

1. to paralyze the critical infrastructure activities;
2. to steal infrastructure information assets.

It is important to evaluate the possible targets so as to assess the consequences, also in terms of time required to restore normal behavior (resilience). Cyber threats are important challenges for the country, because they involve both the digital domain and because of their transnational nature. Cyber threats are not easy to counter: the actors, means, objectives and attack techniques vary continuously (see Box V). Moreover, the attacks may have different origins:

- cyber crime;
- cyber terrorism;
- cyber espionage.

These attacks may even cause a cyber war, a real conflict between nations fought trying to paralyze their vital sectors. It is clear that when the attacks target critical infrastructure and warning systems the consequences for the entire society could be disastrous. In light of the above and of the awareness that this is a continuously changing environment, it is urgent to intervene, at the national level and beyond, against all cyber crime forms, which represent a growing threat to critical infrastructure, society, business and citizens. However, it is rather complex to detect the size of the phenomenon, partly because the operators are reluctant to give exact figures on the number of attacks suffered. In 2012, according to the Verizon 2013 Data Breach Investigations Report[52], various sectors were hit by cyber attacks: 37% of the violations were against financial institutions, 24% against retailers and restaurants, and 20% against industry, transport and utilities, and the remaining percentage were violations against professional and information services. Different percentages are provided by Clusit Report 2013 [8] (see Table 1.3), which analyzed 1.183 attacks that took place in 2012. The only data remarked in all reports is that it is a growing phenomenon.

Table 1.3: Evolution of number of attacks by sector (source: Clusit, 2013).

Sector	**2011**	**2012**	**Total**	**Delta**
Mil, LEAs, Intelligence	153	374	527	144%
Others	97	194	291	100%
Entertainment/news	76	175	251	130%
Online services/cloud	15	136	151	807%
Research/Education	26	104	130	300%
Banking/Finance	17	59	76	247%
Softw./Hardw. Vendor	27	59	86	119%
Telco	11	19	30	73%
Contractors/consulting	18	15	33	-17%
Security industry	17	14	31	-18%
Religion	0	14	14	100%
Health	10	11	21	10%
Chemical/Medical	2	9	11	350%
Total	469	1183	1652	152%

Since 2009 the number of criminal and terrorist actions against energy corporations has nearly doubled. A recent survey [54] conducted by Carnegie Mellon University CyLab and promoted in Italy by AIIC (Association of Italian Experts in Critical Infrastructure) revealed that of 108 companies worldwide, organizations in the financial sector are equipped with the best practices in the field of cyber security and risk management, while companies in the energy and utilities sector have the worst. Despite more than 90% of organizations adopting risk management, only 33% have the intention to manage security in terms of information risk, 29% showed interest in IT operations and only 13% intend to target the suppliers of software and other services.

As far as Italy is concerned, according to Clusit data [8], in 2012 the government sector was the most attacked sector immediately followed by political organizations and industry (see Figure 1.1).

The Verizon report also revealed that, in 2012, the greatest number of cyber attacks were for economic reasons: 75% of attacks were financial cyber crimes, followed by government espionage campaigns, aimed, primarily, at the theft of intellectual property (government information, trade secrets and technical resources), which determined 20% of cyber threats. In particular, espionage attacks are not confined to government agencies and military departments but include production companies, IT and professional organizations.

Considering the methods of attack, the most popular was hacking, which featured in more than half (52%) of data breaches. Analyzing a sample of Italian cyber attacks, Clusit highlights [8] that in 2012 attacks motivated by cyber crime grew more than those related to hacktivism activities (see figure 1.2); despite this, attacks due to hacktivists still remain the most substantial portion (67%) of the total.

With regard to types of cyber threats, the McAfee annual report, 2013 Threats Prediction, revealed that mobile devices are already, and will be even more so, in the crosshairs of cyber crime. The influence of the Anonymous group should decrease, while large-scale attacks against critical infrastructure will probably increase. The trend is fueled by the changing technological landscape: smartphones and tablets are becoming very important for every type of service [6].

[6] Norton (2012) reveals that, compared to 2011, cases directly related to social networks and mobile devices are on the rise, affecting about 21% of the sample of respondents (about 13,000 adults aged between 18 and 64 years in 24 countries).

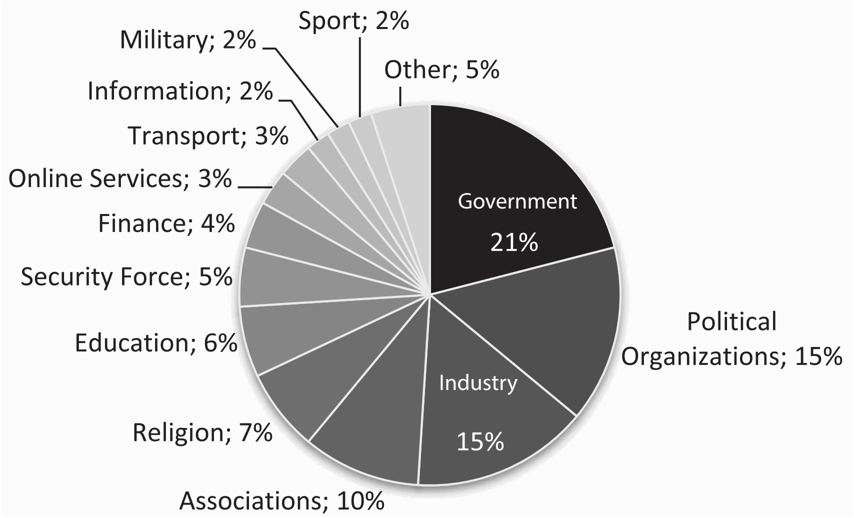


Figure 1.1: Breakdown of number of attacks (percentage on 129 attacks analyzed) by sector in Italy (source: Clusit, 2012).

On the front of cyber crime, according to data from Symantec [41], in 2012 Italy was ranked ninth globally for the spread of malware and occupies the first place in Europe (and fourth place in the world) for its number of infected PCs controlled by hackers (so-called botnets).

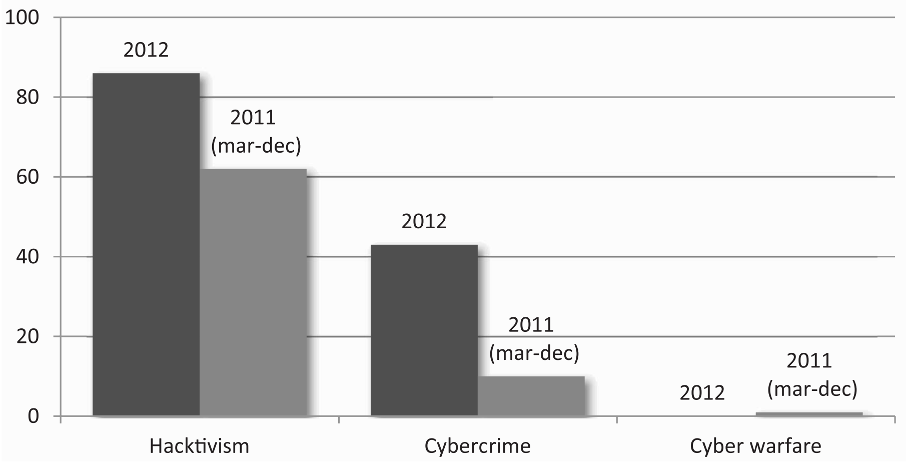


Figure 1.2: Evolution of cyber threat origins in Italy (source: Clusit, 2013).

Even if the percentage of people connected to the Internet in Italy with at least one device [25] is smaller than other EU countries (see figure 1.3), in the last year the number of people connected to the Internet (aged between 11 and 74 years old) has reached about 33 millions (+ 8,3% on a yearly basis).

The number of people actively connected to the Internet has also increased consistently on a daily basis (+13.2%), passing from 12 million in 2011 to 14.8 million in 2012. Furthermore, the number of older people using social networks recorded an increase (see figure 1.4) as did the intensity of usage [25]. Specifically, the average time spent by Italians on social networks is equal to about one third of total online time during the month (6 hours out of 19).

In general, however, the development of apps and online services will bring more security threats, because, thanks to online services, users perform many more operations directly from their device. Under attack is, therefore, the general public, public services, and business - especially the financial sector.

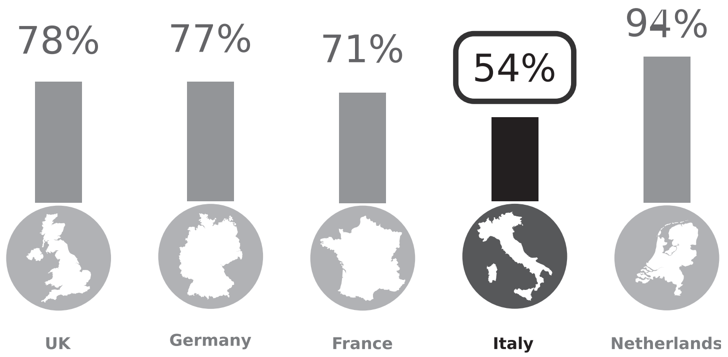


Figure 1.3: People networked with at least one device (source: Audiweb, 2012).

Table 1.4: Devices used by Italians to stay connected (source: Audiweb, 2012).

Device	**Percentage**
Computer	73%
Smartphone	31%
Tablet	4%
Connected TV	5%
Videogame Console	8%

The main cause of the spread of attacks is the limited use of threat protection solutions. Only 33% of Italian users (the percentage rises to 44% on a global scale) actually uses software able to ensure the necessary security of their data and only 45% of Italian users employ privacy settings to control the information they share with their contacts. In addition, 44% of users in Italy (about 40% in the world) do not use complex passwords or change their keywords frequently. The number of criminal activities and the level of sophistication of attacks do not correspond to a proportional growth of attention.

Despite the large and increasing use of the Internet among Italians, there is still a low level of awareness of the risks associated with careless use of the Internet. Consequently people buy products and services which are inherently insecure, or implement and configure in an insecure manner, without any guarantee or protection. As reported in figure 1.5, the main consequence [34] in Italy is that about 44% of PCs are attacked by malware while browsing the Internet, compared with 20% in Denmark [33].

Furthermore, the question of the direct costs generated by the activities of cyber criminals is very important. The Norton Cybercrime Report 2012 found costs between 2011 and 2012, of about $110 billion globally and just under 2.5 billion euro at the Italian level, relating, respectively, to the number of victims of 556 million and 8.9 million. A study conducted by ABI Research estimated that global spending on security will increase to $1.8 billion by 2018, partly as a result of the intensification of electronic defenses with new Internet security solutions related to data center systems and control procedures (see Section 1.5).

In the light of the data provided and given its strength and spread, the cyber threat could be fought on two levels. On the one hand, it is necessary to enhance international cooperation and create shared terminology, rules and practices in order to respond to any attacks made on a large scale. On the other hand, it is necessary to build a national strategic framework for cyber security.

In this direction, in Europe, the following two most urgent objectives have been identified: to increase the awareness of key risks related to cyber security and to improve European and national preparedness and response capabilities to cyber attacks or incidents. Both with respect to the first objective and with reference to European initiatives against cyber crime, the European Commission will support dialogue between the member states and between them and the European Community institutions, as well as between the key players in the public and private sector. For this purpose, ad hoc structures have been created, e.g. the aforemen-

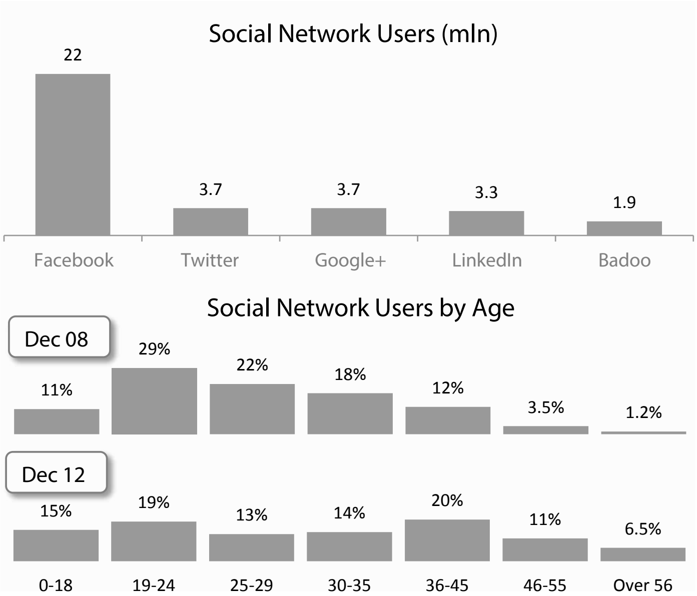


Figure 1.4: Italy and social networks (source: Audiweb, 2012).

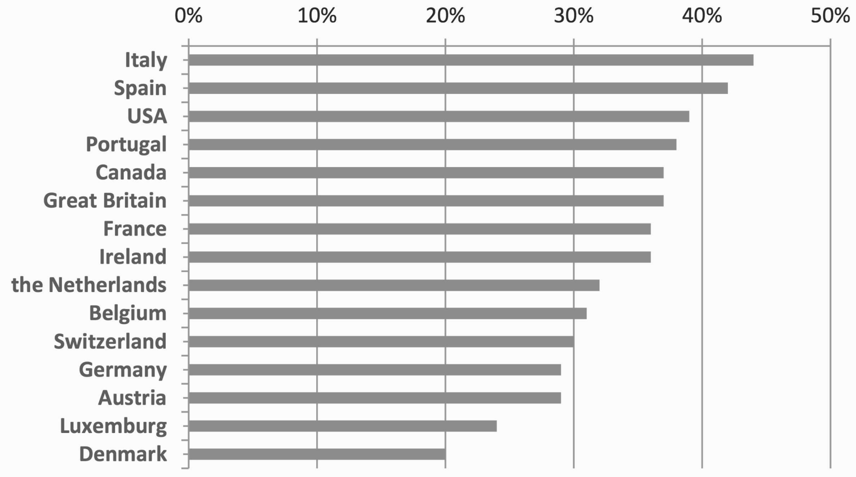


Figure 1.5: Percentage of personal computer attacked by malware while browsing the Internet (source: Kaspersky Lab, 2012).

tioned ENISA, the European Agency for Network Security and Information and Europol, the European Police Office, which oversees the European Platform for Cyber crime, whose function it is to facilitate the collection, exchange and analysis of information on cyber crimes among the member states. With regard to operational aspects, the reaction to attacks or cyber incidents varies considerably between EU member states. Efforts to bridge the gap between the most and least equipped focus on the dissemination of skills and training, but also on the creation, in each member state, of CERTs. As stated above, these and other structures will be discussed in more detail in the next sections.

1.5 The cost of cybercrime in Italy

Currently there are no official statistics on the cost of cybercrime in Italy. The only available statistics come from the private sector. According to the Norton Cybercrime Report [37] (September 2012), which analyzes the impact of cyber crime on consumer users, the total net cost of consumer cyber crime in Italy in the previous 12 months amounts to 2.45 billion euros, whereas the cost at global level amounts to $110 billion (about 85 billion euros). The report estimates the number of cyber crime victims to be 8.9 million people, about one third of Internet users active in Italy in 2012 [8]. This results in an average cost per person of 275 euros (more than the global average cost per person, estimated to be 197 US dollars). In particular, Norton registers an increasing number of victims among mobile and social network users, suggesting that cyber crime is evolving towards new technologies. Indeed, approximately 17% of adults in Italy have been victim of social or mobile cyber crime in 2012, and about 10% of social network users have had someone hack into their profile.

In the business context, an analysis led by the Ponemon Institute[38] estimates the cost of data breach in Italy, in terms of direct, indirect and opportunity costs incurred by an organization in response to data breach. The analysis, conducted in 2011 and published in March 2012, reports the average cost of data breach per record (i.e. the total cost divided by the number of compromised records) and the average total organizational cost of data breach. As shown in figure 1.6, the average cost per record incurred by Italian organizations is 78 euros. This cost accounts for a range of business costs: detection (26 euros), notification (3 euros), ex-post response (22 euros) and lost business (27 euros). The majority of the total cost (41 euros) is due to indirect costs, while the remaining part (37 euros) is due to direct costs.

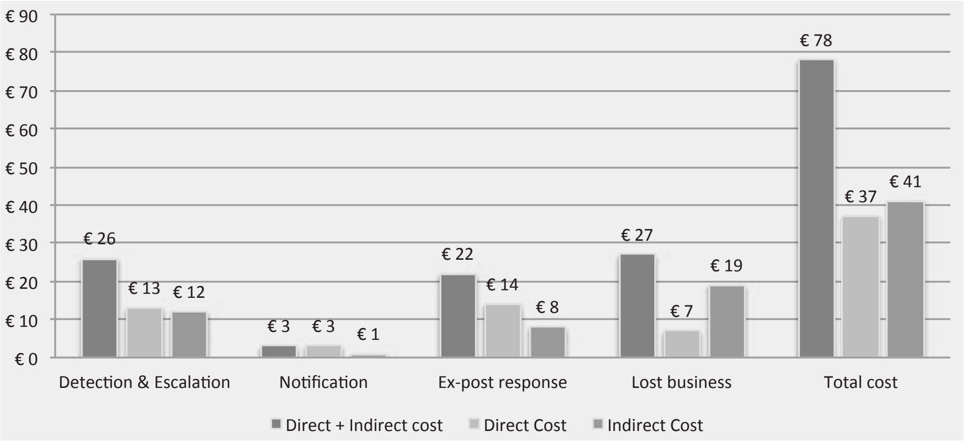


Figure 1.6: Average cost of data breach per record (source: Ponemon Institute, 2011).

Figure 1.7 shows the average total organizational cost of a data breach (1,384,798 euros) and its constituent costs. Both figures show that the largest cost is represented by lost business. This cost is mainly due to abnormal turnover in customers (a higher than average loss of customers for the organization) and reputation loss. Indeed, customers often abandon the organization after a data breach. The analysis also revealed that the primary cause of data breach is negligence (39%), followed by system glitches (33%) and malicious or criminal attacks (28%). However, malicious attacks are on average the most costly.

The Microsoft Security Intelligence Report [36] contains interesting statistics on software vulnerabilities and malicious software in Italy and worldwide, related to the period July through December 2012. The report

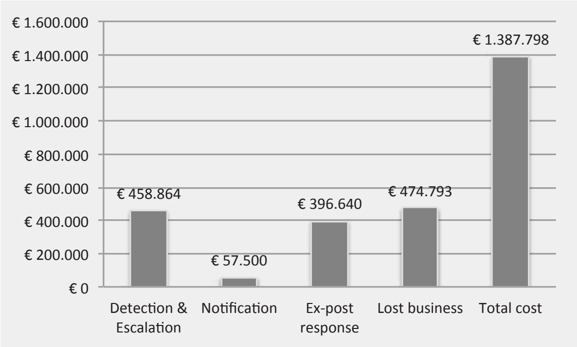


Figure 1.7: Average total organizational cost of data breach per record (source: Ponemon Institute, 2011).

Table 1.5: Infection rate statistics for Italy (source: Microsoft, 2012).

CCM	1^{st} **quarter of 2012**	2^{nd} **quarter of 2012**	3^{rd} **quarter of 2012**	4^{th} **quarter of 2012**
Italy	6.5	4.5	3.7	3.2
Worldwide average	6.6	7.0	5.3	6.0

uses the Computer Cleaned per Mille (CCM) metric, which represents the number of computers cleaned for each execution of the Microsoft Malicious Software Removal Tool (MSRT). CCM represents a useful metric to measure infection rates. Table 1.5 shows a comparison between the infection rate statistics for Italy and the worldwide average in 2012. From the report it emerges that computers without up-to-date real-time anti-malware protection were 5.5 times more likely on average to report malware infections than computers with protection. The document also contains statistics on malware and potentially unwanted software categories. Figure 1.8 shows the detection percentages of threat categories for the last quarter of 2012. The most common category in Italy in this period was miscellaneous potentially unwanted software (32.2% of computer reporting detections), followed by adware (25.6%) and miscellaneous trojans (23.8%).

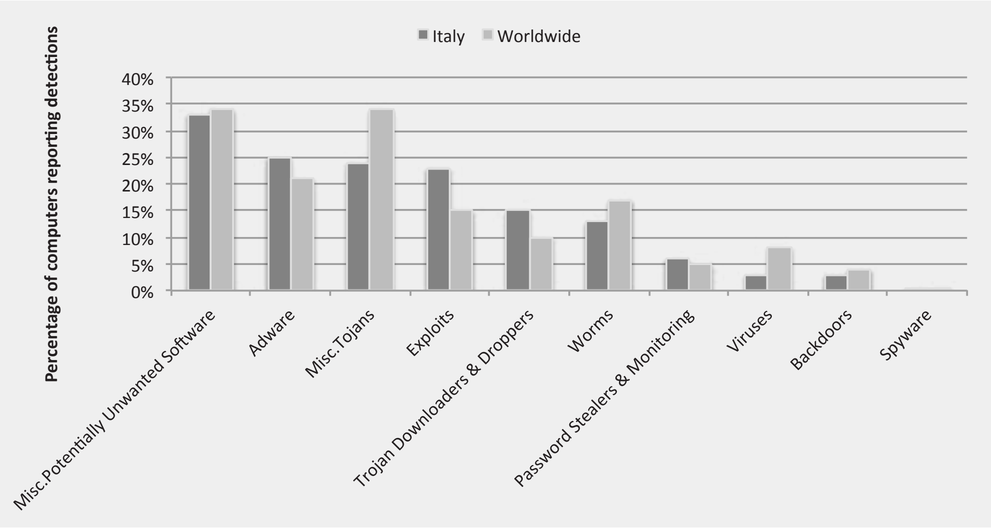


Figure 1.8: Threat categories (source: Microsoft, 2012).

CHAPTER 2

Cyber Security: Italian Governance and Legislative Overview

The intrinsic characteristics of cyber security require a national strategic plan for critical infrastructure protection organizations and the identification of practices to realize this as well as response actions to threats with technical and organizational tools able to face the new socio-technological context and the new interdependencies produced by cyberspace. In other words, a governance of cyber security. To achieve this goal primary and secondary regulation which individuates specific competency areas, jurisdictional areas, involved subjects, types and modalities of a-priori and a-posteriori intervention is needed, thus applying extra-national regulations. The growing number of threats and security breaches has already caused considerable economic damage, leading to reduced user confidence in the use of new services and technologies and hindering the development of electronic commerce and the realization of the so called digital agenda in Italy. In fact in this area Italy presents a slight delay in the definition of the governance of cyber security. Even though the cyber security issue has been debated since early 2000, significant improvements in the identification of a road-map for the implementation of a national Italian strategy have been observed only recently.

2.1 Actors involved in cyber security governance

This section describes the legislative landscape during the last decade and the assets that now are leading the process of making Italy a secure place from cyber threats.

1999-2004 (D.M. 378/September 1999, D.M 28 September 2001, D.M January 2003) The Inter-Ministerial decree of 21 September, 1999 established a working group made up of representatives from the Ministry of Communications (Ministero delle Comunicazioni), Ministry of Justice (Ministero della Giustizia), and Ministry of Interior (Ministero dell'Interno), with the task of operating in the sector of network security and communications protection as a support to administrative and regulatory interventions. To achieve these goals the working group mainly dealt with internationally harmonized regulations in the telecommunication sector.

In 2003, the working group became the Permanent Observatory for Network and Communications Protection and Security (Osservatorio permanente per la sicurezza e la tutela delle reti e delle comunicazioni) within the Ministry of Economic Development (Ministero dello Sviluppo Economico). The observatory was established with the Inter-Ministerial decree of 14 January, 2003. Its aim is to take into account the technological and regulatory evolution of the different aspects of the telecommunications sector, with particular attention to security. It is permanently integrated with representatives of the Ministry of Defense (Ministero della difesa), Department of Public Service (Dipartimento per la funzione pubblica), Department of Innovation and Technology (Dipartimento per l'innovazione e le tecnologie) and Ministry of Productive Activities(Ministero delle attività produttive).

The observatory, among others, has played a supporting role aimed at transposing Directive 2002/58/EC into reality. This directive concerns the processing of personal data and the protection of privacy in the electronic communications sector, and the legislative decree concerning the Electronic Communications Code (Codice delle comunicazioni elettroniche) which was issued September 16, 2003.

In October 2001, the Technical Interdepartmental Committee of Civil Defense (Commissione Inter Ministeriale Tecnica della Difesa Civile - CITDC) was established as a political and military unit (supporting Nucleo Politico Militare) supporting organ for the technical coordination of civil defense activities in case of crises. It operates within the Department of Fire and Public Rescue and Civil Defense (Dipartimento dei Vigili del Fuoco e del Soccorso Pubblico e della Difesa Civile), as part of the Central Directorate for Civil Defense. It has the role of evaluating emergencies and planning the measures to be taken in the event of crisis. The committee also considers other hypotheses of risk, not directly related to malicious acts, which can lead to situations of crisis for the continuity of government as well as damage to the population and, in general, the security of the country. In this sense, the committee and the department delve into the issues related to critical infrastructure and, in close collaboration with the Ministry of Health, the management of a crisis produced by the spread of serious epidemic diseases. The CITDC meets at the Ministry of Interior which presides over it and ensures the coordination of the central government departments involved.

In March 2003, the Ministry for Innovation and Technology established the Working Group on CIIP , in which representatives from ministries involved in critical infrastructure management (Interior, Infrastructure, Communication, etc.), major private providers (ABI, ASI, CESI, GRTN, RFI, Snam Rete Gas, Telecom Italia, Wind and others) and the research and academic world took part. In March 2004, this working group issued the document Critical Information Infrastructure Protection: The Italian Situation, in which the results of work carried out during the previous year are reported.

2005-2006 (D.L. n. 155 of 31/7/05) In 2005, the Ministry of Communication established a special working group to analyze the responsibilities and security requirements that CII imposes on communication infrastructure operators, and to analyze the dependencies of the latter on other critical infrastructure. This working group has issued several guidelines[1]. As far as critical information infrastructure protection is concerned, the legislative decree (D.L.) n. 155 of 31/7/05 (the so called Legge Pisanu) conferred jurisdiction to the Ministry of Interior, identifying the Postal and Communications Police as the unit responsible for law enforcement initiatives against cyber attacks on critical information infrastructures

In 2005 by Legislative Decree n.82/7 (March 2005) the Digital Administration Code (CAD) (Codice dell'amministrazione digitale) was introduced as a primary point of reference for the Italian PA sector; the code constitutes the necessary premise for implementing the process of digitalization of administrative activities as a prerequisite for real modernization of public bodies. A proper and effective use of these instruments begins from the stage of acquisition of services and equipment , for which DigitPA (see below) offers its know-how, through the formulation of opinions on policies issued by central PA, monitoring plans and ICT the publication of guidelines on the quality of ICT goods and services , which are valid for all PA, central and local. Since 2005 several working groups have been set up by DigitPA for the implementation of CAD and documentation related to the following topics:

- Formation and conservation of an electronic document system and management of document flows;
- Digital identity;
- Access to PA data;
- Business continuity and critical infrastructure in the PA sector;
- Digital signatures.

Box VI: The Digital Administration Code (CAD) [26].

In 2006 a new coordinating body was established, the so called Tavolo PIC (Inter Ministerial Coordination Platform) and Contact Point for the Sector of Critical Infrastructure Protection (Tavolo interministeriale di coordinamento per la protezione delle Infrastrutture critiche). It is chaired by the Military Advisor to the President of the Minister's Council.

Tavolo PIC assigned the CITDC to set the CI identification criteria and has determined, from time to time, the national position on the initiatives and activities in the EU and other international forums.

[1] The Network Security of Critical Infrastructures (2005); Network Security: From Risk Analysis to Protection Strategies (2005); Guideline on Managing Local Emergencies (2006).

2008 (CNAIPIC) To improve the protection of critical information infrastructures against cyber threats, in 2008 the Ministry of the Interior established the National Anti-Cybercrime Center for the Protection of Critical Infrastructure (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche - CNAIPIC) as a special unit within the Postal and Communication Police Service [28].

CNAIPIC acts as a police authority for all activities of prevention, repression and contrast of criminal actions committed against the different critical infrastructure through cyberspace. For this purpose CNAIPIC and critical infrastructures maintain and protect exclusive dedicated ICT links, for a mutual and constant sharing of data and information relevant to the assessment, prevention and repression of threats and cyber crime (see Box VII).

In 2012, the CNAIPIC managed a total of 286 events relating to the damage of critical information infrastructures of national interest (private and institutional). In particular, the Operations Room of the CNAIPIC managed:

- 136 DDOS attacks or defacement, against internet services related to institutional sites and critical information infrastructure of national interest;
- 61 intrusions and unauthorized access to computer systems related to critical infrastructure or institutional databases;
- 51 compromised authentication credentials on the computer systems of critical infrastructure, implemented through computer viruses and BOTNETS.
- Furthermore, CNAIPIC also issued 38 alerts for computer system /data transmission vulnerabilities.

During this year, there was a significant increase in the activity of public-private partnership, which led the signing of four new agreements by Enel, H3G, Finmeccanica and Atac.

Box VII: CNAIPIC's activities in 2012 [8]

CNAIPIC carries outs its functions through the activities of the Operational Sector (Settore Operativo) and Technical Sector. The service is organized into distinct areas of intervention which include [30]:

- Cyber terrorism;
- Copyright;
- Hacking;
- Critical infrastructure protection;
- E-banking;
- Analysis of emerging criminal phenomena;
- Betting and gaming systems on line.

Furthermore, the Unit of Cybercrime Analysis (Unità d'analisi del crimine informatico - UACI) was established, within the service, to study and analyze the phenomenon of cyber crime in partnership with major Italian universities.

Territorial departments have an organization similar to this service, but with a more operative profile and more bounded to their jurisdictions. These departments manage the legal cases and the emergencies that arise from reports made by citizens to police hot lines.

In order to enhance the effectiveness of strategy against cyber crime, the Communications Police participate with some of its representatives in permanent working groups established by the government or international organizations, including the Inter Ministerial Group for Network Security (Gruppo Inter Ministeriale per la sicurezza delle reti), G8, the European Community, the Council of Europe, OCSE, Interpol, Europol. Moreover, it cooperates with institutions and private operators dealing with communications in general.

2009 (SCIIC) Following the EU Directive 114/2008, in 2009[2] the Inter Ministerial Coordination Secretariat for Critical Infrastructure Protection (Segreteria di Coordinamento Inter Ministeriale per le Infrastrutture critiche

[2] Ordinance 3836 PCM.

- SCIIC) was established within the Italian Presidency of the Council of Ministers. The aim is to ensure coordination, coherence and synergy between the initiatives and activities of the authorities concerned with the protection of CI.

The functions of the SCIIC are attributed to an operational nucleus [3]. In addition to the aspects of civil protection associated with risk CBRN (Chemical, Biological, Radiological, and Nuclear), SCIIC is responsible for coordinating Inter-Ministerial activities (including those of an international context) which regard critical infrastructure. The SCIIC is under the control of Military Adviser to the President of the Council of Ministers.

2010 (DPCM 5 May 2010) In 2010, by decree, the President of the Council of Ministers established the Organization for Crises Management, which led to a reorganization of the crises management system by creating new bodies, such as:

- (art. 4) the Political Strategic Committee (Comitato politico strategico - CoPS) a permanent body, which has been set up within the Presidency of the Council of Ministers and tasked with the political and strategic guidance of crises. It is chaired by the prime minister and is composed of the Ministers of Defense, Foreign Affairs, Interior, Treasury, Economic Development; It meets exclusively during a state of crisis, and builds on the results of the pre-decisional phase undertaken by the technical staff.
- (art. 5) the Inter Ministerial Unit for Situation and Planning (Nucleo interministeriale situazione e pianificazione - NISP) is responsible for supporting CoPS and the President of the Council of Ministers. The NISP, which replaced the Political Military Unit, is a non-permanent body which systematically monitors the national and international security situation to foresee and prevent possible crisis. It relies on an early-warning system provided by the bodies represented within the NISP. The NISP in its activities is supported by CITDC.

In the event of an international crisis or attack (including CBRN) involving more than one critical infrastructure, the prime minister who is in charge of operations, uses CoPS's structures and coordinates with CPS (Comitato Politico Strategico) and NISP; the latter one cooperates with CITDC in order to manage the emergency involving civil defense.

A common secretariat for CoPS and the NISP was instituted in the same year (DPCM 22 December 2010) and called Secretariat for Critical Infrastructure (Segreteria per le infrastrutture critiche - SIC). It has the task of looking after the inter ministerial coordination of all national and international activities and of all technical and scientific activities for the identification and designation of ECI.

2011 (DL 61/2011) In April 2011 the Italian government approved Legislative Decree 61/2011 which transposes in Italy the European Directive on Critical Infrastructures. The decree made the NISP responsible for the individuation and designation of an ECI, and integrates its composition with representatives of the ministries involved (Economic Development, Infrastructure and Transportation, Interior, Foreign Affairs, and Civil Protection Department). This structure is also in charge of defining sectorial criteria thresholds through which the criticality of a structure is established.

From an operating point of view, the infrastructure's operator, with the support of representatives of the ministries involved and the responsible structure, draws up the Operator Security Plan (on the basis of the minimum requirements stated by Annex B of the decree) PSO. The PSO identifies critical infrastructure assets and which security solutions exist or are being implemented for their protection. At procedural level it covers: the identification of important assets; risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact; identification, selection and prioritization of counter-measures and procedures with a distinction between permanent security measures and graduated security measures.

Furthermore, the same decree gives the responsibility for the protection of an ECI, at national level, to the ministries involved and the Civil Protection Department and at local level, to the prefect with territorial jurisdiction. A secrecy classification, according to in force legislation, is also attributed to sensitive information related to CI.

In May 2011, the Secretariat for Critical Infrastructure (Segreteria Infrastrutture Critiche - SIC) was designated as the NIPS supporting structure (mentioned in the Legislative Decree 61/2011). It supports NIPS with technical and scientific activities, for individuation of an ECI and for cooperation with the European Commission with similar structures existing in other member states.

[3] Established by decree PMC n.3275 on 28 March 2003, article 4, para 1

2012-2013 (ADI and AGID) In March, the Italian Digital Agenda (Agenda Digitale Italiana - ADI) was approved. It is part of a decree about growth which tackles a number of areas that are key to economic development at a critical juncture in the country's history. The decree covers infrastructure investments, support for easier creation and development of start-up companies, financing schemes for small and medium sized enterprises and broadband deployment in specific areas. As far as the government is concerned, it addresses open data, digital identities, electronic health records, electronic student records and measures to make the judicial system more efficient by increasing the use of electronic communication and online notifications.

One of the biggest challenges will be re-engineering and digitalizing Italy's public administration system, which is currently very fragmented system. Only 20% of it is interoperable and individual authorities, including for reasons of hanging on to power, claim difficulties in pooling information. Another area of great significance is the planned digitization of the education system, to which end the re-skilling of teaching staff will also be crucial. ADI stresses the importance of investment in infrastructure aimed at improved access to faster network for the population. It also stresses the need to ensure the safety and reliability of the infrastructure through the establishment of more efficient networks which ensure high quality service and by building structures dedicated to their preservation and protection (see Box VIII).

According to ADI, the national cyber security strategy plans to act on the following areas:

- Educate citizens, business and industry: raising awareness of the serious risks related to the web (e.g. the UK initiative Get Safe Online, a public-private online campaign to raise awareness);
- Enhance threats detection and contrast tools: develop tools (organizations, processes, legislation and applications) able to detect and contrast potential threats (e.g. the National Cyber Security Centre of the Netherlands will adopt tools to enhance awareness and classification of threats and vulnerabilities through public-private information sharing);
- Promote education: create education paths able to provide the necessary competences from early school years (e.g. the United States has issued a draft plan, National Initiative for Cyber Security Education Strategic Plan, which outlines the educational steps, from primary school, for a career in cyber security);
- Strengthen public-private cooperation: create mechanisms of debate, sharing and coordination between the public and private sectors, especially with regard to critical infrastructure protection (e.g. Germany, in its strategy, envisaged a National Cyber Security Council where representatives of the private sectors are asked to participate as associated members);
- Strengthen mechanisms of international cooperation: involvement in international forums for the discussion of standards, policy and international principles on cyber security (e.g. the Czech republic's strategy envisages an active participation in EU and NATO forums);
- Create and enhance mechanisms for incident response: it is necessary to enhance, through the establishment of national CERTs and, in some cases, to create, specialized structures able to respond to cyber attacks and incidents within national boundaries and able to coordinate with the corresponding centers at international level.
- Define a standard for the management of digital identities as well as for guiding principles for the creation of a federated system at national and international level, able to satisfy the daily needs of digital citizens, including improved security for Internet payment systems.
- Stimulate the growth of an Italian cyber security industry, concerning both technology/services, and skills and talents. This will not only allow for the growth and maintenance of specialized competences, but will also attract talent and experts from other countries.

Box VIII: ADI line of action on Italian cyber security [23].

A few months later Decree n. 83 15/6/2012 converted by law n. 147 established the Agency for Digital Italy (Agenzia per il Digitale DigitPA). It is responsible for the implementation of the objectives of the Italian Digital Agenda, taking into account the European Digital Agenda and the guidelines developed by the Steering Committee (Cabina di regia, Article 47 of Decree-Law 9 February 2012, n. 5).

2012-2013 (Law 133/2012, DPCM 24 March 2013) Two other regulatory measures, adopted between 2012 and 2013, contribute to defining organization and strategy for national cyber security. Law no 133 /2012[4] and DPCM 24 March 2013.

Law 133/2012 attributes new and more detailed responsibility in the field of national cyber defense and security to the Italian intelligence system. For instance this law gives the prime minister the power to issue directives to the Intelligence and Security Department (Dipartimento informazioni per la sicurezza - DIS)[5], after prior consultation with the Inter Ministerial Committee for the Security of the Republic (CISR)[6], and to the security intelligence services in order to strengthen security intelligence activities for the protection of critical infrastructure, with particular reference to national cyber defense and security. Regarding DIS, it will coordinates intelligence activities directed at strengthening national cyber defense and security.

The DPCM 24 January 2013[7] defines the institutional architecture tasked with safeguarding national security in relation to critical infrastructure and intangible assets, with particular attention to the protection of cyber security and national security. It indicates the tasks assigned to each component and the mechanisms and procedures to follow in order to reduce vulnerability, to improve risk prevention, to provide timely response to attacks and to permit immediate restoration of the functionality of systems in the event of crisis. The decree responds to the need to define a national strategic framework capable of protecting critical infrastructure from cyber attacks. The DPCM identifies three different levels of intervention:

1. Strategic and political level (level 1);
2. Operating level, granting support and coordination between all bodies involved (level 2);
3. Crisis management (level 3).

More specifically,

A. the decree assigns the prime minister the responsibility for the adoption (on the basis of CISR's proposal) of the national strategic framework and a national plan (deliberated by CISR) to ensure cyberspace security; the prime minister has also the power to issue directives (after prior consultation with the CISR) to the DIS and to the security intelligence agencies in order to strengthen security intelligence activities for the protection of critical infrastructure, with particular reference to national cyber defense and security.

B. the decree assigns to the CISR the responsibility of deliberating the following activities:

   1. overseeing the implementation of the National Plan to Secure Cyberspace;
   2. approving the guidelines to facilitate effective collaboration between institutional and private operators interested in cyber security, aimed at information sharing, best practices adoption and definition of measures directed to cyber security:
      - the elaboration of general and fundamental objectives in the field of cyber security to be pursued in the context of information policy for the security of the organizations involved in information security;
      - promoting the adoption of the necessary steps to ensure, in a coordinated manner, the full participation of Italy at various international cooperation forums (both bilaterally and multilaterally, both the EU and NATO), for the definition and adoption of policies and prevention and response strategies;
      - the elaboration of proposals for legislation and organization necessary to improve measures for prevention and response to cyber threat, and for crisis handling.

[4] Law no. 133 of 7 August 2012 (published in the Official Journal no. 186 of 10 August 2012).

[5] By Law n. 124/2007, DIS supports the President of the Council of Ministers to ensure a fully unified approach in the Security Intelligence System's planning of intelligence collection as well as in the Security Intelligence Services' analyses and operational activities. DIS, among other activities coordinates the two Italian intelligence agencies, namely AISE and AISI.

[6] Law n. 124/2007, CISR makes proposals and take decisions regarding the lines and general goals of security intelligence, also setting intelligence requirements. The CISR consist of: the President of the Council of Ministers, the Minister of Foreign Affairs, the Minister of the Interior, the Minister of Defense, the Minister of Justice, the Minister of Economy and Finance, the Minister of Economic Development.

[7] Published in GU n.66 del 19-3-2013.

C. The decree reinforces the role ceded by DIS, which is in charge of coordinating intelligence agencies in order to reinforce cyber security.

In order to coordinate all the activities implicit in the CISR functions, art. 4 of the decree established the Collegial Co-ordinating Body (Organismo collegiale di coordinamento), chaired by the Director General of the DIS. Its main tasks are:

- to prepare all meetings regarding cyber security;
- to grant all preliminary investigations regarding CISR's decision and acts;
- to monitor the implementation of the national plan to ensure cyberspace security, guaranteeing the effectiveness of all private and public organizations involved.

Interestingly the Collegial Co-ordinating Body has the task inter alia of identifying potential threats and vulnerabilities to national systems (both private and public) and defining the best practices with the help of a scientific committee which has been set-up at the Intelligence System Training School (Scuola di formazione del Sistema di Intelligence). Public sector representatives (i.e. government, universities etc.) and private sector representatives (i.e. research, industry etc.) will be part of this scientific committee. On the basis of guidelines provided by CISR and information provided by all parties involved (PA, Intelligence Information system, Nucleus for Cyber Security, Scientific Committee) the Collegial Co-ordinating Body coordinates the formulation of the necessary indications in order to identify and recognize vulnerabilities in cyberspace; and to adopt best practices and security measures. In addition to the above, it is worth mentioning the setting up of a so-called Nucleus for Cyber Security (Nucleo per la sicurezza cibernetica) within the Military Adviser's Office. It is a permanent body responsible for maintaining links and coordination between the different components of the institutional architecture involved in various capacities in the field of cyber security, in accordance with the powers conferred by law to each of them. Members of National Intelligence, Ministry of Internal Affairs and Foreign Affairs, Ministry of Defense, Ministry of Economic Development, Ministry of Economy and Finance, Civil Protection and the Digital Agency are part of the Nucleus for Cyber Security. The nucleus was established to support the prime minister in all activities concerning the prevention and/or preparation for a possible crisis and the activation of warning procedures. The nucleus, among other activities, will:

a) promote the planning of the response to crisis situations by both government and private stakeholders and the development of all necessary procedures for inter-ministerial coordination, fitting in with the schedules of Civil Defense and Civil Protection;

b) assess and promote procedures for information sharing, including with private stakeholders, for the dissemination of alerts relating to cyber events and crisis handling;

c) promote and coordinate cyber security exercises, both Inter-Ministerial and at international level, involving the simulation of events.

In order to handle a crises event in a coordinated manner, the decree assigns to the NISP the role of Inter Ministerial Cybernetics Crises Table. The inter ministerial body is chaired by the prime minister's military advisor and will include representatives of all the institutions involved. It will ensure that the response and the appointment of the various departments' and agencies' responsibilities in relation to cybernetic crisis's are performed in a coordinated manner. The decree, furthermore, establishes a strict collaboration between the Inter Ministerial Cybernetics Crisis Table and the national CERT (see next section) in order to deal with all technical aspects in elaborating emergency responses.

Only one article, Article 11, in the decree refers to private operators. The decree establishes that private operators[8] (as required by this law or by prior special agreement) have to:

a) communicate to the Nucleus for Cyber Security - also via institutionally authorized assets as per Article 16-bis, paragraph 2, letter b) of Legislative Decree n. 259/2003 - of each and every security or integrity breach of their software systems, using protected broadcast channels;

b) use the best practices and cyber security measures defined in Article 16-bis, paragraph 1, letter a), of Legislative Decree n. 259/2003 and Article 5, paragraph 3, letter d) of this decree;

c) supply information to security information bodies and grant access to their data bases for the purpose of the respective cyber security, in the cases provided by Law n. 124/2007.

[8] Those private operators identified by Article 1, paragraph 1, letter d) of the Decree of 9 January 2008 [28].

d) assist in managing cybernetic crises by helping to restore the working order of systems and networks that they manage.

Private-public partnerships are crucial for mitigating cyber risks and fostering collaboration to improve cyber resilience. These include information sharing initiatives which help government and businesses prevent, protect, deter and recover from cyber threats. While partnerships have been established, several challenges still prevent stakeholders from reaping the full benefits of information sharing. The need to build trust among parties and share actionable information is crucial. Jurisdictional boundaries, the fear of being held liable, and the quality and quantity of information shared still represent major barriers to information sharing. Important progress has been made in using and promoting information sharing organizations. However, some challenges still limit the information flow between the public and private sectors. While many organizations recognize the importance of information-sharing, some observe that there are still gaps regarding the "how, what, when and to whom" [42]. Several factors, such as challenges related to the management and organization of the group, the risk of a damaged reputation, legal repercussions and the lack of clear agreements and expectations, may explain why the current environment is not fully effective [10].

2.2 Emergency response: focus on CERTs

A computer emergency response team (CERT) can be defined as an organization responsible for setting up a framework for responding to cyber security incidents. It provides the necessary services for handling incidents and supports its constituents in their recovery from breaches of computer security. In order to mitigate risks and to minimize the number of required responses, many CERTs also provide preventative and educational services for their constituents. More recently the term CSIRT which stands for Computer Security Incident Response Team is starting to replace CERT. It invokes a more holistic approach to security rather than relying only on reactive forces. CERTs worldwide are generally founded and financed by governments or academic institutions. The reason for this is that government agencies are interested in protecting national security and universities by their very nature try to find solutions to new problems.

Historically, the name Computer Emergency Response Team is the designation for the first team at Carnegie Mellon University (CMU). CERTs existence is linked to malware, especially computer worms and viruses. After the Morris Worm paralyzed a good portion of the Internet in 1988, CERT/CC at Carnegie Mellon University was started under a US government contract.

To respect the indications of EU Directive 140/2009 and to achieve the target fixed by the European agenda, in several EU member states, governments have set up the so called National CERTs. The main goal of a national CERT, from a cyber security perspective, is to protect national and economic security, the ongoing operations of a government, and the ability of critical infrastructure to continue to function. Therefore a national CERT typically monitors incidents at a national level, identifies incidents that could affect critical infrastructure, warns critical stakeholders about computer security threats, and helps to build organizational CERTs in the public and private sectors. Typical tasks of national CERTs include:

- establishing a national point of reference within a country or region to coordinate security incident management activities;
- analyzing and synthesizing information on incidents and vulnerabilities disseminated by other CERTs, vendors and technology experts to provide an assessment for their own constituents and communities;
- facilitating communications across a diverse area, in order to bring together multiple sectors (government and military, critical services and infrastructures, commercial, academic, banking and finance, transportation, etc) to share information and collaborate in addressing computer security problems, such as widespread computer security incidents, threats and vulnerabilities;
- developing protocols and mechanisms for trusted interaction with other relevant stakeholders such as the intelligence community, law enforcement agencies, policymakers, etc.

Compared to other main EU countries, Italy has recorded a significant delay in the setting up of the national CERT. Although the identification of a national CERT at the MISE was introduced by Legislative Decree 28 May 2012, n. 70 (to comply with the transposition of Directive 2009/140/EC relating to electronic communications), to date there is not any operating structure of this type.

Table 2.1: Taxonomy of private-public information sharing system

Levels of communication	**Strategic**: The exchange of cyber security risk information among organizations enable companies and governments to develop a full plan to improve cyber resilience based on best practices and lessons learned from others, or to partner in the creation of a broader national plan. **Operational**: The exchange of data needs to be integrated into the organization's on-going risk management practices and policies. Operationally, the organization should also have routine points of contact with major partners, vendors, suppliers and customers to exchange information and receive reports about incidents or issues, preferably through a center of excellence for operational risk and security issues. **Technical**: Once the incident has concluded, entities return to their more normal state of sharing a limited or tailored set of data. It is critical that companies have clear and trusted points of contact with whatever information sharing clearing house it may use (Information Sharing and Analysis Centers, Computer Emergency Response Teams, a national incident management capability, a local law enforcement agency, etc.) so that when a cyber incident begins, the organization can draw on known contacts and familiar processes until a normal operational state is achieved.
Information type	**Threats**: The exchange of comprehensive and timely alerts and information on attacks can help private and public organizations determine the nature of an attack, implement a mitigation strategy or advise others on how to respond to an imminent attack. It enables an organization to gather the most up-to-date threat data, integrate it in their systems and processes, make real-time decisions and take defensive actions. **Vulnerabilities**: Sharing information about vulnerabilities and new discoveries helps organizations address weaknesses before they are exploited and shift from reactive to proactive security measures. Sharing information on known and "fixable" issues can also be important, as a matter of good corporate citizenship.
information sharing lifecycle	**Preventive**: A preventive approach enables an organization to assess the current threats and define a set of capabilities that should be met when implementing its cyber risk management program. **Real time**: To ensure such a response, an organization needs to establish a systematic approach to manage alerts, oversee the network attacks and monitor responses to incidents. Some organizations are already using one or more real-time sources to react against cyber attacks. **Post event**: Information sharing may also relate to a cyber incident that is no longer active. It enables an organization to take advantage of lessons learned from other organizations and integrate these in its cyber risk management program. As such, an organization is able to improve its response mechanisms and prevent future threats and attacks.

Source: based on World Economic Forum (June2012)[9]

The main regulatory intervention on emergency response strategy and crisis management is basically made up of the aforementioned decree of 24 January 2013. The decree fixes the role and responsibility of all bodies and organizations involved in national critical infrastructure security protection by defining:

- all tasks and responsibilities assigned to each member,
- procedures to be followed in order to reduce vulnerability, to improve risk prevention, to provide timely response to attacks and to allow for the immediate restoration of the functionality of systems in the event of a crisis.

The government's intentions were those of providing the organizational-functional model for a full integration between the activities pertaining to:

- the Ministry of Economic Development and the Agency for Digital Italy,
- the structures the Ministry of Defense dedicated to the protection of their networks and systems,
- the structures of the Ministry of the Interior dedicated to the prevention and combating of cyber crime and civil defense, and those of civil protection.

As shown in the previous sections, the Decree has established the activities pertaining to the national CERT. However, even after this further regulatory intervention, the national CERT is still far from a concrete implementation. It is easy to assume that the national CERT should be developed according to public-private model, in order to benefit from the exchange of good practices, from the sharing of information, and in order to implement a body which does not result in the need for further financing. In fact, for the effective implementation of the actions outlined above, it plays central role in information sharing, as no person, though endowed with great resources, can build a security system in total autonomy.

The national CERT should, therefore, be based on a cooperative model between public and private, which is essential for rapidly building processes and services of information sharing and mutual support in case of accident management on a large scale[53]. Such cooperation could be achieved by setting appropriate memoranda of understanding and agreements, ensuring effective coordinated action in the event of an accident with a greater reduction of impact and abatement costs. Another distinctive feature is that the CERT should be closely connected with the academic world. Looking at the international experiences, the CERTs generally tend to benefit enormously from the close connection with the academic world; CERTs in fact, can exploit academy's capacity to produce the most innovative solutions in the field of secure information and in education.

The E-government 2012 Information Security Plan foresees the stabilization and strengthening of the CERT of the Connectivity Public System (CERT del Sistema Pubblico di Connettività - CERT-SPC) within DigitPA. The structure acts as a national contact point for the prevention, monitoring, coordination of information and analysis of security incidents within the Public Connectivity Services. It is a governmental CERT which provides:

1. Proactive services, such as the organization and monitoring of information sources, the production of newsletters for the members (early warning) and the preparation of operational tools for information management;
2. Operating activities, such as coordination and information support during the occurrence of cyber incidents;
3. Strategic activity: i.e. the ability to use data collection and analysis aimed at supporting decisions of the Committee responsible for the coordination of Connectivity Public System (Sistema pubblico di connettività - SPC) and necessary for improving the overall level of safety of the SPC.

From an operating point of view, the CERT-SPC acts as a central organ of the public administration structure through the Local Security Unit (Unità Locali di Sicurezza - ULS). The ULS are established in each domain related to SPC, in conjunction with the Security Operation Center (SOC), and provide access to a federated SPC network to oversee operational management and service continuity.

At government level, in Italy, in addition to the CERT-SPC and the planned national CERT, there is the CERT DIFESA which coordinates all army units.

Concerning other CERTs operating in Italy, a complete and updated list is not available. Table 2.2 lists CERTs reported at the beginning of June 2013 on ENISA website. Such CERTs, however, seem in some cases

Table 2.2: List of private-public information sharing system as reported by ENISA web site (June 2013)

Name	Website	Date	TI Status	First Membership	Area
CERT-IT	http://www.galileo.it/crypto/cert-it.htm	1Q 1994	Not listed	Not member	Research and Education
GARR-CERT	www.cert.garr.it	01/03/1999	Accredited	Not member	Research and Education
S2OC*	www.tuconti.telecomitalia.it	Not specified	Not listed	Not member	ISP Customer Base
CERT ENEL*	www.enel.it/attivita/servizi_diversificati/informatica/cert	Not specified	Not listed	Not member	Energy Sector
CERT-RAFVG	cert-rafvg.regione.fvg.it/	Not specified	Not listed	Not member	Local Agencies
SICEI-CERT*	cert.chiesacattolica.it/	Not specified	Not listed	Not member	Dioceses of Catholic church

inactive or there is a lack of information necessary for understanding the activity which is actually performed. For example, no information was found on the existence of the CERTs listed in the table which are marked with an asterisk.

CHAPTER

3

Cyber Security Strategy in EU and Some Developed Countries

The maintenance of a good level of cyber security in the EU context involves disparate sectors with different jurisdictions and responsibilities, both at national and EU level. Managing cyber security through centralized supervision at European level is not feasible. National governments have the main responsibility for the maintenance of a good level of security and must cooperate at EU level in case of risks and security breaches that extend beyond national boundaries.

The structures involved in the maintenance of cyber security are organized in three fundamental areas: Network and Information Security (NIS), law enforcement and defense. At national level member states should have already, or as a result of the European cyber security strategy, national structures in each of the aforementioned areas (see figure 3.1). Member states are responsible for carefully defining the roles and responsibilities of such national structures.

The European strategy invites member states to encourage information sharing between national structures involved in cyber security and the private sector, so that they can have both a comprehensive vision of risks and security threats, and a better comprehension of cyber crime techniques so as to respond more rapidly and effectively.

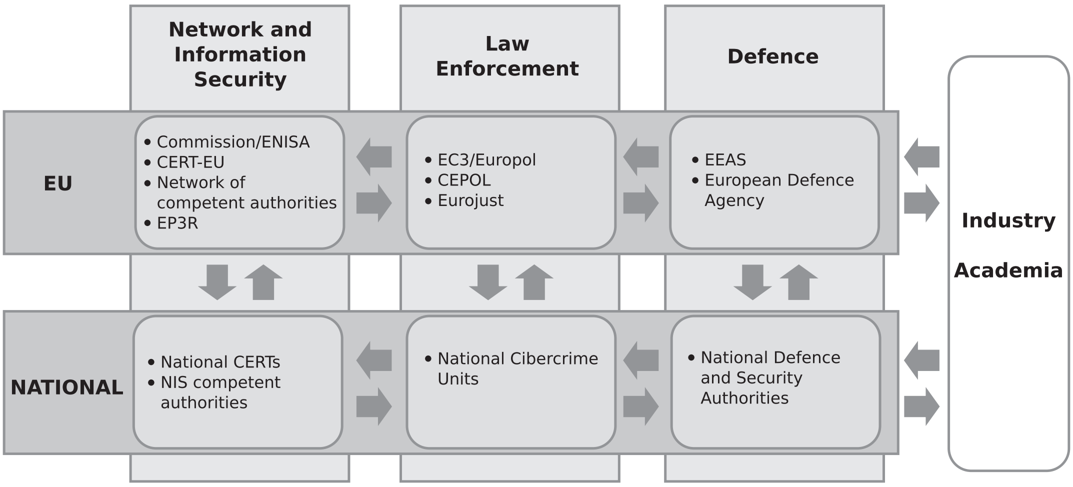

Network and Information Security
Law Enforcement
Defence
EU
• Commission/ENISA
• CERT-EU
• Network of competent authorities
• EP3R
• EC3/Europol
• CEPOL
• Eurojust
• EEAS
• European Defence Agency
NATIONAL
• National CERTs
• NIS competent authorities
• National Cibercrime Units
• National Defence and Security Authorities
Industry
Academia

Figure 3.1: EU cyber security strategy: Interacting organizations at national and EU level [16].

Several organizations are involved at EU level. In the NIS area, the European Network and Information Security Agency (ENISA), established in 2004, is responsible for improving network and information security. Currently a new regulation [15] to strengthen ENISA and modernize its mandate is under examination by the

Council of Europe and the European Parliament. ENISA will also be responsible for building expertise in security of industrial control systems, transport and energy infrastructure. A Computer Emergency Response Team at EU level (CERT-EU), responsible for the security of the IT systems of EU agencies and institutions, was established in 2012.

Furthermore, in March 2009, the European Commission established the European Public-Private Partnership for Resilience (EP3R) with the objective of encouraging sharing of NIS related information between interested parties in the public and private sector at European level. In the area of law enforcement, in 2013, the European Cyber Crime Centre (EC3) was formed within Europol to represent the European focal point of fight against cyber crime. In particular, EC3 will provide analysis and intelligence, support investigations, provide high level forensics and facilitate cooperation and information sharing between the competent authorities of member states, the private sector and other stakeholders. Europol/EC3 and Eurojust will cooperate closely to improve their capability in fighting cyber crime. In the area of defense, the main responsibility for cyber defense at EU level is the European Defence Agency (EDA). The European strategy for cyber security supports cooperation and information sharing between these organizations, in particular ENISA, Europol/EC3 and EDA, and between these and their counterparts at national level.

Finally, at international level the European Commission and the member states engage in dialogue with international partners and organizations such as the Council of Europe, OECD, OSCE, NATO and UN. A list of national cyber security strategies can be found here [19].

3.1 Germany

The German Federal Government provides a substantial contribution to cyber security, maintaining and promoting economic and social prosperity in Germany. The latest German strategy, 2011, mainly focuses on civilian approaches and measures. These are complemented by the measures undertaken by the armed forces (Bundeswehr) aimed at protecting its capabilities and measures based on mandates to include cyber security as part of the preventive security strategy. The global nature of information and communication technologies raises the necessity for an international vision and coordination on security policy aspects with the aim of enhancing cyber security capabilities of the international community. For this purpose, Germany cooperates with the United Nations, the European Union, the Council of Europe, Nato, G8, OCSE and other international organizations.

The German strategic plan is organized in 10 specific strategic areas:

1. Protection of CII (Critical Information Infrastructure).
   CIIs constitutes the central component of almost all critical infrastructure. Thus, protecting such infrastructures is the primary objective of cyber security. In order to support CIIs protection the introduction of new technologies is taken into consideration by the plan. Cooperation and information sharing between public and private sectors is also a priority.

2. Security of IT systems.
   Germany aims to support security of IT systems with an informative intervention, to provide citizens and small and medium-sized businesses with consistent information concerning risks related to the use of IT systems, and by promoting the use of fundamental security functions, such as electronic proof of identity and De-mail[1], which are certified by the state. Furthermore, providers will have to make available to clients a basic collection of security products and services and might be subject to greater responsibilities.

3. Strengthening IT security in the public administration.
   The German plan for strengthening IT security in the public administration includes the creation of a common, uniform and secure network infrastructure in the federal administration to serve as the basis for electronic audio and data communications.

4. Creation of a National Cyber Response Centre.
   The National Cyber Response Centre aims to optimize cooperation between state authorities, thus improving response to IT incidents. Information sharing on vulnerabilities, form of attacks and profiles of

[1] De-mail is a German government communication service similar to the Italian certified e-mail service (Posta Elettronica Certificata - PEC).

attackers allow the National Cyber Response Centre to analyze IT incidents and provide recommendations for action to be taken in response to incidents. To favor readiness for IT incidents, the National Cyber Response Centre will submit recommendations to the National Cyber Security Council both regularly and when specific incidents occur. In case of cyber security incidents that reach the level of a crisis the National Cyber Response Centre will directly inform the crisis management staff headed by the State Secretary at the Federal Ministry of the Interior.

5. Creation of a National Cyber Security Council.
   The National Cyber Security Council will coordinate preventive tools and the interdisciplinary cyber security approaches of the public and private sector. Several ministries of the state and representatives of the federal states (Lãnder) will participate in the council. Representatives from business and academia will be invited on specific occasions.

6. Effective crime control in cyberspace.
   The German strategic plan envisages the strengthening of the capabilities in fighting cyber crime of law enforcement agencies, the Federal Office for Information Security and the private sector. To deal with global cyber crime Germany will make an effort to achieve global harmonization in criminal law based on the Council of Europe Cyber Crime Convention, and will also examine whether new conventions on cyber crime should be adopted at UN level.

7. Effective coordinated action to ensure cyber security in Europe and worldwide.
   The German federal government recognizes the importance to conform to European and international standards related to cyber security. At European Union level Germany adopts measures based on an extension and moderate enlargement of the mandate of ENISA. Germany intends to shape its external cyber security policy so that German interests and ideas concerning cyber security will be pursued by international organizations, such as United Nations, OSCE, the Council of Europe, OECD and NATO.

8. Use of reliable and trustworthy information technology.
   Given the importance of availability and reliability of IT systems, Germany intends to increase research into IT security and critical information infrastructure protection, in particular, by further developing its technologies in these areas. Moreover, Germany approves diversity in technology, combining, when necessary, its own resources alongside those of its partners and allies, favoring the use of technologies certified by international standards.

9. Personnel development in federal authorities.
   One of the priorities of the Federal government is to examine whether authorities require additional staff to enhance cyber security. In order to improve inter ministerial cooperation it will favor personnel exchange between federal authorities, providing appropriate staff training measures.

10. Tools to respond to cyber attacks.
    In order to achieve an adequate preparedness against cyber attacks, the German Government recognizes the importance of the creation, in collaboration with the specific state authorities, of a collection of tools to effectively respond to cyber attacks.

The objective of the German government is the sustainable implementation of these strategic objectives to ensure freedom and prosperity in Germany. Technologies used in the area of IT security have short innovation cycles. Thus, the German Federal Government will periodically verify whether the objectives of the strategic plan have been achieved, under the control of the National Cyber Security Council, and will conform them, if necessary, to national and international requirements.

3.2 France

The French president first presented the French strategy on defense and national security in June 2008 with the French White Paper on Defense and National Security. Given the unexpected emergence of cyberspace in the field of national security, in 2009 the government set up the French Network and Information Security Agency (Agence nationale de la sécurité des systèmes d'information - ANSSI)[2]. In 2010 the president decided to give the agency, in addition to its security role, the responsibility for the defense of information systems. Four strategic objective characterize the French strategy [21]:

[2] Decree No. 2009-834 of 7 July 2009 creating the French Network and Information Security Agency* (ANSSI).

- Becoming a cyber defense world power;
- Safeguarding France's ability to make decisions through the protection of information related to its sovereignty;
- Strengthening the cyber security of critical national infrastructures;
- Ensuring security in cyberspace.

In order to reach these objectives, seven area of action have been identified by the French strategy:

- Effectively anticipate and analyze the environment in order to make appropriate decisions. Monitor the latest technology developments in order to understand and even anticipate the actions of public or private actors.
- Detect and block attacks, alert and support potential victims. France is developing detection capability for attacks on information systems deployed within the ministry networks for enabling the personnel to be alerted, assess the nature of attacks and create countermeasures. ANSSI has been equipped with an operations room to meet the challenges.
- Enhance and perpetuate French scientific, technical, industrial and human capabilities in order to maintain independence. Driving forward research into cryptology, formal methods and other security-related areas, creating cyber defense research centers in collaboration with industrial partners. Strategic investment funds will be provided by the state in order to promote the strengthening of industry.
- Protect the information systems of the nation and of the critical infrastructures to ensure better national resilience. The French strategy on security products and components has been redefined in order to take account of France re-joining NATO integrated command. Robust authentication systems will be integrated in the ministerial networks having a significant impact on the level of security. A public-private partnership will be set up in order to enhance the security of information systems of operators of critical infrastructures. The operators will benefit from the information gathered by the state on threat analysis and the State will be able to ensure the appropriate level of protection of the infrastructure that is crucial to keep the country running properly.
- Adapt French legislation to incorporate technological developments and new practices: new rules to protect information systems and alert government authorities in case of incidents regarding operators of electronic communications. Enforcement of the General Security Framework in order to raise the protection level of the information systems of the public authorities.
- Develop international collaboration initiatives in the areas of information systems security, cyber defense and the fight against cyber crime in order to better protect national information systems: promote the sharing of essential data (information on vulnerabilities, services, threats) by establishing a wide network of foreign partners.
- Communicate, inform and raise understanding by the French population of the extent of the challenges related to information systems security: ensure the awareness and motivation of individuals and organizations; ANSSI will conduct appropriate communication campaigns targeting the general public and companies.

3.3 United Kingdom

The UK strategy builds on more than ten years of development. The first step was carried out in 2001 by the Communications-Electronics Security Group (CESG). This group recognized the increasing use of online services required the development of security measures to protect data and recommended the appointment of a central sponsor for information assurance of government data. Therefore, the government published its first national strategy in 2004, in which a network of Senior Information Risk Owners was established.

In 2009, the government recognized the risk of cyber threats and published its first cyber security strategy. In 2010 the government ranked cyber attacks as a key risk for national security and announced a fund of 650 million pounds for a four-year National Cyber Security Programme. Since 2011 the Cabinet Office has been responsible for cyber security. The most recent strategy was published in 2011 and set out how the government planned to deliver the National Cyber Security Programme until 2015. Four objectives characterize the strategy [**?**]:

- Tackling cyber crime and making the UK one of the most secure places in the world to do business;
- Making the UK more resilient to cyber attack and better able to protect its interests in cyberspace;
- Helping shape an open, stable and vibrant cyberspace which the UK public can use safely and which supports an open society;
- Building the UK's cross-cutting knowledge, skills and capability to underpin all cyber security objectives.

Six central departments and nine government organizations are responsible for delivery: Home Office, Serious Organized Crime Agency, Child Exploitation and Online Protection, Police Central e-crime Unit, Police force, National Fraud Authority, Department for Business, Innovation and Skills, Technology Strategy Board, UK Trade and Investment, the Cabinet Office, the Intelligence and Security Agencies, Ministry of Defense, Department for Culture, Media and Sport, Foreign and Commonwealth Office.

Concerning critical infrastructure protection in the United Kingdom, everything is delegated to the Centre for the Protection of National Infrastructure (CPNI). CPNI protects national security by providing protective security advice, in terms of personnel security, physical security and cyber security. CPNI takes into special consideration the policy context. Policy considerations are one of the building blocks of the mechanism of protective security advice provided by CPNI. In particular, several government policies influence CPNI's work:

- National security strategy: Establishes the strategies aimed at reacting effectively and rapidly to security threats, such as: acts of terrorism, attacks on UK cyberspace, natural accidents and disasters and international military crises that involve the United Kingdom and its allies.
- Strategic defense and security review: Establishes how the objectives of the national security strategy have to be pursued.
- Counter terrorism strategy: The UK's counter terrorism strategy is developed in four main directions: prevent, pursue, protect and prepare. CPNI's work falls within the "protect" category which aims at reducing the vulnerability of the UK to terrorist attacks.
- Cyber security strategy (as described above).
- National Risk Register: The National Risk Register is the public version of the confidential National Risk Assessment that registers the events that may cause damage to people or property, or disruption of essential services. Events are categorized in three broad areas: natural events, major accidents, malicious attacks.
- Resilience of infrastructure to natural hazards: In order to enhance critical infrastructure and essential services resilience to disruption due to natural hazard, the Civil Contingencies Secretariat within the Cabinet Office developed the Critical Infrastructure Resilience Programme (CIRP).

CPNI actively cooperates with partners in the public and private sector. In the public sector CPNI works closely with the National Technical Authority for Information Assurance (CESG) and, within the police, with the National Counter Terrorism Security Office (NaCTSO) and with the Counter Terrorism Security Advisor (CTSA) network. Government departments are responsible for taking appropriate actions to improve security in their respective sectors. These departments are also responsible for the identification of critical infrastructure in their sectors in cooperation with CPNI and sector organizations. The departments involved are:

- Department for Business, Innovation and Skills;
- Department of Health;
- Department for Communities and Local Government;
- Department for Transport;
- Home Office;
- Department for Energy and Climate Change;
- HM Treasury;
- Department for the Environment, Food & Rural Affairs and Food Standards Agency;

- Cabinet Office.

Concerning cyber security, the U.K.'s Government established in 2010 the Cyber Security Operations Centre (CSOC) and the Office of Cyber Security & Information Assurance (OCSIA). CPNI cooperates with CSOC, OCSIA and CESG in order to conduct the cyber security program for the UK government. In the private sector, CPNI interacts with the organizations that operate in the national infrastructure. The relationships, established over the years, between CPNI's security advisers and security managers in several sectors enable information sharing between trusted entities and, when appropriate, sharing of vulnerabilities and effective response measures in order to improve the protection of the national critical infrastructure and private organizations. Moreover, CPNI has established a partnership program, Risk Management Delivery Group, which aims to promote strong links between the principal UK consultancy partners.

3.4 USA

In May 2009, President Obama declared his intention to make cyber security a priority for his administration. This brought about the publication of a document entitled "Cyber Security Policy Review" (CPR) [47]. In particular this document identifies 10 short-term actions:

1. Appointment of a cyber security policy official responsible for coordinating the nation's cyber security policies and activities.
2. Preparation for the president's approval of an updated national strategy to secure the information and communications infrastructure.
3. Designation of cyber security as one of the president's key management priorities and establishment of performance metrics.
4. Designation of a privacy and civil liberties official to the NSC cyber security directorate.
5. Conductng interagency-cleared legal analyses of priority cyber security related issues.
6. Initiating a national awareness and education campaign to promote cyber security.
7. Development of an international cyber security policy framework and the strengthening of international partnerships.
8. Preparation of a cyber security incident response plan and initiation of a dialogue to enhance public-private partnerships.
9. Development of a framework for research and development strategies which focuses on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure.
10. Building a cyber security based identity management vision and strategy, and leveraging privacy-enhancing technologies for the nation.

The achievement of such objectives must respect the Comprehensive National Cybersecurity Initiative (CNCI) [48], launched by President George W. Bush in January 2008, which consists of a set of initiatives aimed at strengthening US cyber security. President Obama established that CNCI had to be included and extended in the updated strategy of national cyber security, and that it would play a key role in the realization of the 10 objectives. During the 14 months following the issue of CPR many of the objectives were achieved [46]:

- President Obama appointed a cyber security coordinator at the head of the Cyber Security Directorate created within the National Security Staff (NSS). This coordinator works closely with the Office of Management and Budget and the Office of Science and Technology Policy.
- The Cyber security Directorate started the development of an updated cyber security strategy that expands and implements the strategy envisaged by CPR and CNCI.
- A continuous and real-time monitoring of federal networks has been introduced, thus enabling faster detection of vulnerabilities and more effective infrastructure protection.
- According to CPR, a privacy and civil liberties official has been designated within the NSS.

- The National Initiative for Cybersecurity Education (NICE) has been released to improve the recruitment, training, and retention of cyber security professionals, to raise public awareness in cyber security, and to enhance cyber security education by expanding the education programme of CNCI.
- The United States is working to strengthen cooperation and dialogue with international partners. In cooperation with allied countries, the United States has taken on a leading role in international organizations, such as the United Nations, to make cyber security an international priority.
- The National Cyber Incident Response Plan (NCIRP) has been developed to enable a coordinated national response to cyber incidents.
- The administration has developed a research and development strategy based on three main themes: moving targets (systems that change continuously to increase their complexity, thus limiting attackers and exposition to vulnerabilities), tailored trustworthy spaces (trusted environments that allows the definition of tailored requirements) and cyber economic incentives (incentives to adopt appropriate cyber security solutions for individuals and organizations).
- A draft "National Strategy for Trusted Identities in Cyberspace" (NSTIC), aimed at reducing cyber security vulnerabilities through the use of trusted digital identities, has been released.

With regard to the US roadmap, in February 2013, President Obama issued an executive order to further improve the management of critical infrastructure cyber security. The aim of this executive order is to establish a new partnership with the critical infrastructure owners and operators in order to increase cyber security information sharing and collaboratively develop risk-based standards.

Information sharing on cyber security issues, such as suffered and foiled attacks, threats and vulnerabilities, between the public and private sector is the key factor in the improvement process envisaged by the executive order. The US government is responsible for improving such exchange of information in terms of volume, timeliness and quality of information shared with the private sector, thus enabling entities of the private sector to better protect themselves against cyber threats. As a result of the executive order the Secretary of Homeland Security, the Attorney General[3] and the Director of National Intelligence will be responsible for ensuring the timely production of specific unclassified reports of cyber threats to the US homeland. Moreover, classified reports will be delivered to authorized critical infrastructure entities. The Secretary of Homeland Security and the Attorney General, in coordination with the Director of National Intelligence, will be also responsible for setting up a system to track the production, dissemination and disposition of the reports. The aim is to maximize the utility of information sharing related to cyber threats and attacks.

The executive order also addresses the protection of privacy and civil liberties. Important roles in this context are covered by the Chief Privacy Officer and by the Officer for Civil Rights and Civil Liberties (of the Department of Homeland Security). They are responsible for assessing the privacy and civil liberties risks of the functions performed by the Department of Homeland Security and for identifying and report ways to minimize such risks in a publicly available report to be released within one year from the issue of the executive order. In the production of the report the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties will consult the Privacy and Civil Liberties Oversight Board and the OMB.

The executive order issued by President Obama also envisages the creation of a Cyber Security Framework aimed at reducing cyber risks to critical infrastructure. The Secretary of Commerce will direct the Director of the National Institute of Standard and Technology in the development of the framework. The Cyber Security Framework will include a collection of standards and procedures to align policy, business and technological approaches to better address cyber risks. The framework will also include as much as possible industry best practices and will be available in final version by February 2014. The Secretary of Homeland Security will support the adoption of the framework by the owners and operators of the critical infrastructure and other interested entities.

[3] In the federal government of the United States, the Attorney General is a member of the Cabinet and as head of the Department of Justice is the top law enforcement officer and lawyer for the government (Wikipedia).

CHAPTER

4 Analysis of the Italian Cyber Security Landscape

In order to conduct a deep analysis of the Italian cyber security situation, the Research Center of Cyber Intelligence and Information Security of Sapienza Università di Roma submitted an anonymous questionnaire to 68 organizations sensitive to cyber attacks according to the definition given in Section 1.3. A successful attack on any of these organizations would produce an impact that goes beyond the same organizations boundaries and affects other organizations or society as a whole. A total of 28 fully filled-in questionnaires were collected.

The organizations targeted by the study where then clustered in four groups on the basis of the organization competences and the economic sectors they act within:

- Public Administrations (PA): public administrations are concerned with the implementation of government policies at national, regional and local levels. Ministries are examples of central public administrations. This group includes local administrations (e.g., municipalities), central administrations (e.g., ministries) and government agencies;

- (Public) Utilities: any organization which provides services to the general public, although it may be privately owned, participates to this group. Utilities include electricity, gas, telephone and water;

- Financial: a financial organization focuses on dealing with financial transactions, such as investments, loans and deposits. Conventionally, financial organizations include banks, trust companies, insurance companies and investment dealers.

- Industrial: companies that consider their intellectual property, such as patents, data, specific non-public management processes, and other confidential information, a critical asset to be protected against possible attacks. In this study mainly large IT industries and large Italian manufacturing industries were considered.

The questionnaire was sent to organizations in July 2013, and the results were collected until September 2013. Details about each group are reported in Table 4.1 while Figure 4.1 depicts the category separation among the returned questionnaires.

Table 4.1 shows that the percentage of filled-in questionnaires was between 41% and 50% for all groups except the financial one, which returned only 35% of them. The average percentage of returned questionnaires was 42,23%. The third column of Table 4.1 reports how many different companies were contacted. Some big companies (with more than 10.000 employees), in fact, have distinct areas with distinct systems and perhaps a distinct Coordinator of Information System Security (CISO), and were thus asked to fill-in more than one single questionnaire.

Organizations of different sizes were contacted in order to better cover the whole Italian landscape. In particular, among those that returned the questionnaires, 20% of the organizations have up to 1000 employees; 36.7% between 1000 and 10000 employees; 30% between 10000 and 100000 and the remaining 13.3% have more then 100000 employees. Among the contacted organizations, 50% of them operate only within the Italian territory while the remaining 50% operate outside of the frontier, at a European or worldwide level. It can also be observed that at least 75% of the organizations have a central element responsible for security. Taking into account the sample analyzed, the results presented in the following sections of this chapter are not meant to

Table 4.1: Sent/Received Questionnaires per group.

Target groups	**Questionnaires sent**	**Questionnaires returned**	**Number of organizations**	**% of returned questionnaires**
PA	31	13	26	41.9%
Utilities	8	4	7	50%
Financial	17	6	17	35.3%
Industrial	12	5	12	41.7%
Total	68	28	62	Avg. 42.23%

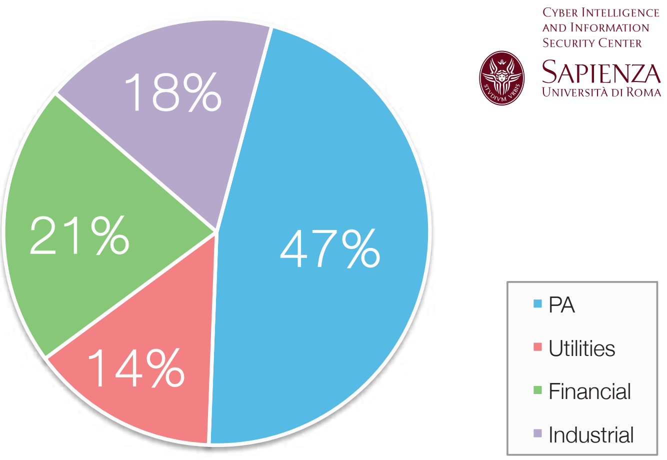


Figure 4.1: Percentage of questionnaires returned per group.

have statistical significance, especially in terms of groups representativeness. Rather, their aim is to provide a snapshot of the degree of risk perception and cyber security measures currently implemented in Italy.

4.1 Organization recognition of being a critical infrastructure

It should be noted that only a fraction of the organizations that participated in the analysis consider themselves to be critical infrastructures. The breakdown of the results on this point are reported in Figure 4.2. The graph shows that utilities fully recognize their role as critical infrastructure. This result was expected as this group is recognized as critical by the European Union Directive 2008/114/EC [20].

Half of the PAs recognize themselves critical infrastructure; however, we can further divide this result by grouping PAs in three subgroups, namely government agencies, central administrations and local administrations and then analyzing the awareness at this finer level of detail. As Figure 4.3 shows, a large fraction of government agencies and central administrations, consider themselves as critical infrastructure, while local administrations acknowledge that a failure of their services caused by cyber attacks would probably have a limited impact from a national standpoint. The industrial group reported a mixed level of awareness; subdividing group results, it is possible to see that companies that responded affirmatively to the question usually provide fundamental services to other organizations that manage the critical infrastructure. Other companies were mainly targeted as they manage important intellectual assets that should be protected from cyber attacks; however, these organizations do not consider the protection of these assets as a national problem necessary for defending Italian economic interests.

Finally, it is important to underline the fact that almost none of the organizations pertaining to the financial group recognized themselves as critical infrastructure. This could be seen as a consequence of the fact

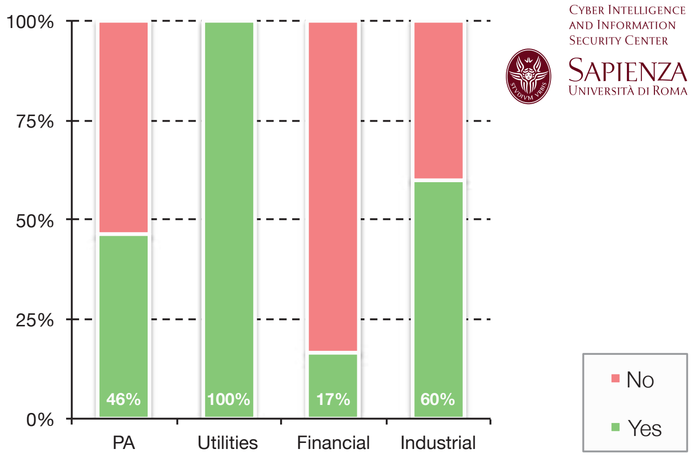


Figure 4.2: Question #1.1.5 - Awareness of being critical infrastructure (per group).

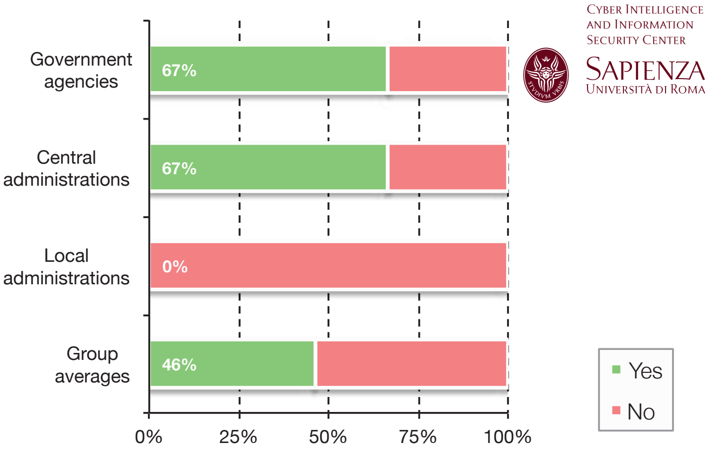


Figure 4.3: Question #1.1.5 - Awareness of being critical infrastructure (breakdown for the PA group).

that the financial system is not officially considered as a critical infrastructure at the European level. However, recent facts (e.g. the Lehman Brothers crack or the Royal Bank of Scotland IT failure [50]) clearly show how severe failures of financial organizations may easily have a broad impact at both the national and international level. This latter aspect, in fact, has been recognized by two of the financial organizations that participated in the survey.

4.2 External dependencies

The questionnaire contained some questions to asses the existence of organizational inter-dependencies with third parties. The first question of the set was, "Is your company using (or planning to use) cloud services?" Figure 4.4 shows the distribution of responses. A majority of the respondents use cloud services in their organization. The responses breakdown (shown in the left side of the figure) reports similar behavior with the exception of financial players that use cloud services less than companies belonging to other group.

The next question aimed at understanding if such cloud services support core business processes that are necessary to deliver critical services. Answers to this question are depicted in Figure 4.5. A sizable share of the

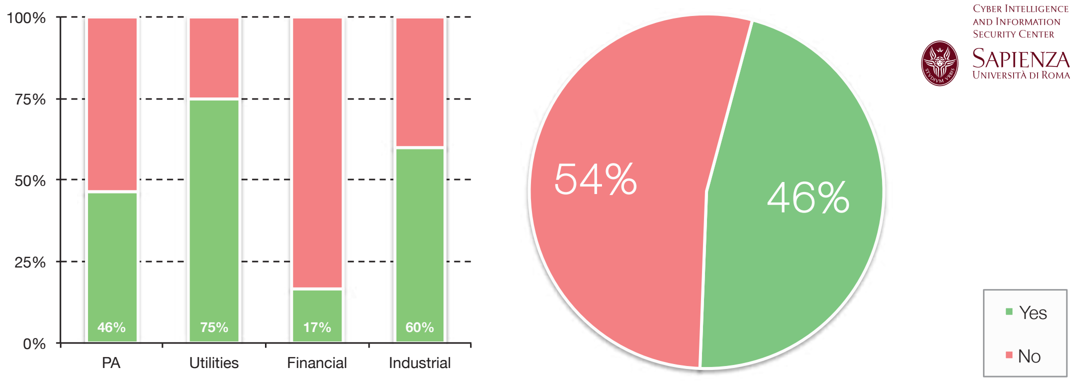


Figure 4.4: Question #1.2.1 - "Is your company using (or planning to use) cloud services?" Left chart shows answer distribution by group. Right chart depicts the overall picture.

interviewed companies did not answer this question; this is due to the fact that the question is strictly related to the previous one. A key point is that there is a significant part of respondents (18%) that use cloud services to support their core business and to deliver critical services. This percentage is fairly similar for all groups, except the financial one where no organization brings critical services in the cloud.

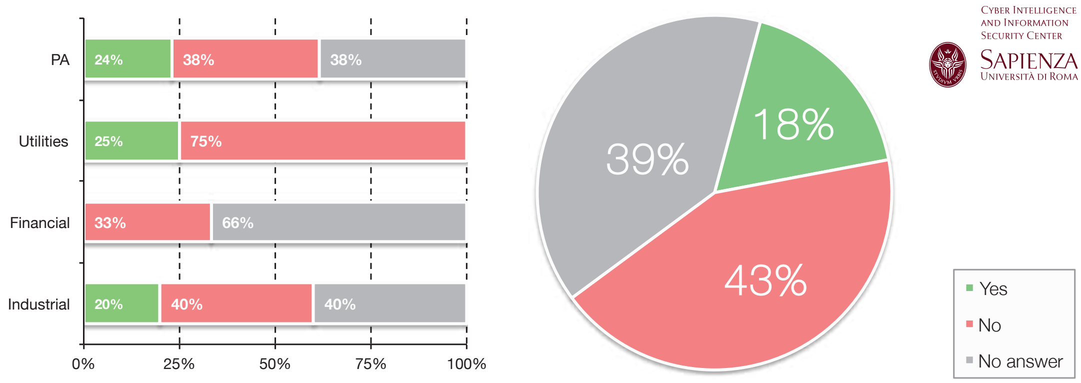


Figure 4.5: Question #1.2.2 - "Do cloud services support core business processes that are necessary to deliver critical services?" Left chart shows answer distribution by group. Right chart depicts the overall picture.

Continuing the evaluation of external dependencies, the questionnaire included the following question, "Is it possible that an ICT service failure in one (or more) third-party company will have a significant impact on your company?" Results are reported in Figure 4.6. In this case a majority of the organizations answered affirmatively, indicating that they depend on an external ICT system. Only a small fraction (11%) is free from this kind of dependency. Another 11% does not know if a failure of a third-party ICT system could impact its organization.

The next question asked, "Do you know if your software providers are following a strategic approach to address application risks in each phase of the application development process?" In this way it was possible to evaluate if the strategy behind externalization of software development takes into account security aspects. The majority of respondents (Figure 4.7)does not know if their software providers follow a specific approach to address application risks. 50% of respondents think that their providers probably implement some sort of security strategy during the development phases. Only 14% is certain about the conduct of their software providers.

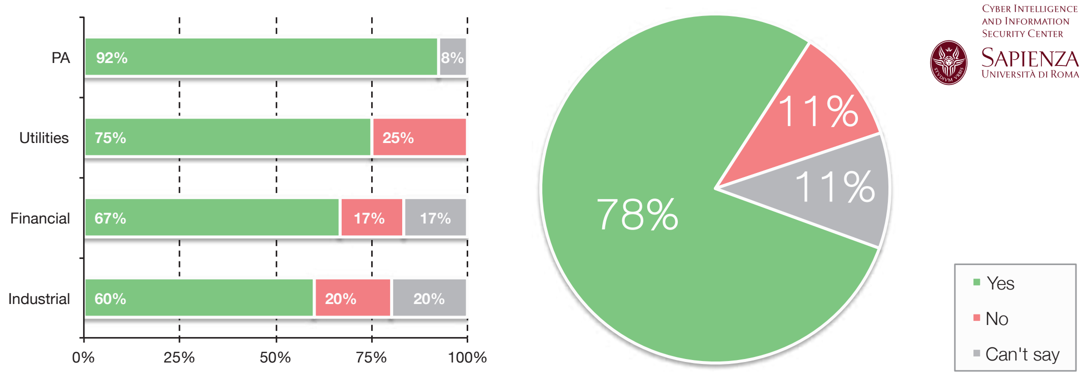


Figure 4.6: Question #1.2.5 - "Is it possible that an ICT service failure in one (or more) third-party company, will have a significant impact on your company?" Left chart shows answer distribution by group. Right chart depicts the overall picture.

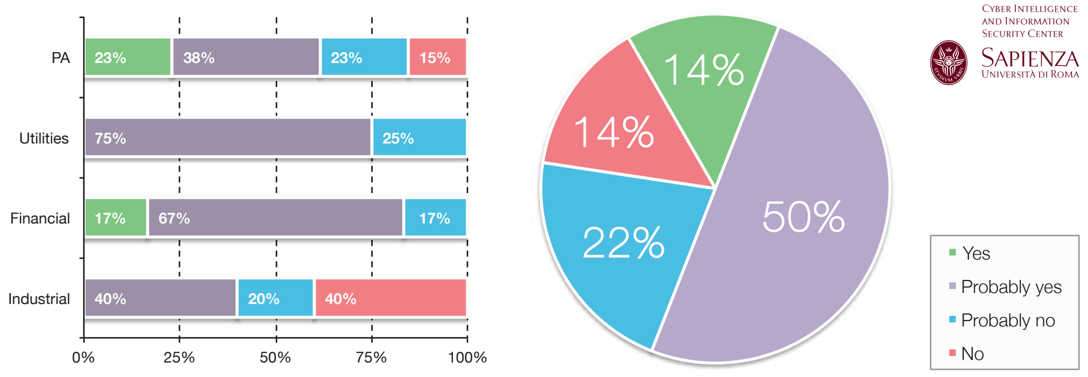


Figure 4.7: Question #1.2.6 - "Do you know if your software providers are following a strategic approach to address application risks in each phase of the application development process?" Left chart shows answer distribution by group. Right chart depicts the overall picture.

4.3 Anomalies and cyber attacks

Figure 4.8 reports the percentage of organizations, divided by group, which regularly register anomalies. Anomalies refer to events that are not cyber attacks but that go beyond the normal behavior of the organization infrastructure. It was revealed that utilities are the organizations that record the maximum number of anomalies. All the interviewed organizations belonging to this group acknowledged the presence of anomalies within their systems. On the contrary, the financial group seems to be the one that is least affected by such events (67%), followed by the public administration (77%) and then the industrial group (80%).

Figure 4.9 shows the percentage of interviewed organizations that have been subject to cyber attacks conducted by insiders. This could be an employee or any contract or staff member (e.g. cleaner, caterer, security guard) who has authorized access to the organization premises. The utility group is clearly a common target for these kind of attacks. Indeed, 50% of the interviewed organizations confirmed that they have been targeted by an insider at least once. However, it is worth noticing that this group is also the one that best responded to these threats. None of the reported attacks, in fact, were successful. On the contrary, financial and public administration have been hit by successful internal attacks. In particular, in the financial group, half of the tentative internal attacks were successful, while one attack in four against the public administration achieved its target. Interviewed companies in the industrial group did not declare any attack conducted by insiders. Many studies are now analyzing how to increase the employees trustworthiness (e.g., [4]).

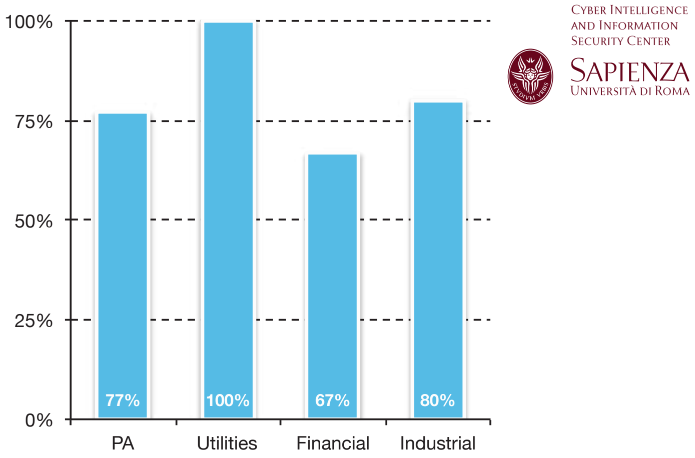


Figure 4.8: Question #1.3.10: Companies regularly registering anomalies per group.

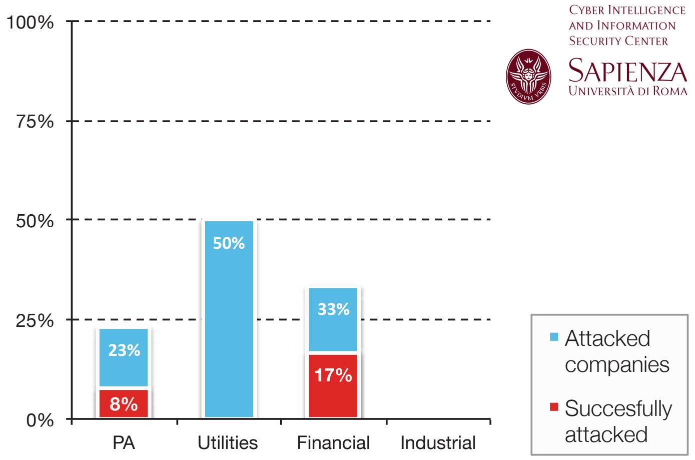


Figure 4.9: Question #1.1.5 - Companies that have been attacked by an insider (per group).

Figure 4.10 reports the percentage of organizations that have been the target of an external cyber attack per group. By analyzing the data, it can be seen that all financial organizations have been attacked and attacks have been successful in 17% of cases. The public administration group is the one exhibiting the highest number of successful attacks 62%. Probably, this is an indicator of poor security policies. Conversely, the industrial group is the least attacked. Indeed, only 40% of the interviewed companies have been attacked, and half of the attacks were successful. The aim of the external attacks is reported in Figure 4.11.

From the chart, it is clear that financial organizations are attacked in order to subtract data, impair the availability of their services and to tamper with data. Protest is by far the main motivation for attacks that target the public administration. Surprisingly, utilities do not declare attacks aimed at impairing service availability while industrial group does not suffer protest attacks.

4.4 Defensive measures

Defense from insider threats

A set of questions was designed to asses the measures organizations implement in order to avoid possible misuse of organization data or attacks from internal employees. Each respondent had the possibility of se-

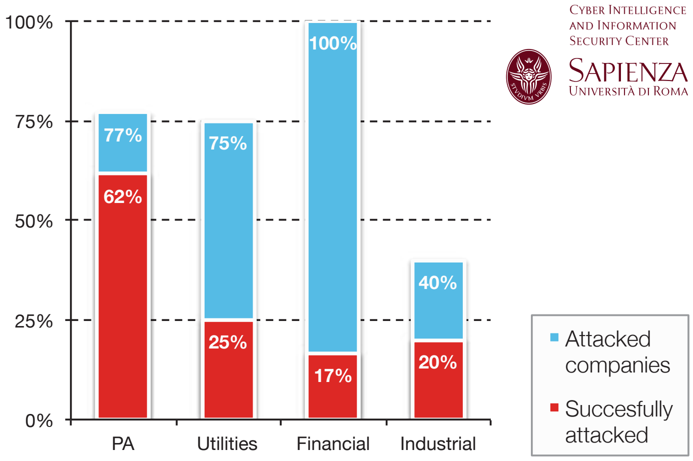


Figure 4.10: Question #1.3.5 - Companies experiencing external cyber attacks (per group).

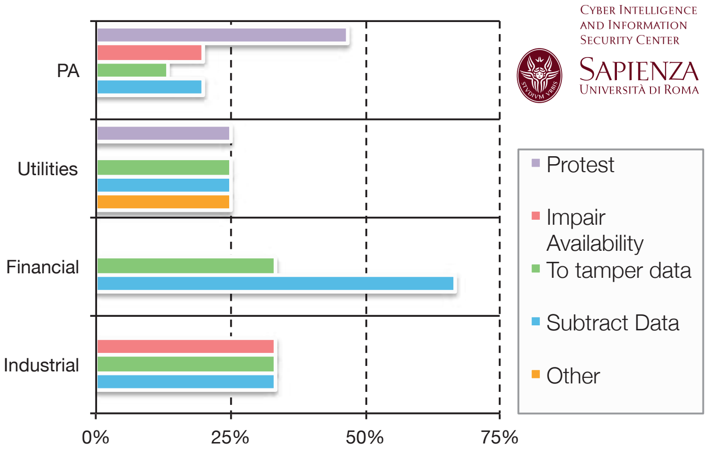


Figure 4.11: Question #1.3.7 - Aim of external attacks (per group).

lecting none, one or more countermeasures to fight internal misuse. Thus, Figure 4.12 depicts as a percentage the number of times a given countermeasure has been selected by the respondents with respect to the total number of countermeasures selected by all respondents. The two most common measures implemented are employee training and information classification/access control policies (both more than 30%). Restrictions on the use of personal emails and/or cloud services from the inside of the organization's network and restricted use of personal equipment are both 15%.

The adoption rate of each reported measure was also computed. Adoption rates were additionally computed per group. For example, 100% adoption of a measure m (e.g. employee training) in a group means that all organizations belonging to that group implement m. Figure 4.13 shows adoption rate for each countermeasure and for each group. Results show that the PA group focuses on classification and employee training, almost neglecting other measures. The financial and industrial groups are more willing to adopt other measures such as restricting the access of personal mail or cloud services and forbidding the use of personal equipment at work. Utilities consider training of employees as the main measure and there is a high percentage of them that restrict use of email/cloud. Finally it should be pointed out that one of the primary measures for counteracting internal misuse, employee training, is also perceived by the respondents as one of the things that they can/would like to improve in order to better protect their organization (See Section 4.7).

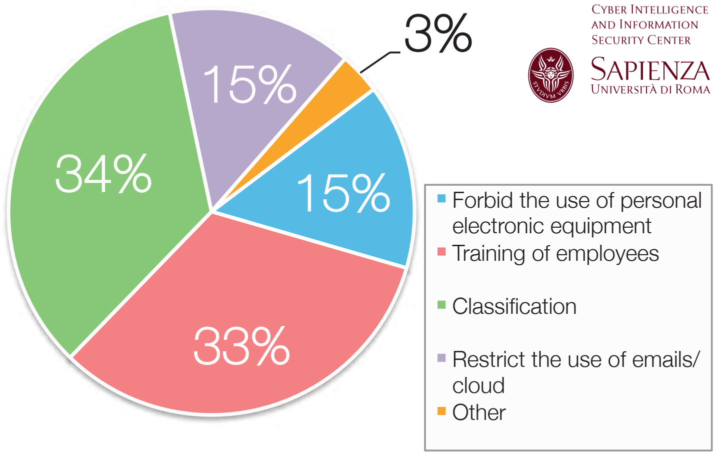


Figure 4.12: Question #1.4.8 - “Which of the following measures to protect data and critical systems from misuse by employees does your company implement?” Overall internal misuse countermeasures adoption.

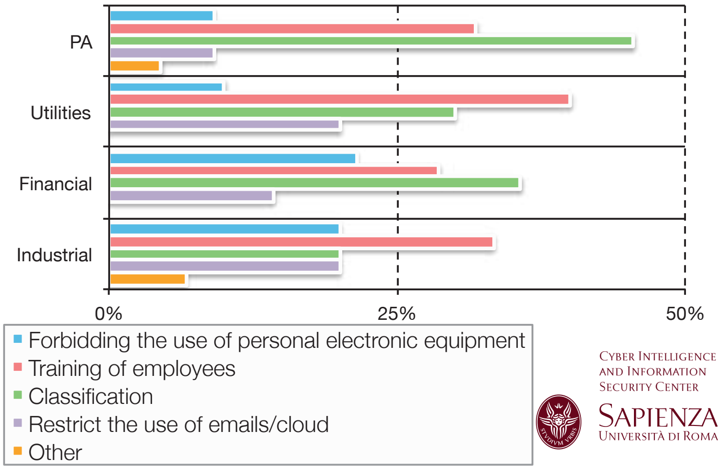


Figure 4.13: Question #1.4.8 - “Which of the following measures to protect data and critical systems from misuse by employees does your company implement?” Adoption rate for each of the countermeasures per group.

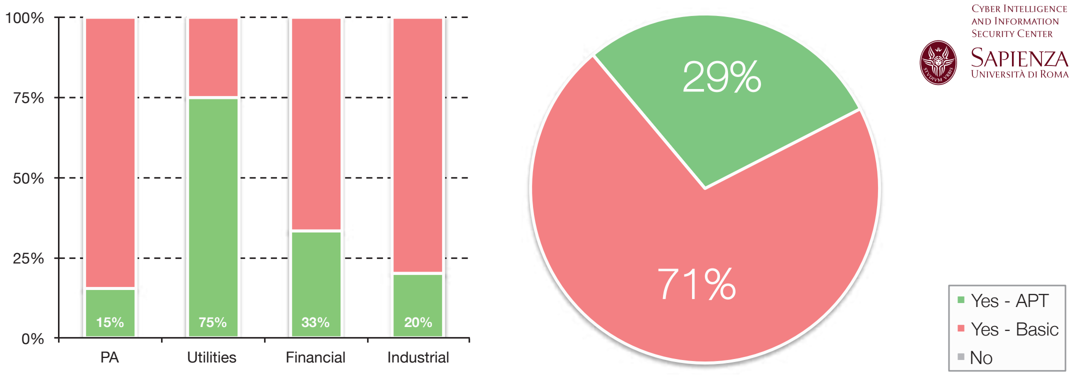


Figure 4.14: Question #1.4.5 - “Do you have the infrastructure to detect active attacks?” Left chart shows answer distribution by group. Right chart depicts the overall picture. Responses: “Yes basic" We have an infrastructure to detect attacks that are based upon standard malware or basic techniques (sql-injection, known computer worms, phishing ecc), “Yes-APT" We have an infrastructure to detect sophisticated attacks carried out by an advanced adversary that uses 0-day vectors (Advanced Persistent Threats).

Defense from external threats

One section of the questionnaire was designed to assess the security measures implemented. Specifically, if the organization has measures to detect active attacks (see Figure 4.14). 71% of the organizations declare they own an IT infrastructure which is able to detect simple attacks. The remaining 29% of the organizations declare they own an IT infrastructure that is capable of detecting Advanced Persistent Threats (APTs[1]). This percentage of basic setups is 85% for the PA and 80% for the industrial group. 75% of the organizations belonging to the utilities group declares they own an IT infrastructure able to detect APTs.

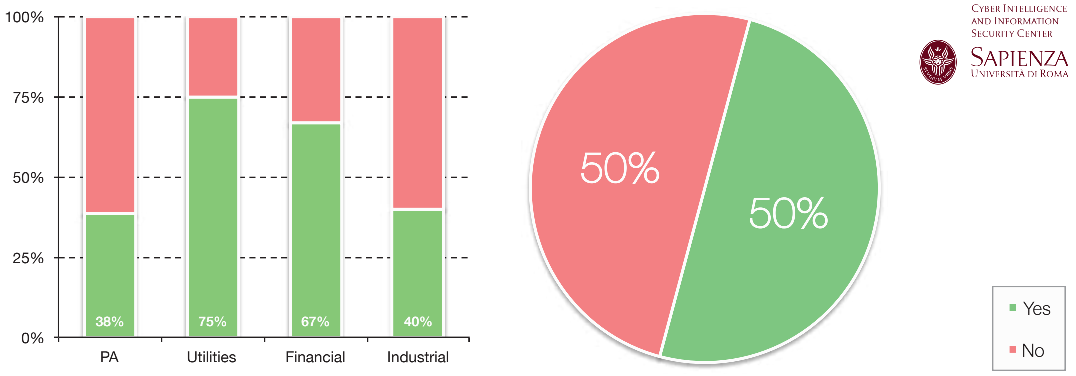


Figure 4.15: Distribution of response to question, “Are your web applications tested using standard methodologies for security assessment of webapps?” Left chart is divided by group. Right chart depicts the overall picture.

Given the widespread adoption of web applications, all respondents claimed to use web applications to support their business, the survey asked about their security assessment. The results are presented in Figure 4.15. Roughly half of the respondents do not test their web application for security, at least not using standard and well established methodologies. The situation is common to all groups with slightly better results for financial and utilities groups. Testing of web applications is a key point for the security of a company, since such applications have been proven as a high risk target for attacks.

[1] Advanced Persistent Threat `https://en.wikipedia.org/wiki/Advanced_persistent_threat`

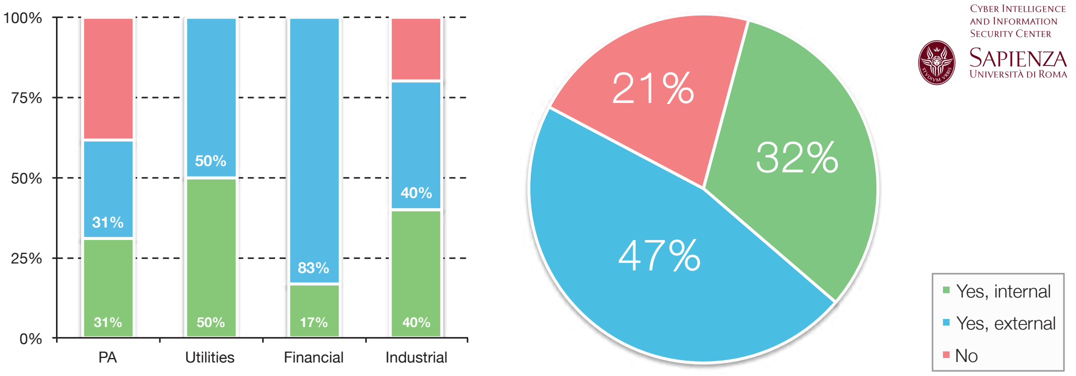


Figure 4.16: Distribution of response to the question, "Does your company actively audit (penetration testing) the security of your ICT systems?" The chart on the left is divided by group, that on the right is the overall picture.

Figure 4.16 reports results about the diffusion of penetration testing methodologies. Overall, 80% of the participants actively test their systems and 47% of the respondents rely on an external company to assess the security of their infrastructure. Examining the individual groups, it can be seen that the PA group is the one which executes the least active testing with roughly 35% of respondents admitting to not running any form of penetration testing. The financial group is characterized by 83% of the penetration tests being executed by external companies while utilities reach a balance of 50% between internal and external penetration test activities. All organizations in both groups declare to execute such activity.

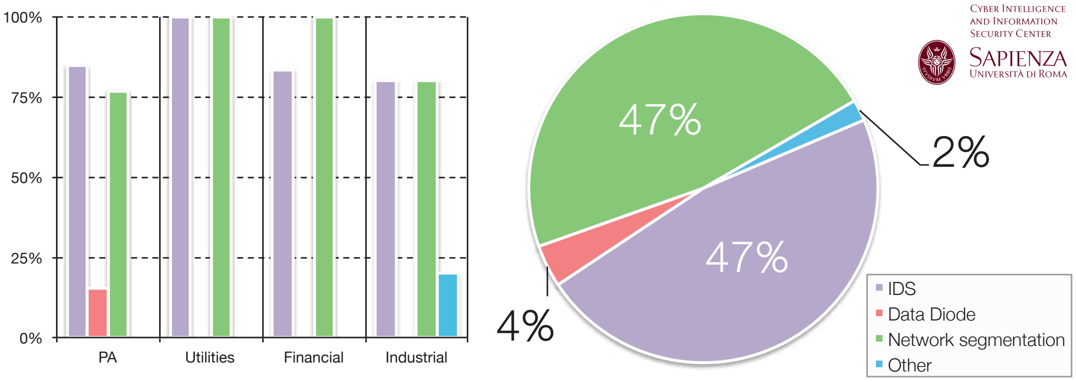


Figure 4.17: Questions #1.4.13, #1.4.14 - "Do you have measures that prevent the spread of an attack if your systems are penetrated? If so, what kind of measures?" Left chart shows answer distribution by group. Right chart depicts the overall picture.

Figure 4.17 shows measures that can be used to block the spread of an attack. It is clear that the majority of participants (in all groups) have some form of protection to prevent an attack spreading. In detail, the sum of network segmentation and IDs constitutes 94% of the adopted measures, a ratio that is maintained group by group, while different measures are adopted by just 5% of the participants.

As a final point, the capabilities of an organization to mitigate the effect of an attack was investigated. (Question #1.5.1 "Do you have processes and resources to respond to cyber security incidents?"). Results are in Figure 4.18. The PA group was the only one to admit that some of them, 25%, do not have the capabilities to respond to a cyber security incident. The utilities group claims to be autonomous with 100% of the interviewed believing that they can cope with a cyber security incident. The financial group responds to cyber security incidents mainly with internal resources (67%) while the opposite is true for industrial group where 60% of resources are external.

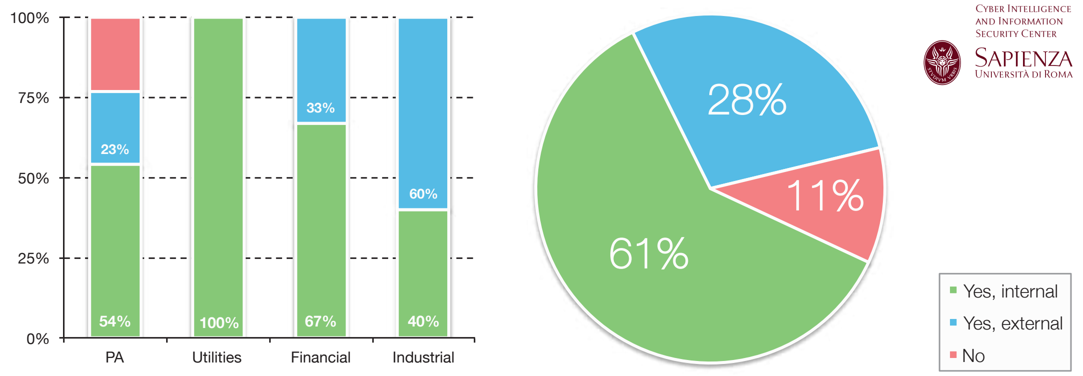


Figure 4.18: Question #1.5.1 - "Do you have processes and resources to respond to cyber security incidents ?" Left chart shows answer distribution by group. Right chart depicts the overall picture.

4.5 Recovery capabilities

A set of questions to assess the capacity of an organization to recover from a significant cyber security incident was designed into the questionnaire (Figure 4.19). The majority of respondents in the PA group are quite confident about the possibility to recover from a cyber attack. Financial and utilities groups also share a very high percentage of positive answers. This confidence decreases for other groups arriving at a minimum for the industrial group, in which 40% of the respondents admit to not having the capabilities to autonomously recover from a significant attack. This is probably due to the fact that PA recovery is (most of the times) operationally simpler than in other groups where recovering a service could take much more time due to potentially longer supply chains.

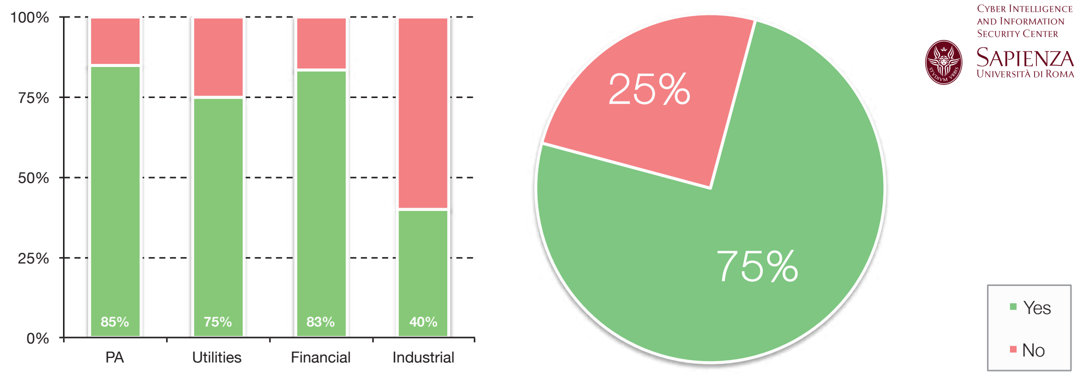


Figure 4.19: Question #1.5.2 - "Do you have processes and resources to recover from a significant cyber security incident ?" Left chart shows answer distribution by groups. Right chart depicts the overall picture.

Figure 4.20 refers to the adoption of a disaster recovery plan per group. It can be noticed that the financial and utilities groups seem to be those that most perceived the necessity of such a plan. Indeed, all the companies in these groups already have a disaster recovery plan, or are going to implement one. Not all the public administration group, instead, has a disaster recovery plan or the intention to implement one in the near future, regardless of the legislative constraints they are subject to. Surprisingly, 25% of the interviewed companies in the industrial group seem not to be interested in disaster recovery.

Figure 4.21 reports the distribution of the seven tiers of disaster recovery [35] among the companies that currently implement it. It can be noticed that more than 50% of the companies implement a Tier 4 disaster recovery plan, that assures a fast recovery time. More than 17% implement the highest available tier, which allows little or no data loss.

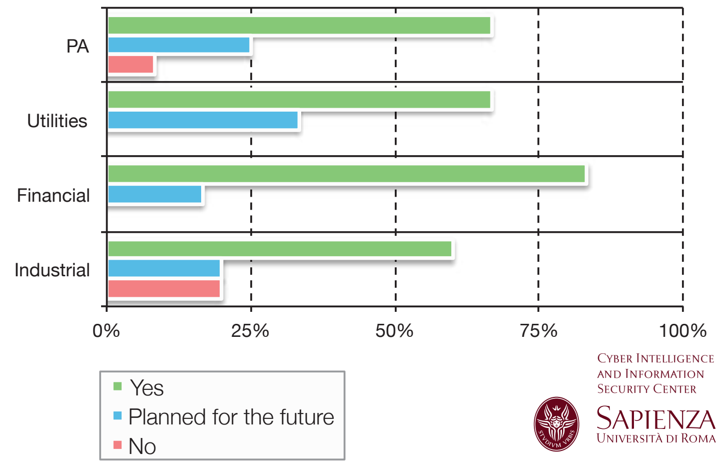


Figure 4.20: Question #1.2.4 - “Do you have a disaster recovery plan that allows your company to operate in case of a partial or complete failure of your ICT infrastructure?"

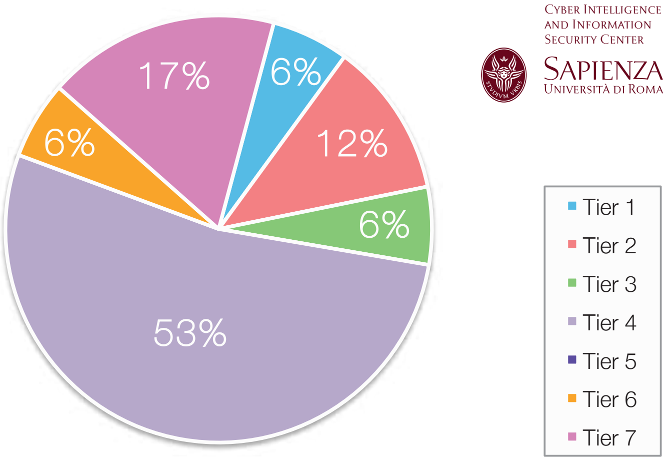


Figure 4.21: Question #1.2.4 - Disaster Recovery Tiers.

4.6 Policies

One section of the survey was targeted at assessing the adoption of policies by respondents. They were asked about the adoption of specific policies (ISO/IEC 27001, ISO/IEC 27005:2008, ISACA Risk it) for security and risk management, and about the adoption of an Information Security Management System (ISMS). Roughly half of the respondents implement some form of ISMS (see Figure 4.22). The same result is evident for the single groups. Public administration and industrial groups show the lowest adoption of ISMS. The utility and financial groups are the ones with the widest adoption (above 75%). For the ISO/IESC 27001 standard, adoption is greater in the industrial and financial fields and less in the utilities and PA groups. Results are shown in Figure 4.23.

The scenario changes when asked about the adoption of an Operator Security Plan, a measure that is requested by the European Council Directive 2008/114/EC. In this case the overall situation shows a general adoption by 18% of the interviewed companies. This standard is largely adopted by organizations belonging to the utilities group (50%). For the other groups, the standard is adopted by a number of organizations that is always less than or equal to 20% (see Figure 4.24). Finally respondents were asked if they keep their Operator Security Plan updated. The outcome of this question is reported in Figure 4.25).

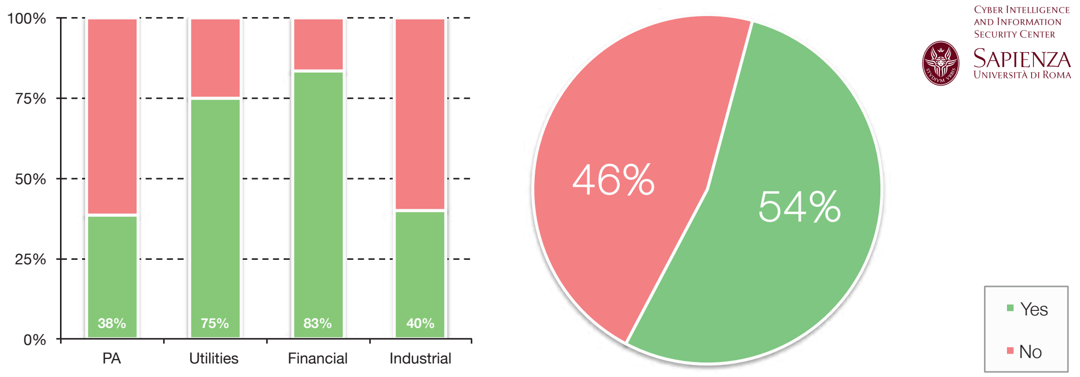


Figure 4.22: Question #1.4.1 - "Is your company using an Information Security Management System (ISMS) ?" Left chart shows answer distribution by group. Right chart depicts the overall picture.

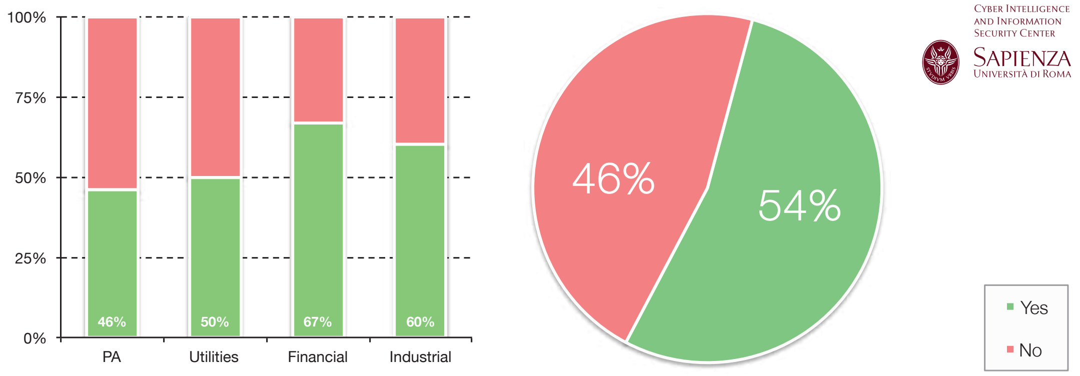


Figure 4.23: Question #1.4.2 - "Has your company adopted the ISO/IEC 27001 ?"Left chart shows answer distribution by group. Right chart depicts the overall picture.

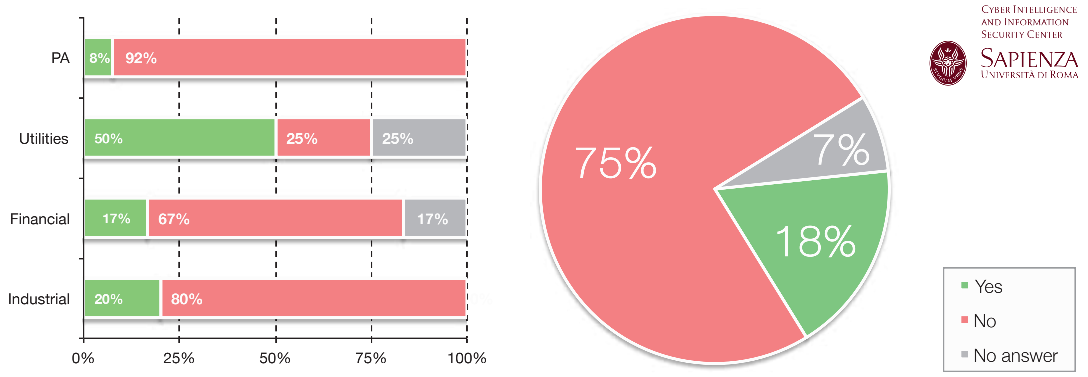


Figure 4.24: Question #1.4.6 - "Do you use an Operator Security Plan or an equivalent measure, as defined in the European Council Directive 2008/114/EC of 8 December, 2008 ?" Left chart shows answer distribution by group. Right chart depicts the overall picture.

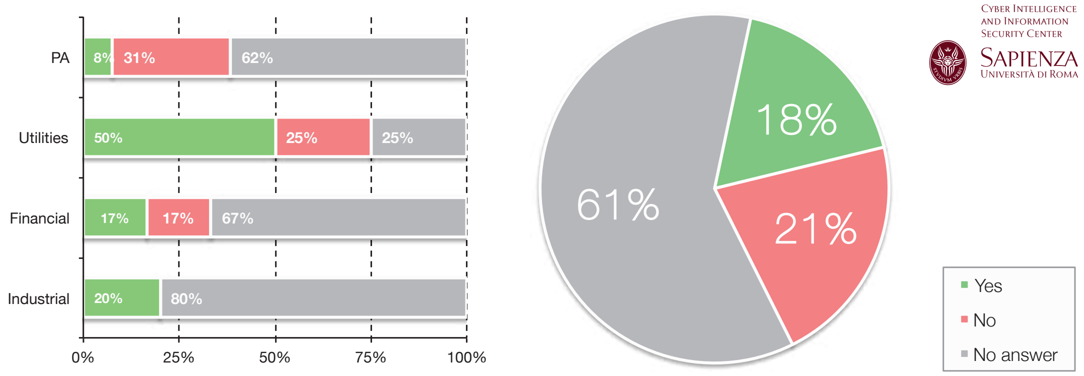


Figure 4.25: Question #1.4.7 - "If yes, is the Operator Security Plan regularly updated?" Left chart shows answer distribution by groups. Right chart depicts the overall picture.

4.7 How organizations would like to improve their security

The questionnaire contained a few questions aimed at assessing security measures organizations feel they should adopt in order to improve their cyber security. Figure 4.26 shows how the highest percentage of the respondents (31%) ask for better policies or a strict implementation of the existing policies; this is followed by the request for improved security tools and a basic security training for employees. Nevertheless, Figure 4.26 points out there is no large gap among measures that could improve organization security.

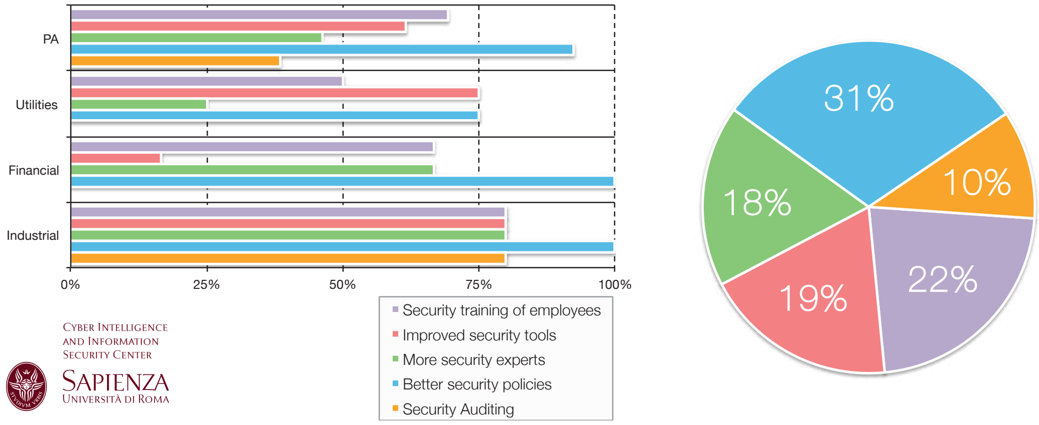


Figure 4.26: Question #1.5.4. - "Do you think that the security of your company could be improved with: (i) Better security policies, or strict implementation of the existents, (ii) More ICT security experts / security expert with expertise conformity externally tested, (iii) Improved security tools, (iv) Security focused training of all the employees with regard to their duties, (v) Security audit periodically executed by an external certified organization". Left chart shows answer distribution by group. Right chart depicts the overall picture.

The utilities group seems to have a high sensibility for policies adoption and implementation (75% of respondents ask for this) and for the request of better security tools (75% of respondents); these two demands are followed by better security training for employees and the presence of more security experts; for the financial group, the request for employees' training is comparable to the request for security experts, and it is worth noticing that 100% of the respondents belonging to this group asked for better policies; security auditing is seen as something that can improve security by the industrial group. Respondents of utilities and financial group does not even mention this measure. The PA group thinks auditing, security experts and tools could improve the security of their organizations, furthermore policies are seen by the widest majority of the group as something that could enhance security. Last but not least, note that all groups strongly believe in better policies as a way to improve their security.

4.8 A cyber security readiness index

Analyzing the questionnaire answers, various aspects related to the cyber security habits of the organizations were assessed. To this aim, a score system that evaluates the answers to a subset of questions in the questionnaire was designed. The evaluation is based on four indexes: awareness, defense, policy and external independency.

The cyber security readiness index is a composite measure of the capacity and willingness of an organization to face cyber threats. A nice cyber security habit for an organization is considered to be the one which is able to cover the largest area on a radar chart taking into account the four indexes. Thus the cyber security readiness index reflects the dimension of this area. The complete structure of the score system that computes the cyber security readiness index based on the four indexes is reported in Appendix B.

Awareness index - Assesses the situational awareness related to cyber risks of the organization and it is influenced by the majority of the questions in the survey (see appendix B); as an example positive responses to questions like, “Does your company regularly register anomalies? For anomalies we mean an event that is not a cyber-attack but is outside the normal behavior of the company infrastructure” (Question #1.3.10) and, “If so, the average number of these anomalies during last year is: [...]” (Question #1.3.11) influence negatively the awareness score since the presence of a frequent anomalous event in an organization network should be carefully analyzed in order to exclude the presence of sophisticated attacks. On the contrary, the awareness score is influenced positively when responses to questions show behavior which is cyber security aware; one example is the question, “Do you know if your software providers are following a strategic approach to address application risks in each phase of the application development process?” (Question #1.2.6); a positive response to this question shows a careful consideration of the risks that could derive from bad software design processes.

Defense index - Assesses the capacity of an organization to protect itself from a cyber attack. This considered the evaluation of the defense mechanisms and tools employed by an organization. An example of a question that influences positively this index is, “Which of the following measures to protect data and critical systems from misuse by employees does your company implement?” (Question #1.4.8); no answer to this question influences negatively both the awareness and defense index; on the contrary, a response like, “Restrict the use of personal emails and cloud services" has a slightly positive score on the defense index; the response, “Forbid the use of personal electronic equipment (laptop, smartphone, tablet)" has a significant positive impact on the defense score. Notice that the defense index is somewhat correlated with the awareness index. Some responses that positively impact the defense index, also impact the awareness index. This correlation is well-grounded since the implementation of strong defense mechanisms shows cyber security awareness.

Policy index - Assesses the implementation of security related policies. A high score in this index shows compliance to several security policies and their constant update. This index is influenced positively by Questions #1.4.1, # 1.4.2, # 1.4.3, # 1.4.6 and # 1.4.7. As an example Question # 1.4.7 asks, “Do you use an Operator Security Plan or an equivalent measure, as defined in the Council Directive 2008/114/EC of 8 December 2008?"; an affirmative response positively influences the index. As for the defense index there is a strong correlation of the policy index with the awareness index since the adoption of updated security policies show an increased awareness.

External independency index - Assesses the correlation between internal systems and external providers. A low score on this index shows the correlation of the organization mechanism to external providers since the fault of an external cloud provider could impact on its possibility to deliver the core product of its business. As an example the Question #1.2.2 that asks, “Do cloud services support core business processes that are necessary to deliver critical services?” with a negative answer would increases the external independency score. A high score on this index shows an organization that relies minimally on external services that could impact on its security. Note that such high scores imply larger operational costs as the organization has to insource software services without the involvement of third parties.

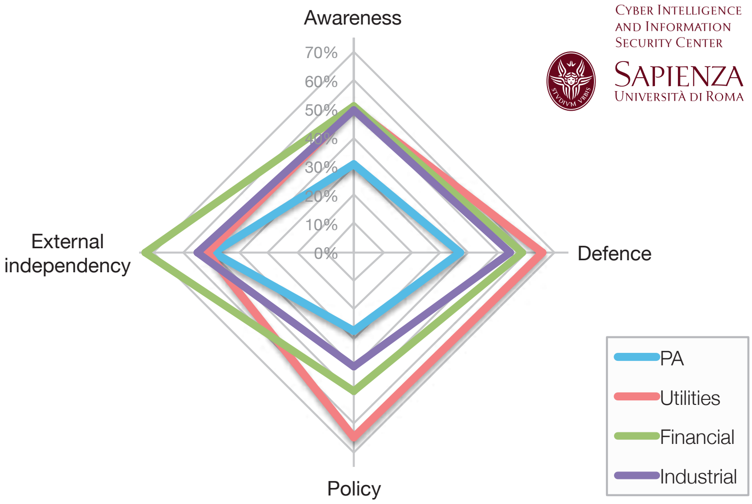


Figure 4.27: Cyber security readiness index: Awareness, Defense, Policy and External Dependencies indexes per group.

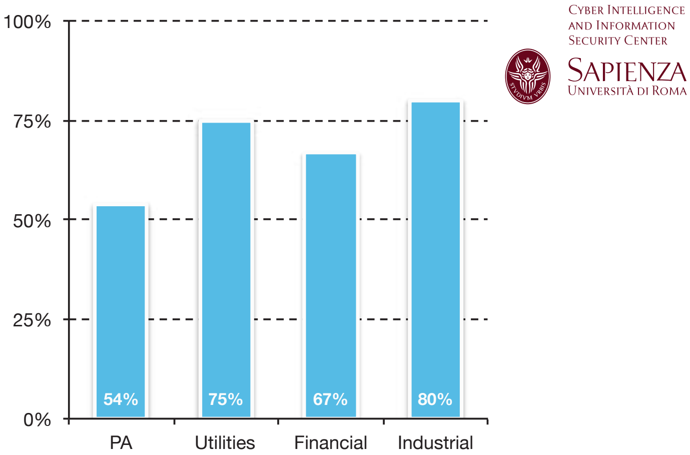


Figure 4.28: Question #1.5.3 - “Do you have situational awareness on the state of cyber threats to your organization?"(per group)

A radar chart is depicted in Figure 4.27 showing the results of the cyber security readiness index per group. As expected, the utility group covers the largest area in the ranking. It scores better than other groups along two axes, namely defense and policy. It has also a high score on awareness. Nevertheless, it suffers from a low external independence; this problem is shared by all the other groups, with the exception of the financial group that seems still reluctant to heavily rely on external service providers.

The financial group also exhibits a large covered area in the radar chart by showing high values for external independency, defense and awareness indexes. Surprisingly it does not score as expected on policy index. However, keep in mind that some of the questions that influence the policy index (e.g., question # 1.4.7) are related to the specific policy imposed by the EU directive 2008/114/EC on European Critical Infrastructure that financial organizations are not obliged to comply with.

The industrial group is the third one in the ranking, showing a high level of awareness and a good defense index while lagging behind in policy adoption. The PA group shows a low degree of cyber security readiness with respect to the other groups; indeed, the area covered by the radar plot is the smallest among all the groups. It has by far the lowest indexes on policy, defense and awareness.

It is interesting to compare the awareness index with the answers to question #1.5.3, that is, “Do you have

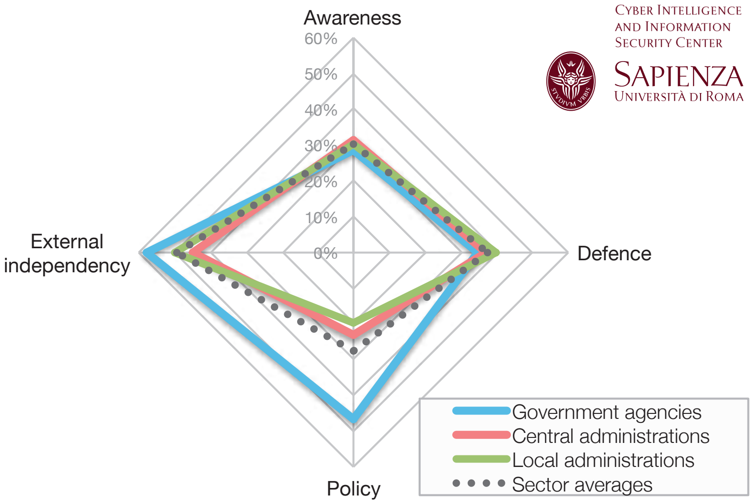


Figure 4.29: Cyber security readiness index for PA group.

situational awareness on the state of the cyber threat to your organization?" (Figure 4.28). It can be pointed out that the greatest value of the awareness index (see awareness axis in Figure 4.27) is scored by the industry, financial and utility groups. They actually share the same score. However, the perception that organizations belonging to these three groups have is quite different: the awareness declared by respondents from industry is very high while that declared by financial is 13% smaller. A similar argument can be used for the PA group. While the PA group seems to be quite well aware of the cyber security landscape (54% of the answers were positive in Figure 4.28), its awareness index is much smaller than the ones sported by the other groups. The utility group, instead, declares good situational awareness and its awareness index confirms this.

As last interesting note the PA group was disaggregated into government agencies, central administrations and local administrations and the cyber security readiness index for each sub group was computed. Results are shown in Figure 4.29 where the dotted line represents the group average. It can be seen that government agencies have better scores for policy index and external independency. This can be due to the fact that they have small information systems compared to central and local administrations, thus allowing for a more in-house approach. Local and central administrations show roughly the same area.

CHAPTER

5

Recommendations for a National Cyber Security Strategy

The aim of a national cyber security strategy is to increase the global resilience and security of national ICT assets that support critical functions of the state or of the society as a whole [17]. Setting clear objectives and priorities is of paramount importance for successfully achieving this aim. In order to manage risk in a proper way, it is necessary to design an effective risk management process by identifying what could go wrong (identification of risk), evaluating which risks should be dealt with (risk analysis and evaluation), and implementing strategies to deal with those risks, preventing or detecting all situations of risk, and implementing the adequate response. The UK is an example of a country which followed a risk management approach to implement a national strategy [49].

In the following, a risk management process (see Figure 5.1) is used as a useful paradigm to frame some recommendations for setting an effective national cyber security strategy for Italy. These recommendations do not aspire to be a complete set of rules to be followed, but rather they represent a set of points that we believe the national strategy on cyber security should take into account. Recommendations consider the legislative scenario, experiences from other countries, and results of the questionnaire. The target of these recommendations are in general all companies and PAs that manage or control critical infrastructures, security professionals working in economic sectors sensitive to cyber attacks and all government agencies and bodies involved in the definition and implementation of the Italian cyber security strategy.

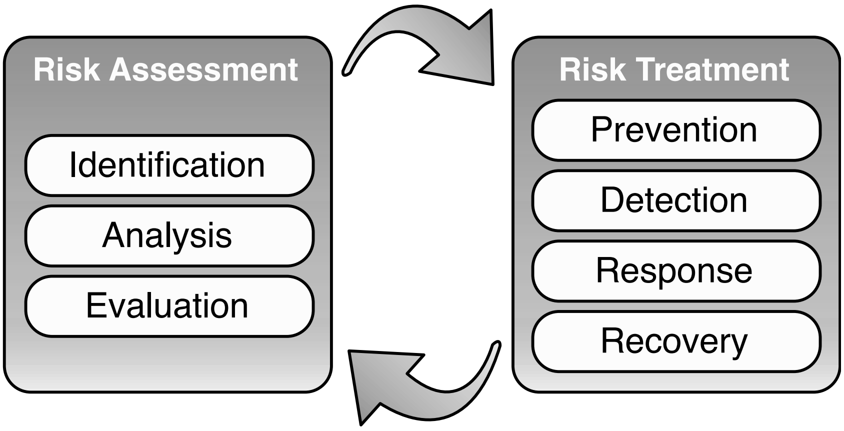


Figure 5.1: Risk management process

5.1 Recommendations for risk assessment

One of the key elements of a national cyber security strategy is the risk assessment process. It consists of three steps [18]:

Risk identification - identification of important assets/organizations/sectors and main sources of risk;

Risk analysis - determining the likelihood that a potential vulnerability can be exploited and the impact that the threat could have on a critical economic sector;

Risk evaluation - taking decisions about (i) the significance of risks for a critical economic sector and (ii) whether each specific risk should be accepted or treated.

Risk assessment can provide valuable information for developing, executing and evaluating a strategy. By carrying out a nationwide risk assessment process and by aligning the objectives of the strategy with national security needs, it is possible to focus on the most important challenges with regard to cyber security. In order to develop correct risk identification at national level it is important to clearly define and identify: critical economic sectors, cyber threats and vulnerabilities. A list of recommendations for risk assessment follows.

Understanding the dimension of cyber threats

Most of the events that can harm a critical economic sector sensitive to cyber threats are due to failures or human mistakes happening both in the physical and the cyber world that then propagate and escalate through the cyber world. Therefore, attackers exploiting vulnerabilities of an information system for damaging, for example, a national critical infrastructure are just one side of the coin. Failures and cyber attacks have to be studied and analyzed in the same framework (e.g. mitigation, inter-dependencies and awareness strategies) in order to make the economic sector infrastructure more dependable.

Identify priorities within critical economic sectors

A key aspect in have a compelling security strategy is to clearly identify priorities in the protection of critical economic sectors (including national critical infrastructure). As a matter of fact, it is not possible to ensure the same degree of protection to all systems. Therefore, it is important to give higher priority to those systems which have a greater impact on national security. At the same time, all economic sectors should be protected with at least a minimum level of security.

Understanding attackers' habits

To establish a national cyber security priority for defending services of critical economic sectors that underpin our society and economy, there is the need to understand the habit of attackers, their targets, their strategies and their methodologies. Thus a risk framework must reflect such factors, that is to say the key assets or functions of economic sectors that could be targeted by criminals, hacktivists, and state-sponsored organizations and potential avenues for attack or exploitation. This process involves understanding what motivates cyber threat actors, and the classification of cyber threats.

Taking critical economic sector infrastructure inter-dependencies into account

In section 4.2 it was shown that almost 50% of the protagonists in the Italian panorama are going to use third party solutions. Moreover, 80% of them know they depend on failures suffered by third party companies. The priorities and security baselines should consider of paramount importance the dependency relations among critical infrastructures and assign appropriate priorities according to their level of dependency, e.g. if the correct functioning of a system is mandatory for more than one critical infrastructure, that system must have a higher level of priority, with respect to assets that depend on it. Ranking of threats in the national strategy has to be addressed taking into account the implications for critical economic sectors, including the theft of sensitive data, damage to business or operational systems, disruption of services, and other scenarios that could result in substantial financial loss and compromise public safety or national security. Appropriate risk analysis techniques should be adopted to profile the threat.

Cooperative assessment of threats and vulnerabilities

Cyber threats have to be faced keeping in mind a global and unifying perspective. This is necessary since threats nowadays range from low-level attacks of small complexity executed by unskilled adversaries to sophisticated attacks executed from sparse geographical locations by groups of skilled adversaries with a huge number of resources. Coordination and cooperation are fundamental in order to identify threats and to reach an effective protection of critical economic sectors[1]. Service providers working in similar sectors (e.g. utilities) share similarities both in the assets used to deliver critical services (e.g., similar SCADA systems) and in organizational aspects (i.e. similar security policies). They are therefore likely to share the same weaknesses as well. Cooperation among service providers of the same sector should be fostered also through an appropriate legislative framework. Incentives should be given to balance the fact that such providers are usually competitors on open markets. As an example, the US Information Sharing and Analysis Centers (ISACs) could be a good starting point (http://www.isaccouncil.org/). Benefits of a cooperative approach have been deeply investigated in [3].

Nationwide methodology for threat classification

In order to effectively enforce an active cooperative scenario there is the need to develop a national methodology for classifying threats and decide at which level threats must be faced: at the single organization level, at the sector level, at the regional level, at the national level. In order to effectively protect national critical infrastructure and strategic economic sectors this is a very sensitive issue. Taking the wrong decision in such a classification could either underestimate or overestimate the threat. In the former case, the threat might not be blocked and thus spread through the economic sector infrastructure while in the latter case, false alarms are generated that, if not appropriately limited, could make all the protection process inefficient. Note that millions of threats against an infrastructure could be deployed in cyberspace in a few seconds; overestimation could thus hamper the whole process by disrupting the trustworthiness of the security strategy as a whole.

Clear guidelines governing how risks are accepted and documented

Risk evaluation is used to decide the significance of risks to organizations and whether each specific risk should be accepted or treated. Since it is impossible to mitigate all risks, frameworks for national risk developed under the parameters of the national strategy should include clear guidelines governing how risks are accepted and documented. Guidelines should also specify when an economic sector is so vital that a higher standard of protection is needed.

5.2 Recommendations for risk treatment

As shown in Figure 5.1, risk treatment includes the following:

Risk prevention - All categories of management and of technical and operational activities that enable the decision of appropriate outcome-based actions to ensure adequate protection against threats. When adequate preventive protection mechanisms are in place, implemented via physical or logical protection, it is possible to identify and activate the detection mechanisms.

Risk detection - All activities identifying (through ongoing monitoring or other means of observation) the presence of cyber threats, and the processes to assess the potential impact of those threats.

Risk response - Responding to a significant threat (i.e. deciding on the appropriate courses of action to accept, avoid or mitigate the threat) through a risk response plan;

Risk recovery - Once an incident is detected and validated, some actions should follow. They generally include (i) stopping an ongoing incident, (ii) identifying the scope and scale of incident, (iii) limiting damage, (iv) taking measures in order to investigate the course of events and (v) preventing the incident from recurring.

A set of recommendations for risk treatment follow.

[1] 83% of positive answers to question #2.0.1 “Do you think that cooperation among companies of your sector should be enforced by government legislation?”

Clear role and mission for the national CERT

As remarked in Section 2.2, Italy has recorded a significant delay in setting up a national CERT. Although the realization of the national CERT has been introduced by the Legislative Decree 28 May 2012, n. 70 complying with the transposition of Directive 2009/140/EC, to the best of our knowledge a national CERT is still not operating. Moreover, CERT's operative role within the national cyber security strategy is still not clear. Having an operative national CERT with a clear mission and role is the basic building block of any national cyber security strategy.

To work properly, a CERT needs the participation of numerous public and private sector actors, with clear terms of participation. Following the example of many other countries (including the USA), the Italian CERT should be deeply connected with the academic world, which can provide the most innovative solutions in the field of secure information, and that is institutionally committed to research and training activities. Apart from its traditional tasks, as remarked in some of the recommendations of Section 5.1, the national CERT needs to clearly define the guidelines that have to be used to classify threats, their criticality level, and the corresponding sensitivity level. By making use of this classification, it should be possible to clearly distinguish between national, regional and local incidents. This is a priority given the number of players, bodies and boards that have a role within the Italian cyber security landscape as designated by the DPCM of 24 March 2013 (see the last paragraph of Section 2.1).

The national CERT should also have the role of coordinating with other CERTs operating in Italy and being the Italian interface for EU and international CERTs. As already remarked in Section 2.2, in June 2012 ENISA listed Italian CERTs. This list also included some inactive CERTs and other CERTs which do not show any information on activities they actually perform.

Set clear definitions and procedures for incident response

The national CERT will have to provide detailed, timely and accurate information about potential threats that may damage the national critical infrastructure and sensitive economic sectors. This will be possible only by defining clear procedures and plans that have to be followed by all the private and public organizations that will collaborate with the national CERT. For such a reason, the national strategy should clearly define the cooperation and coordination procedures that have to be followed. In particular, high-level goals, objectives, and priorities have to be established and shared with all the organizations involved. Furthermore, it is important to address all the problems related to the information sharing of attacks and discovered vulnerabilities. In this process, organizations need to be guaranteed that only the essential information about security incidents are disclosed to third parties.

Cooperative early threat and vulnerability warning dissemination

When a new threat (e.g. vulnerability, malware, etc) is discovered in the information systems of an organization, an early dissemination of this information to all interested national actors is mandatory in order to properly protect their own organization infrastructure. The dissemination has to be done within a legislative scenario which ensures the organization disseminating the threat is not legally liable. The early warning may allow system administrators to take countermeasures in order to mitigate or monitor possible attacks. Thus the institution of an Italian actor that is in charge of managing a National Vulnerability Database is of national interest for improving the protection of national assets and, therefore, is strongly encouraged. Furthermore, an international standard such as Security Content Automation Protocol (SCAP) framework should be adopted in order to push towards a simple interaction with international partners.

Promote dissemination activities and enhance education skills

Fostering awareness among the population is a priority. No national strategy for cyber security can be implemented without a plan for dissemination activities such as newspaper articles and debates in the mass media to increase awareness of ordinary people not necessarily involved in the protection of critical resources. Conveying an appropriate message to ordinary people on the risk connected to Internet-use at the personal and community level has to be a long lasting objective. In addition to raising the level of awareness of ordinary people, there is the need to develop specialized skills in, and knowledge of, cyber security in universities and research centers. This will lead to the creation of a new class of cyber security experts needed by private and public organizations and research.

5.3 Further recommendations

Research, development and technology investments

Due to the strategic nature of cyber security for a nation, we cannot outsource these competences to other countries but it is imperative to consolidate and possibly increase domestic competence in creating and deploying security technologies. Cyber security can be considered as a giant economic opportunity for Italy. The presence in Italy of key sector players, high-tech SMEs and highly reputed research centers makes Italy a breeding grounds for cyber security initiatives that could be a source of employment and wealth for the current and next generations. Thus, it is important for a nation to have a research and technology agenda to promote advances in research and high-tech development. This investment needs to be done immediately. It is not clear if the situation will continue to be like this ten years from now. Additionally, appropriate investment is necessary for keeping the best researchers in this field in Italy, so contributing to ensure national independence from information technology related risks.

International engagements

Efforts made in improving the protection of national critical economic sectors cannot be made in isolation with respect to the rest of the world because cyber threats intrinsically cross borders. As an example, an attacker can destroy a critical infrastructure of a nation while sitting on a sofa ten thousands kilometers from the attacked place. Thus a defense cannot be only on the perimeter, but there is the need of international collaborations and networking. Cooperation among national CERTs is definitely expected as well as cooperation at the political and law enforcement level with the signature of appropriate bilateral or multilateral agreements. Another important point is to set up a clear and agreed worldwide governance of Internet that will be able to make cyberspace a more regulated place.

Critical economic sector organizations should adopt solid risk management processes

Risk management processes helps organizations determine what assets need protection, the threats they require protection against and the controls. The evaluation helps categorize risks by severity and involves making cost-effective decisions on what needs protection. The process helps organizations to ensure that efforts and investments on security yield cost effective benefits. Good risk management processes recognize that organizations have different business requirements, structures and operational environments. The process defines broad requirements allowing organizations to decide the most cost effective and efficient risk management approaches (ISO/IEC 2008). Effective risk management requires a reporting and review structure to ensure that risks are effectively identified and assessed and that necessary countermeasures and responses are put in place. Making sure that a critical economic sector equips itself with an adequate risk governance process allows to delegate part of the controlling activities to infrastructure owners and operators. The latter has a comprehensive and deeper understanding of the specific needs and characteristics of their systems.

Last but not least, audit activities of critical economic sector infrastructure by external entities is good practice and has to be encouraged. As an example, Figure 4.16 shows that 47% of the interviewed actively audits security levels using external companies. However, organizations still need internal audits or a coordinator of information system security. Cyber security needs clear roles and responsibilities: experts with appropriate skills, authority, and resources to develop security baselines and to satisfy security regulation requirements. This is recommended for all sectors, from government owned organizations to privately owned ones.

Reducing the supply chain risk

This can be done by (i) studying all the supply chain of vendors of products and services employed within the economy, (ii) improving the visibility of the supply chain and building relationships of trust between vendors of products and services and infrastructure providers, (iii) improving the compliance with international standards and having laboratories where such compliance is tested.

A national agency for cyber security

Ensuring cyber security for a nation is a duty that cannot disregard good technology skills and competences. Any government organization that is involved in the national cyber security strategy thus needs to have such skills in-house and its governance needs to be aware of and able to assess cyber and information technology risks. The latter point is critical because if an organization's governance does not have appropriate technology competences, it will either overestimate or underestimate a threat or simply not understanding what is going on. This is why many countries, including France, Israel, Germany, Holland, to cite just a few, decided to converge all activities related to cyber security inside a single organization which most of the time is within the Presidency of the Council of Ministers of its own country (e.g. National Cyber Bureaux in Israel, Federal Office for Information Security in Germany, Network and Information Security Agency in France, National Cyber Security Centre in the Netherlands etc.). We cannot indeed expect that the necessary skills and competences also at governance level can be found in many government organizations and agencies. Additionally when decisions have to be taken about facing a threat, these decisions have to be fast and sharp. The same is true for coordination activities. All of this calls for a national agency for cyber security that empowers procedures, processes and coordination activities actually being the main agent for implementing the national cyber security strategy to make the national cyberspace a safe place.

Bibliography

[1] Andoh-Badoo F.K., Osei-Bryson K.M., “Exploiting the characteristics of internet security breaches that impact the market value of breached firms”, Expert system with Applications, 32, 2007, pp. 703-725.

[2] Aniello L., Baldoni R., Di Luna G.A. and Lodi G., “An event-based platform for collaborative threats detection and monitoring", Information Systems, 39, p175-195, 2014.

[3] Baldoni R. and Chockler G., “Collaborative Financial Infrastructure Protection - Tools, Abstractions, and Middleware”, Springer, 2012.

[4] Baldoni R., Bonomi S., Di Luna G.A., Montanari L., Sorella M.: “Understanding (Mis)Information Spreading for Improving Corporate Network Trustworthiness”, p165-172. EWDC 2013.

[5] Brockett P., Golden L.L. and Song A., “Managing risk in mobile commerce", International Journal Electronic Business, Vol. 10, No. 2, 2012.

[6] Brunner M. and Suter E. M., “International CIIP Handbook 2008/2009”, Center for Security Studies, ETH Zurich, 2008.

[7] Byres E.J. and Lowe J.,“The Myths and Facts behind Cyber Security Risks for Industrial Control Systems”, VDE 2004 Congress, VDE, Berlin, October 2004.

[8] Clusit report, "Rapporto Clusit 2013 sulla sicurezza ICT in Italia", Clusit, 2013 http://www.clusit.it.

[9] Dos Santos B.L., Peffers K., Mauer D.C., “The impact of information technology investment announcements on the market value of the firm”, Information Systems Research, 4, pp. 1-23. 1993.

[10] ENISA (European Network and Information Security Agency), “Incentives and Challenges for Information Sharing in the Context of Network and Information Security", 2010.

[11] European Commission, “Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection”, EC, COM (2006) 787.

[12] European Commission, “Green Paper on a european programme for critical infrastructure protection”, EC, COM(2005)576, Bruxelles, Annex I.

[13] European Commission, “Verso una politica generale di lotta contro la cibercriminalità”,EC, COM(2007)267, pp. 1-2.

[14] European Commission, European Communication from the Commission to the Council and the European Parliament of 20 October 2004, “Critical Infrastructure Protection in the fight against terrorism”, EC, COM(2004) 702.

[15] European Proposal for a “Regulation of the European Parliament and of the Council", Concerning the European Network and Information Security Agency (ENISA), EC,COM(2010) 521.

[16] European Union, “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", JOIN/2013/0001.

[17] European Union Agency for Network and Information Security (ENISA), “National Cyber Security Strategy. Practical Guidebook”, p8, December 2012.

[18] European Union Agency for Network and Information Security (ENISA), Glossary, http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary.

[19] European Union Agency for Network and Information Security (ENISA), National Cyber Security Strategy List, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world.

[20] European Union Directive 2008/114/EC.

[21] French ANSSI website http://www.ssi.gouv.fr.

[22] Gordon L.A., Loeb M.and Sohail T., “A Framework for using insurance for cyber-risk management”, Communications of the ACM, 44, pp. 70-75, 9 March 2003.

[23] Italian Digital Agenda official website, http://www.agenda-digitale.it/agenda_digitale/.

[24] Italian Audiweb Database, June 2011, www.audiweb.it.

[25] Italian Audiweb Database, September 2012, www.audiweb.it.

[26] Italian Digital Administration Code, http://www.digitpa.gov.it/codice-amministr-digitale/attuazione-del-cad.

[27] Italian Information and Security Department, “Report on information policy for security in the year 2010”, Presidency of the Council of Ministers, pp. 23-35, Rome, 2011.

[28] Italian Ministry for the Interior Decree G.U. 30 aprile 2008, n. 101, “Individuazione delle infrastrutture critiche informatiche di interesse nazionale”.

[29] Italian national security official website, http://www.sicurezzanazionale.gov.it.

[30] Italian Police official website, http://www.poliziadistato.it/articolo/18494/.

[31] Italian Presidency of the Council of Ministers, Sistema di informazione per la sicurezza della repubblica, “Il linguaggio degli organismi informativi. Glossario intelligence", Quaderni di Intelligence Gnosis, 2012.

[32] Italian Presidency of the Council of Ministers, “Protezione delle Infrastrutture Critiche Informatizzate", Dipartimento per l’Innovazione e le Tecnologie, Marzo 2004.

[33] Kaspersky Lab, “The geography of cybercrime: Western Europe and North America”, September 2012.

[34] Kaspersky Securelist, http://www.securelist.com/en/analysis/204792244/The_geography_of_cybercrime_Western_Europe_and_North_America.

[35] Kern R. and Peltz V., “Disaster Recovery Levels”, IBM Systems Magazine, November 2003.

[36] Microsoft, “Microsoft Security Intelligence Report", Regional Threat Assessment: Italy”, Volume 14, July through December, 2012.

[37] Norton 2012 cybercrime report - Italy, http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/NCR-Country_Fact_Sheet-Italy.pdf.

[38] Ponemon Institute, “2011 Cost of Data Breach Study, Italy”, March 2012, http://www.ponemon.org.

[39] Rinaldi S.M., Peerenboom, J.P. and Kelly T.K., “Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies”, IEEE Control Systems Magazine, Vol. 21, No. 6, 11-25, 2001.

[40] Shackelford S.J., “In search of cyber peace" Stanford Law Review. 2012, http://www.stanfordlawreview.org/online/cyber-peace.

[41] Symantec, “Internet Security Threat Report 2013", Volume 18, 2013.

[42] US Information Technology Industry Council, “Steps to Facilitate More Effective Information Sharing to Improve Cybersecurity”, October 2011, www.itic.org.

[43] US Presidential Decision Directive 63 (May 22, 1998), “Critical Infrastructure Protection”.

[44] US Presidential Policy Directive 21 (February 12, 2013), “Critical Infrastructure Security and Resilience”.

[45] US Public law 107-56 (October 26, 2001) “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act”.

[46] US Whitehouse official website, http://www.whitehouse.gov/administration/eop/nsc/cybersecurity/progressreports/july2010.

[47] US Whitehouse official website, http://www.whitehouse.gov/cybersecurity.

[48] US Whitehouse official website, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

[49] UK Cabinet Office, “The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world", Cabinet Office, United Kingdom, London, 2011.

[50] UK Financial Services Authority, “The failure of the Royal Bank of Scotland - Financial Services Authority Board Report”, 2011.

[51] United Nation, “Overview of cybersecurity”, ITU Recommendation ITU-T X.1205", ITU-T, p.2, Geneva 2008.

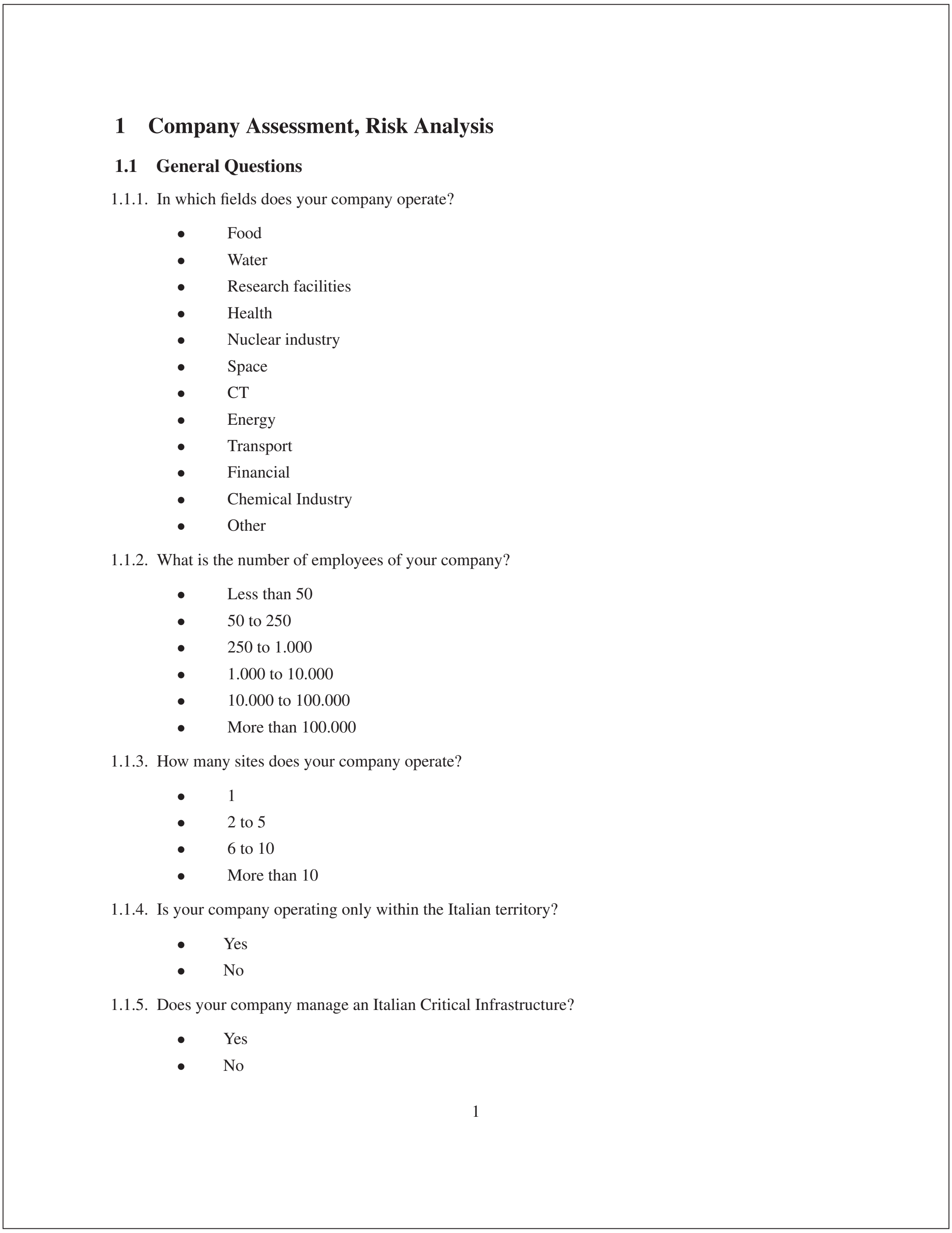
[52] Verizon, “The 2013 Data Breach Investigations Report”, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf.

[53] Vulpiani D., “La cyber threat alle infrastrutture critiche: punto di situazione ed azione di contrasto", Italian Intelligence Culture and Strategic Analysis (ICSA) Convegno, “La protezione delle Infrastrutture Critiche in Italia”, Rome, May 2010.

[54] Westby J. R., “Governance of Enterprise Security: CyLab 2012 Report”, Carnegie Mellon University CyLab, 2012, https://www.cylab.cmu.edu/outreach/governance.html.

Appendix A: Questionnaire

In order to conduct a deep analysis of the Italian cyber security situation, the Research Center of Cyber Intelligence and Information Security of Sapienza Università di Roma submitted an anonymous questionnaire to 68 organizations sensitive to cyber attacks according to the definition given in Section 1.3. A successful attack on any of these organizations would produce an impact that goes beyond the same organizations boundaries and affects other organizations or society as a whole. A total of 28 fully filled-in questionnaires were collected. The following pages report the content of the questionnaire.



1 Company Assessment, Risk Analysis

1.1 General Questions

1.1.1. In which fields does your company operate?

- Food
- Water
- Research facilities
- Health
- Nuclear industry
- Space
- CT
- Energy
- Transport
- Financial
- Chemical Industry
- Other

1.1.2. What is the number of employees of your company?

- Less than 50
- 50 to 250
- 250 to 1.000
- 1.000 to 10.000
- 10.000 to 100.000
- More than 100.000

1.1.3. How many sites does your company operate?

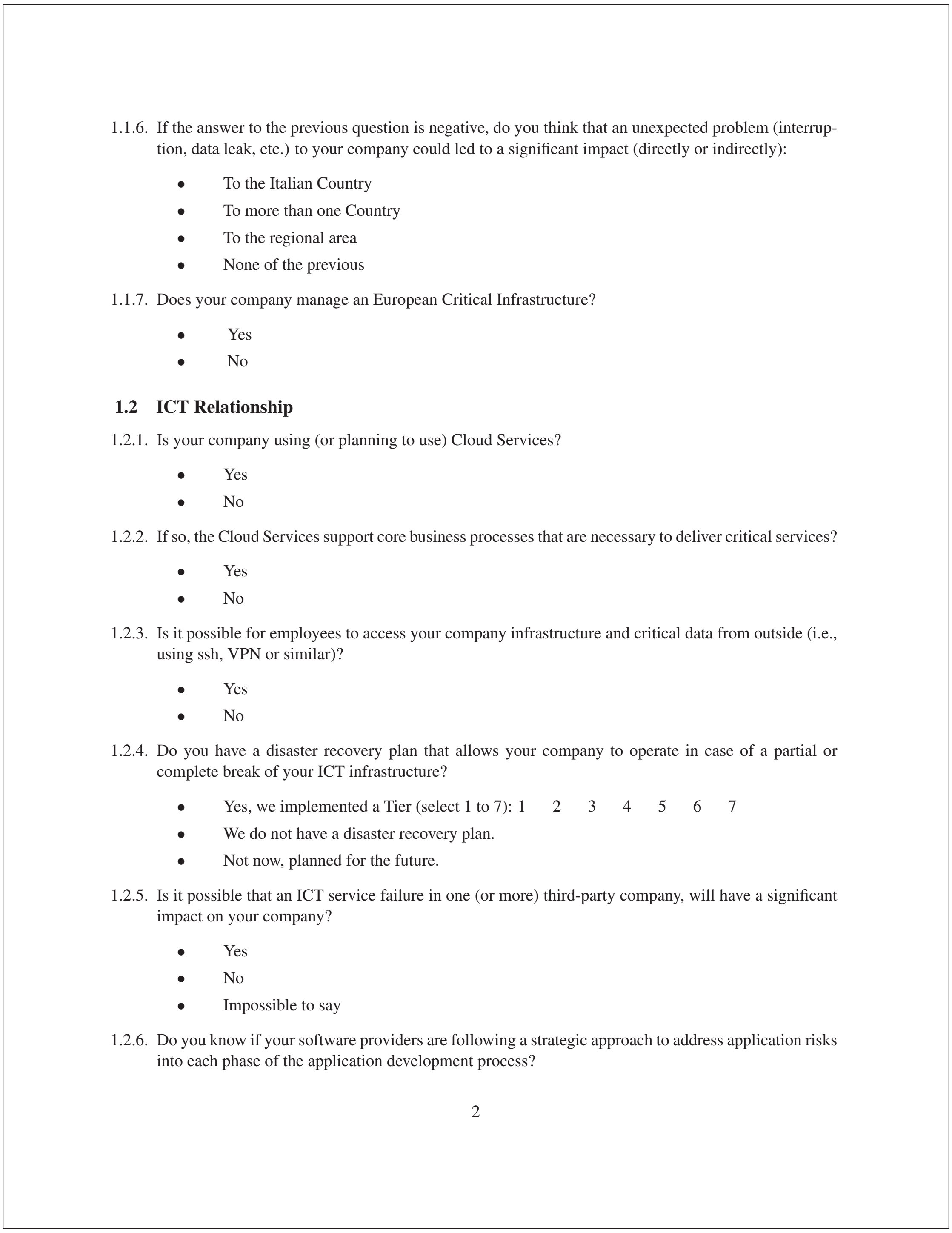
- 1
- 2 to 5
- 6 to 10
- More than 10

1.1.4. Is your company operating only within the Italian territory?

- Yes
- No

1.1.5. Does your company manage an Italian Critical Infrastructure?

- Yes
- No



1.1.6. If the answer to the previous question is negative, do you think that an unexpected problem (interruption, data leak, etc.) to your company could led to a significant impact (directly or indirectly):

- To the Italian Country
- To more than one Country
- To the regional area
- None of the previous

1.1.7. Does your company manage an European Critical Infrastructure?

- Yes
- No

1.2 ICT Relationship

1.2.1. Is your company using (or planning to use) Cloud Services?

- Yes
- No

1.2.2. If so, the Cloud Services support core business processes that are necessary to deliver critical services?

- Yes
- No

1.2.3. Is it possible for employees to access your company infrastructure and critical data from outside (i.e., using ssh, VPN or similar)?

- Yes
- No

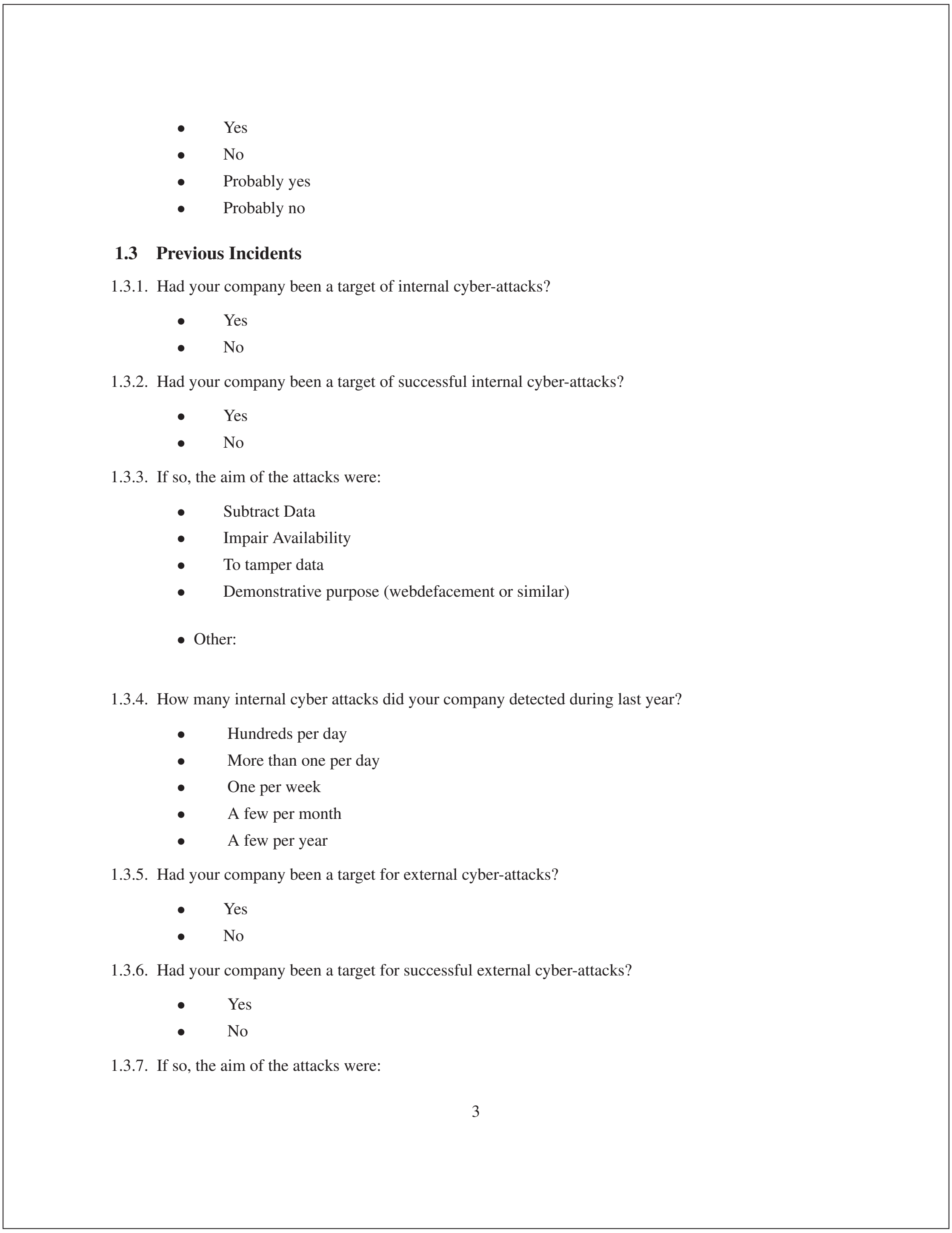
1.2.4. Do you have a disaster recovery plan that allows your company to operate in case of a partial or complete break of your ICT infrastructure?

- Yes, we implemented a Tier (select 1 to 7): 1 2 3 4 5 6 7
- We do not have a disaster recovery plan.
- Not now, planned for the future.

1.2.5. Is it possible that an ICT service failure in one (or more) third-party company, will have a significant impact on your company?

- Yes
- No
- Impossible to say

1.2.6. Do you know if your software providers are following a strategic approach to address application risks into each phase of the application development process?



- Yes
- No
- Probably yes
- Probably no

1.3 Previous Incidents

1.3.1. Had your company been a target of internal cyber-attacks?

- Yes
- No

1.3.2. Had your company been a target of successful internal cyber-attacks?

- Yes
- No

1.3.3. If so, the aim of the attacks were:

- Subtract Data
- Impair Availability
- To tamper data
- Demonstrative purpose (webdefacement or similar)

- Other:

1.3.4. How many internal cyber attacks did your company detected during last year?

- Hundreds per day
- More than one per day
- One per week
- A few per month
- A few per year

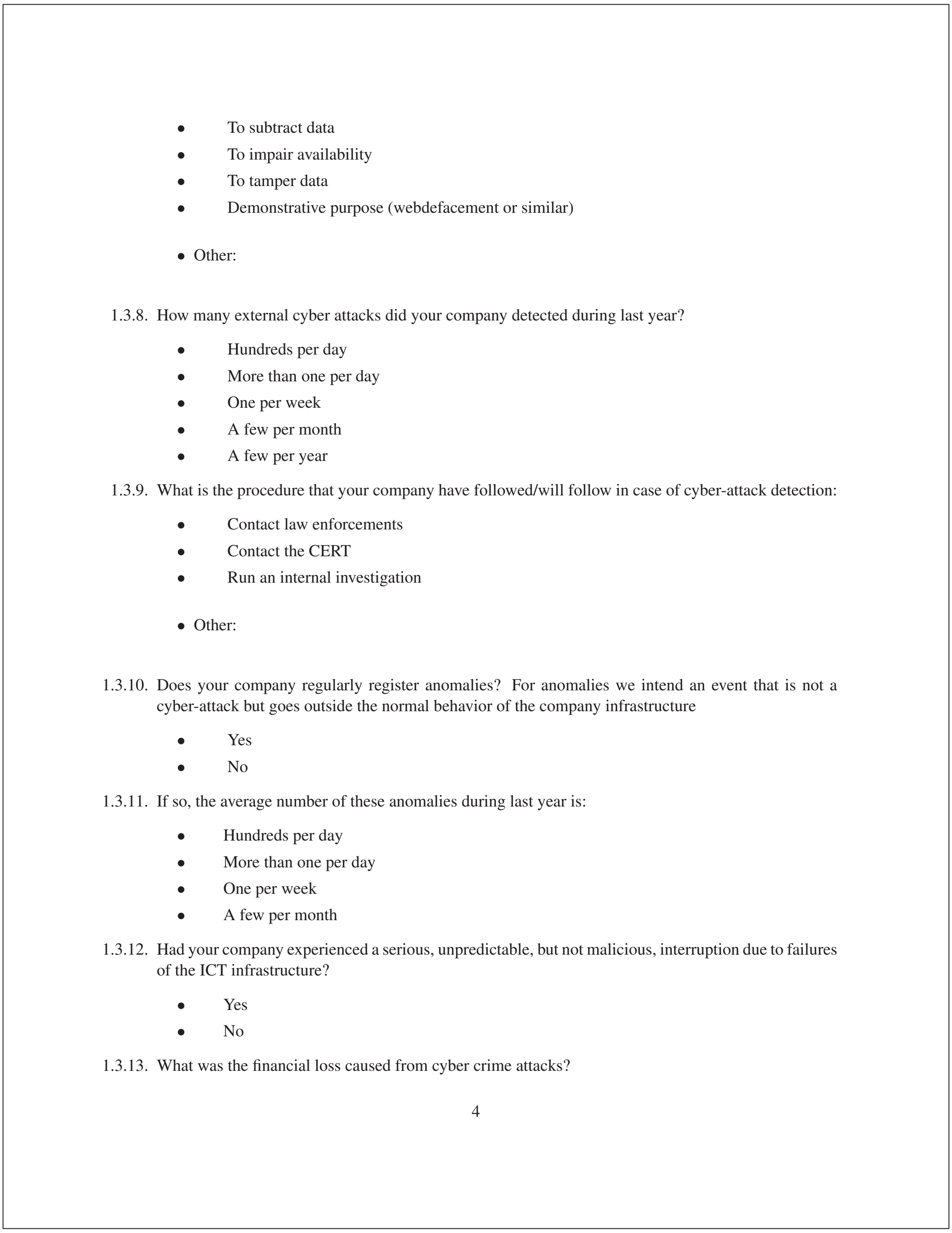
1.3.5. Had your company been a target for external cyber-attacks?

- Yes
- No

1.3.6. Had your company been a target for successful external cyber-attacks?

- Yes
- No

1.3.7. If so, the aim of the attacks were:



- To subtract data
- To impair availability
- To tamper data
- Demonstrative purpose (webdefacement or similar)

- Other:

1.3.8. How many external cyber attacks did your company detected during last year?

- Hundreds per day
- More than one per day
- One per week
- A few per month
- A few per year

1.3.9. What is the procedure that your company have followed/will follow in case of cyber-attack detection:

- Contact law enforcements
- Contact the CERT
- Run an internal investigation

- Other:

1.3.10. Does your company regularly register anomalies? For anomalies we intend an event that is not a cyber-attack but goes outside the normal behavior of the company infrastructure

- Yes
- No

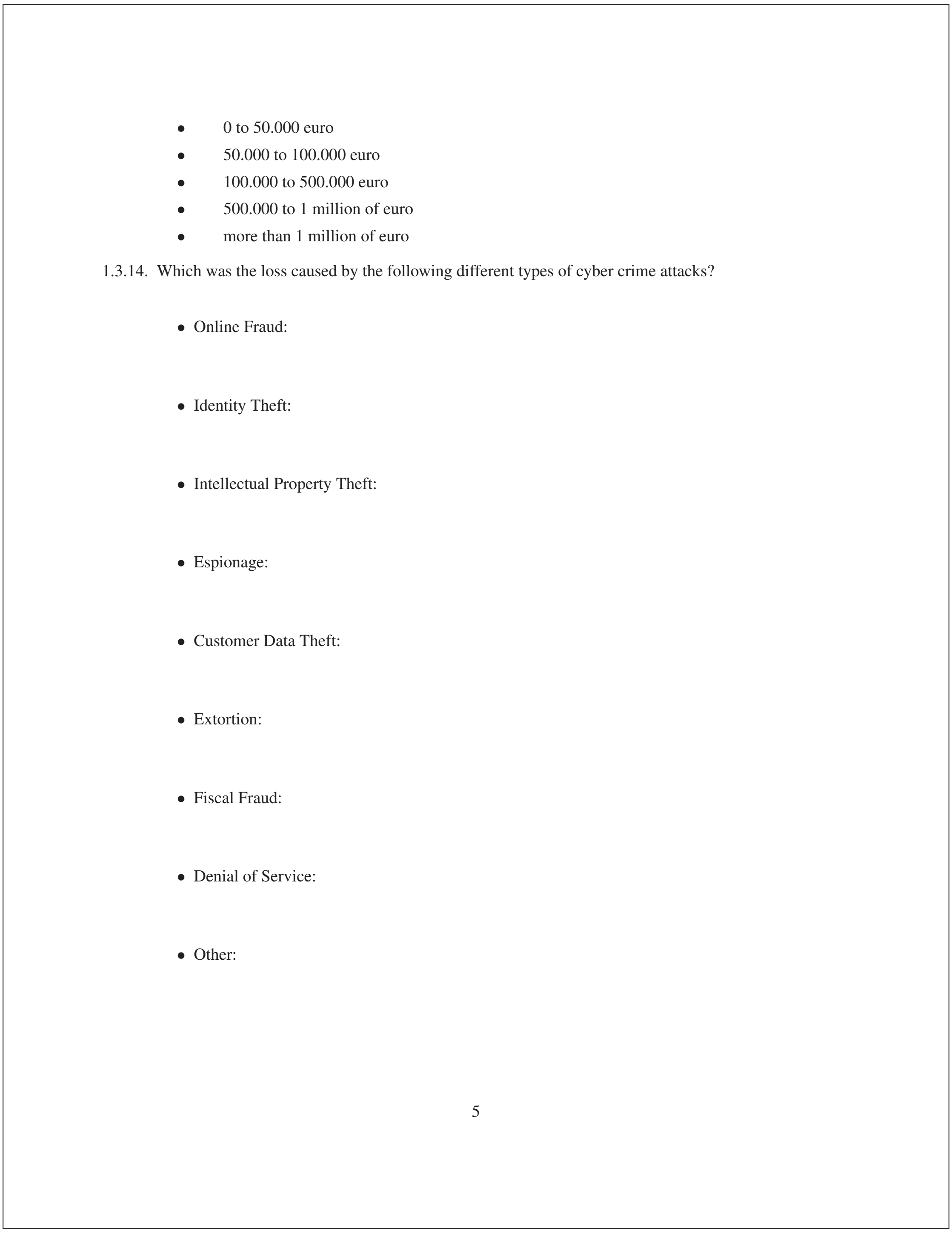
1.3.11. If so, the average number of these anomalies during last year is:

- Hundreds per day
- More than one per day
- One per week
- A few per month

1.3.12. Had your company experienced a serious, unpredictable, but not malicious, interruption due to failures of the ICT infrastructure?

- Yes
- No

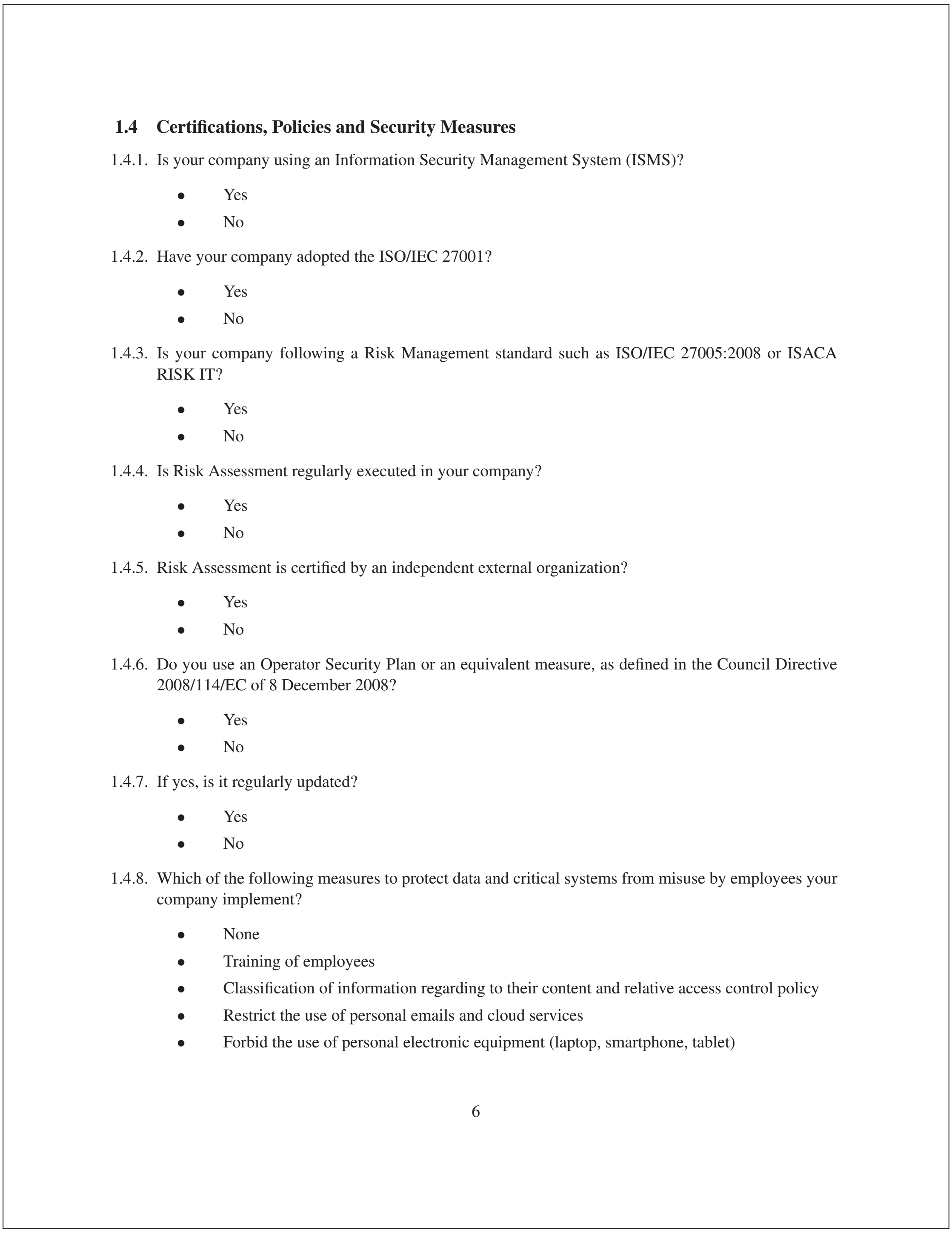
1.3.13. What was the financial loss caused from cyber crime attacks?



- 0 to 50.000 euro
- 50.000 to 100.000 euro
- 100.000 to 500.000 euro
- 500.000 to 1 million of euro
- more than 1 million of euro

1.3.14. Which was the loss caused by the following different types of cyber crime attacks?

- Online Fraud:
- Identity Theft:
- Intellectual Property Theft:
- Espionage:
- Customer Data Theft:
- Extortion:
- Fiscal Fraud:
- Denial of Service:
- Other:



1.4 Certifications, Policies and Security Measures

1.4.1. Is your company using an Information Security Management System (ISMS)?

- Yes
- No

1.4.2. Have your company adopted the ISO/IEC 27001?

- Yes
- No

1.4.3. Is your company following a Risk Management standard such as ISO/IEC 27005:2008 or ISACA RISK IT?

- Yes
- No

1.4.4. Is Risk Assessment regularly executed in your company?

- Yes
- No

1.4.5. Risk Assessment is certified by an independent external organization?

- Yes
- No

1.4.6. Do you use an Operator Security Plan or an equivalent measure, as defined in the Council Directive 2008/114/EC of 8 December 2008?

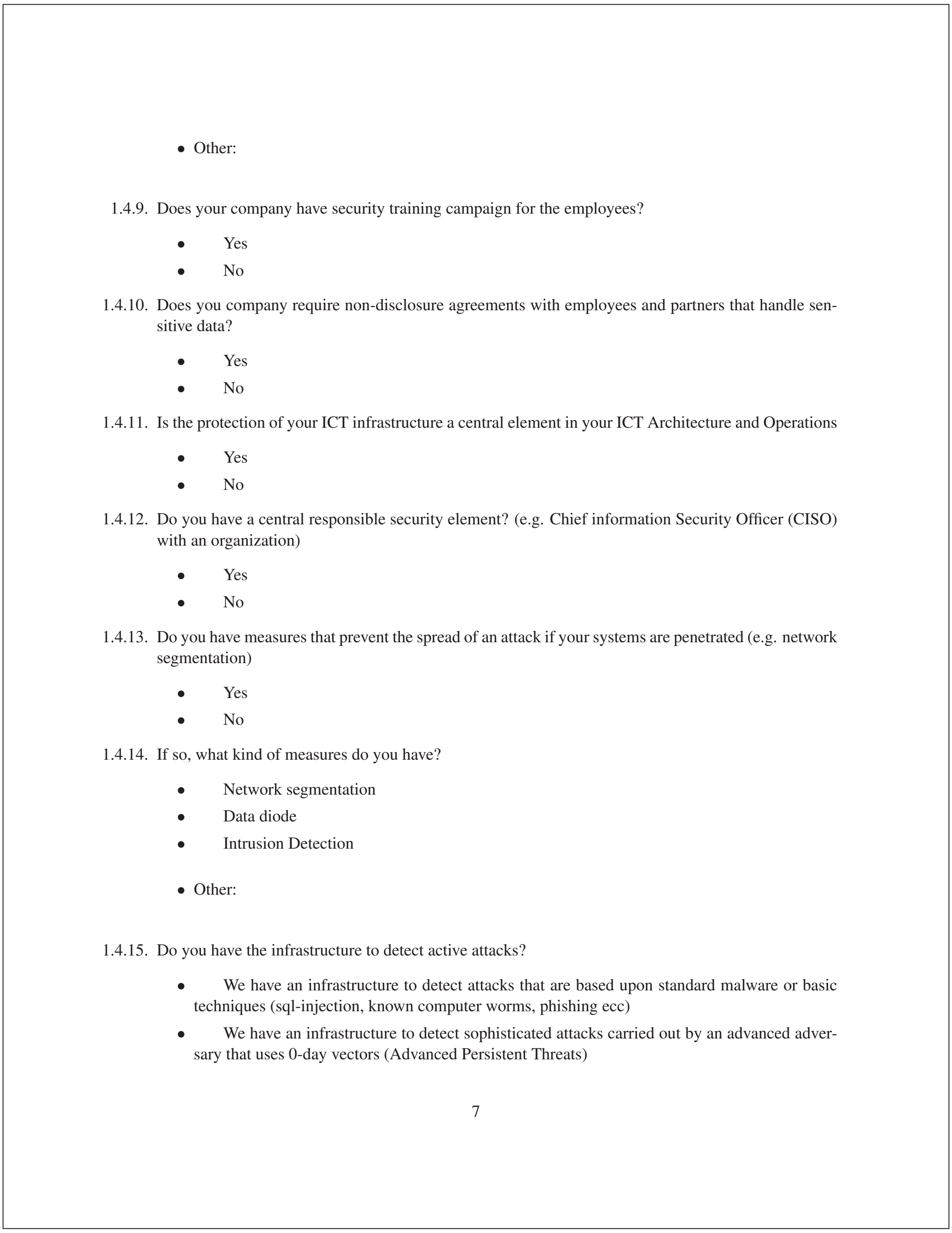
- Yes
- No

1.4.7. If yes, is it regularly updated?

- Yes
- No

1.4.8. Which of the following measures to protect data and critical systems from misuse by employees your company implement?

- None
- Training of employees
- Classification of information regarding to their content and relative access control policy
- Restrict the use of personal emails and cloud services
- Forbid the use of personal electronic equipment (laptop, smartphone, tablet)



- Other:

1.4.9. Does your company have security training campaign for the employees?

- Yes
- No

1.4.10. Does you company require non-disclosure agreements with employees and partners that handle sensitive data?

- Yes
- No

1.4.11. Is the protection of your ICT infrastructure a central element in your ICT Architecture and Operations

- Yes
- No

1.4.12. Do you have a central responsible security element? (e.g. Chief information Security Officer (CISO) with an organization)

- Yes
- No

1.4.13. Do you have measures that prevent the spread of an attack if your systems are penetrated (e.g. network segmentation)

- Yes
- No

1.4.14. If so, what kind of measures do you have?

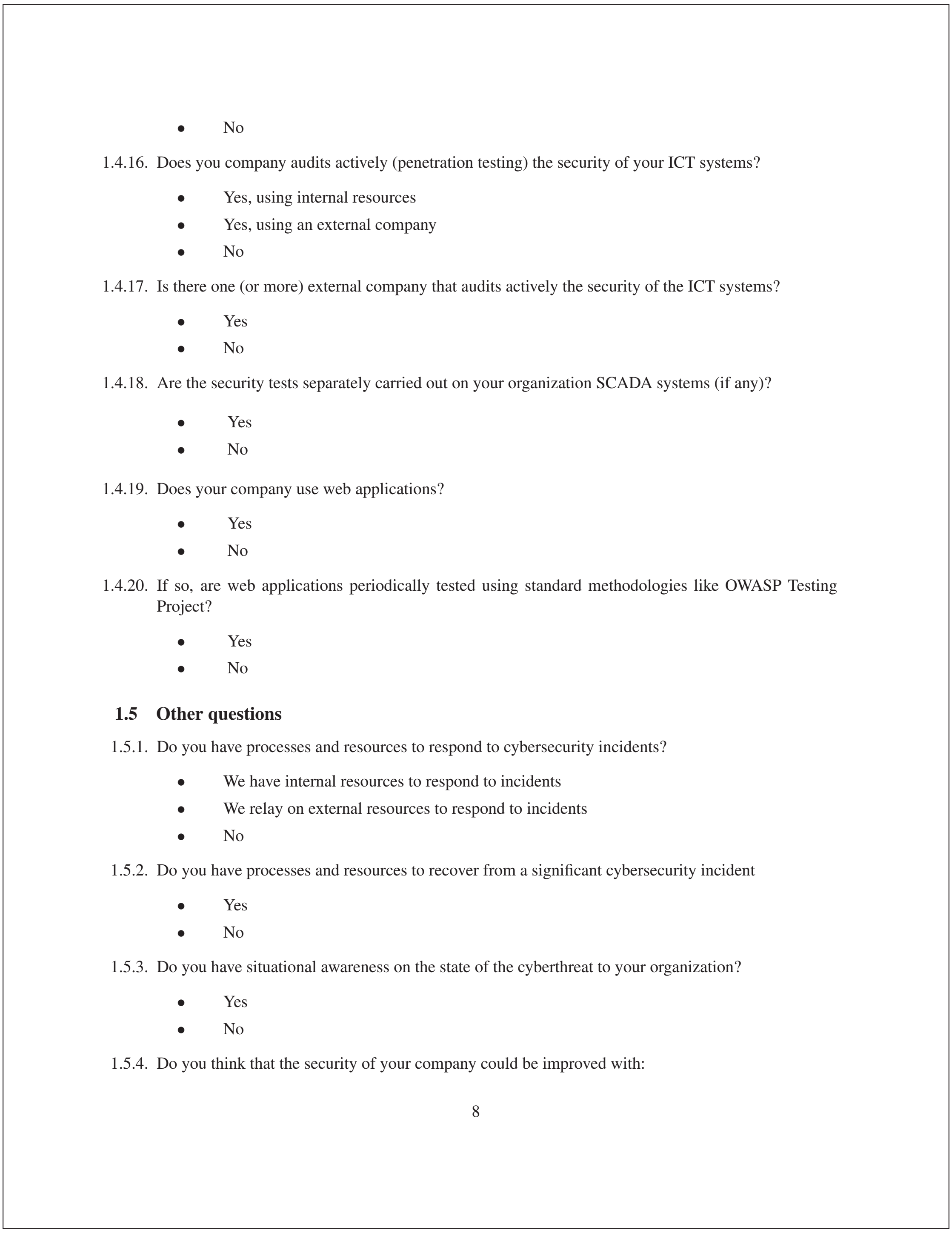
- Network segmentation
- Data diode
- Intrusion Detection

- Other:

1.4.15. Do you have the infrastructure to detect active attacks?

- We have an infrastructure to detect attacks that are based upon standard malware or basic techniques (sql-injection, known computer worms, phishing ecc)
- We have an infrastructure to detect sophisticated attacks carried out by an advanced adversary that uses 0-day vectors (Advanced Persistent Threats)

7



- No

1.4.16. Does you company audits actively (penetration testing) the security of your ICT systems?

- Yes, using internal resources
- Yes, using an external company
- No

1.4.17. Is there one (or more) external company that audits actively the security of the ICT systems?

- Yes
- No

1.4.18. Are the security tests separately carried out on your organization SCADA systems (if any)?

- Yes
- No

1.4.19. Does your company use web applications?

- Yes
- No

1.4.20. If so, are web applications periodically tested using standard methodologies like OWASP Testing Project?

- Yes
- No

1.5 Other questions

1.5.1. Do you have processes and resources to respond to cybersecurity incidents?

- We have internal resources to respond to incidents
- We relay on external resources to respond to incidents
- No

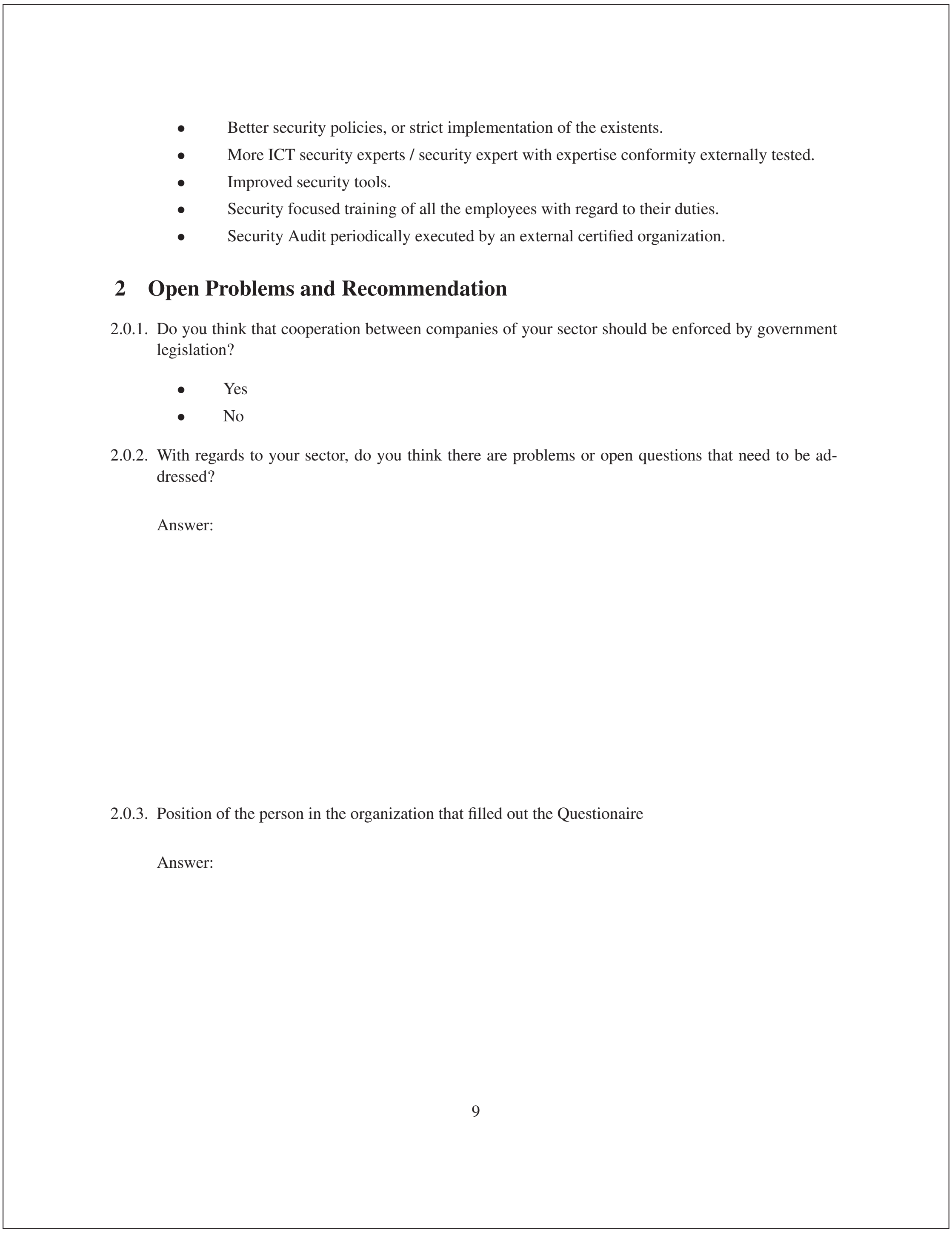
1.5.2. Do you have processes and resources to recover from a significant cybersecurity incident

- Yes
- No

1.5.3. Do you have situational awareness on the state of the cyberthreat to your organization?

- Yes
- No

1.5.4. Do you think that the security of your company could be improved with:



- Better security policies, or strict implementation of the existents.
- More ICT security experts / security expert with expertise conformity externally tested.
- Improved security tools.
- Security focused training of all the employees with regard to their duties.
- Security Audit periodically executed by an external certified organization.

2 Open Problems and Recommendation

2.0.1. Do you think that cooperation between companies of your sector should be enforced by government legislation?

- Yes
- No

2.0.2. With regards to your sector, do you think there are problems or open questions that need to be addressed?

Answer:

2.0.3. Position of the person in the organization that filled out the Questionaire

Answer:

Appendix B: Score Structure of the Cyber Security Readiness Index

		Awareness		Defense		Policy		External independency	
Question	Answer	Positive	Negative	Positive	Negative	Positive	Negative	Positive	Negative
1.2.1	Yes	-	-	-	-	-	-	-	Yes
	Others	-	-	-	-	-	-	-	-
1.2.2	Yes	-	-	-	-	-	-		Yes
	Others	-	-	-	-	-	-	-	-
1.2.4	Yes	-	-	-	-	-	-	-	-
	No	.	Yes	-	-	-	-	-	-
1.2.5	Yes	-	-	-	-	-	-	-	Yes
	No	-	-	-	-	-	-	-	-
1.2.6	Yes	Yes	-	-	-	-	-	Yes	-
	Others	-	Yes	-	-	-	-	-	-
1.3.10	Yes	Yes	-	-	-	-	-	-	-
	Other	-	-	-	-	-	-	-	-
1.3.11	Any Response	-	Yes	-	-	-	-	-	-
1.4.1	Yes	Yes	-	Yes	-	Yes	-	-	-
	Others	-	-	-	-	-	-	-	-
1.4.2	Yes	Yes	-	-	-	Yes	-	-	-
	Others	-	-	-	-	-	-	-	-
1.4.3	Yes	Yes	-	-	-	Yes	-	-	-
	Others	-	-	-	-	-	-	-	-
1.4.4	Yes	Yes	-	Yes	-	-	-	-	-
	Others	-	-	-	-	-	-	-	-
1.4.5	Yes	Yes	-	Yes	-	-	-	-	-
	Others	-	-	-	-	-	-	-	-
1.4.6	Yes	Yes		Yes		Yes	-	-	-
	Others	-	-	-	-	-	-	-	-
1.4.7	Yes	-	-	-	-	Yes	-	-	-
	Others	-	-	-	-	-	-	-	-
1.4.8.1	Checked	-	Yes	-	-	-	-	-	-
1.4.8.2	Checked	Yes	-	Yes	-	-	-	-	-
1.4.8.3	Checked	Yes	-	Yes	-	-	-	-	-
1.4.8.4	Checked	Yes	-	Yes	-	-	-	-	-
1.4.8.5	Checked	Yes	-	Yes	-	-	-	-	-
1.4.10	No	-	Yes	-	-	-	-	-	-
	Others	-	-	-	-	-	-	-	-
1.4.11	Yes	Yes	-	-	-	-	-	-	-
	Others	-	-	-	-	-	-	-	-
1.4.12	Yes	Yes	-	Yes	-	-	-	-	-
	Others	-	-	-	-	-	-	-	-
1.4.13	Yes	Yes	-	Yes	-	-	-	-	-
	Others	-	-	-	-	-	-	-	-
1.4.15	Detect ATP	Yes	-	Yes	-	-	-	-	-
	Normal IDS	Yes	-	Yes	-	-	-	-	-
1.4.17	Yes	Yes	-	Yes	-	-	-	-	-
	Others	-	-	-	-	-	-	-	-
1.4.20	Yes	Yes	-	Yes	-	-	-	-	-
	no	-	Yes	-	-	-	-	-	-

Acronyms

ADI Italian Digital Agenda (Agenda Digitale Italiana)

AIIC Association of Italian Experts in Critical Infrastructure (Associazione esperti Italiani di infrastrutture critiche)

AISE External Security and Intelligence Agency (Agenzia informazioni e sicurezza esterna)

AISI Internal Security and Intelligence Agency (Agenzia informazioni e sicurezza interna)

APT Advanced Persistent Threats

CBRN Chemical, Biological, Radiological, and Nuclear Risk

CCM Computer Cleaned per Mille

CERT-EU Computer Emergency Response Team of European Union

CERT-SPC Computer Emergency Response Team of the Italian Connectivity Public System (CERT Sistema pubblico di connettività)

CERT Computer Emergency Response Team

CESG Communications-Electronics Security Group

CI Critical Infrastructure

CII Critical Information Infrastructure

CIIP Critical Information Infrastructure Protection

CIP Critical Infrastructure Protection

CIRP Critical Infrastructure Resilience Programme

CISO Coordinator of Information System Security

CISR Inter-ministers Committee for the Security of the Republic (Comitato interministeriale per la sicurezza della Repubblica)

CITDC Technical Inter-ministers Commission of Civil Defense (Commissione Interministeriale Tecnica della Difesa Civile)

CIWIN Critical Infrastructure Warning Information Network

CMU Carnegie Mellon University

CNAIPIC National Cybercrime Center for the Protection of Critical Infrastructure (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche)

CNCI Comprehensive National Cybersecurity Initiative

COPASIR Parliamentary Committee for the Security of the Republic (Comitato parlamentare per la sicurezza della Repubblica)

CoPS Political Strategic Committee (Comitato politico strategico)

CPNI Centre for the Protection of National Infrastructure

CPR Cyber Security Policy Review

CSDP Common Security and Defense Policy

CSIRT Computer Security Incident Response Team

CSOC Cyber Security Operations Centre

CTSA Counter Terrorism Security Advisor

DAC Digital Administration Code (Codice dell'Amministrazione Digitale)

DDOS Distributed Denial of Service

DigitPA Italian Agency for Public Administration Digitization (Ente nazionale per la digitalizzazione della Pubblica Amministrazione)

DIS Italian Security Intelligence Department (Dipartimento informazioni per la sicurezza della Repubblica)

DL Ialian Law Decree

DM Italian Ministerial Decree

DPCM Italian President of Council of Ministries' Decree - decreto del presidente del consiglio dei ministri

EC3 European Cybercrime Centre

ECI European Critical Infrastructure

EDA European Defence Agency

EFMS European Forum of Member States

EISAS European Information Sharing and Alert System

ENISA European Network and Information Security Agency

EP3R European Public-Private Partnership for Resilience

EPCIP European Programme for Critical Infrastructure Protection

FMI Financial Market Infrastructure

G-20 Group of Twenty

ICT Information and Communication Technology

ISMS Information Security Management System

MISE Italian Ministry of Economic Development (Ministero delle Infrastrutture e dello Sviluppo Economico)

MSRT Microsoft Malicious Software Removal Tool

NaCTSO National Counter Terrorism Security Office

NCIRP The National Cyber Incident Response Plan

NGN Next Generation Networks

NICE National Initiative for Cybersecurity Education

NIS Network and Information Security

NISP Interministry Unit for and Planning (Nucleo interministeriale situazione e pianificazione)

NSF National Strategic Framework

NSS National Security Staff

NSTIC National Strategy for Trusted Identities in Cyberspace

OCSIA Office of Cyber Security & Information Assurance

OECD Organisation for Economic Co-operation and Development

OMB Office of Management and Budget

PEC Certified E-mail Service (Posta Elettronica Certificata)

PSO Operator Security Plan

SCIIC Inter-Ministers Coordination Secretariat for Critical Infrastructure Protection (Segreteria di Coordinamento Interministeriale per la Infrastrutture)

SIC Secretariat for Critical Infrastructure(Segretaria Infrastrutture Critiche)

SPC Connectivity Public System (Sistema pubblico di connettività)

UACI Cybercrime Analysis Unit (Unità d'analisi del crimine informatico)

ULS Local Security Unit (Unità Locali di Sicurezza)