CIS SAPIENZA

CYBER INTELLIGENCE AND INFORMATION SECURITY

2014 Italian Cyber Security Report

Awareness, Defense and Organization in the Public Sector

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

December 2014

Editors: Roberto Baldoni, Luca Montanari

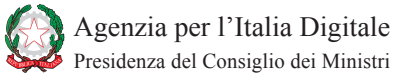
Authors (alphabetical order):

Leonardo Aniello
Stefano Armenia
Roberto Baldoni
Fabrizio D'Amore
Annachiara Di Paolo
Luisa Franchina
Luca Montanari
Ida Claudia Panetta
Leonardo Querzoni
Giovanni Rellini Lerz
Nino Vincenzo Verde

with the help of:

Paolo Agati
Gabriella Caramagno
Mario Cilla
Guglielmo Galasso
Leandro Gelasi
Alessandro Masolin
Diego Mezzina

The 2014 Italian Cyber Security Report has been realized by:



with the participation of the Presidency of Ministry Council (Security Intelligence Department)

with the generous contribution of:

The Cyber Intelligence and Information Security Research Center is a part of the:

Printed in Italy

First printing, December 2014

ISBN X-XXXXXXXXX-X-X

Via Ariosto 25 00185, Roma, Italy

Preface

Within ten years the correlation between the advanced cyber security capability of a nation and its economic prosperity will be an inseparable binomial. To remain in the group of the most developed countries, a nation has then to improve such capability within its industry, government and military sector and in society. This is why each developed country is implementing its own cyber security strategy involving the private sector, the public sector and research. Improving a country's cyber space defenses means, among other things, making the country more attractive for investments by international operators that could see building business realities, such as new companies, in a territory where there is low cyber defensive capability as dangerous. These companies could indeed become a weakness of a multinational corporation. As a consequence, in this millennium, making cyber space a safe place means creating the basis for the independence and the growth of the country.

One year on from the the publication of the Italian cyber security strategy, this report focuses on awareness and defense capability of the Italian public sector. A questionnaire was sent to around 300 national, regional and local public operators: from municipalities to public hospitals, from regional organizations to government ministries. The study has identified many deficiencies but it has also pointed out the path to be taken for achieving a rapid and substantial improvement in the protection of the public sector's cyber space. The study also highlights important gaps both in terms of both security fundamentals and organization. This creates a situation in which only very few public organizations can be considered well aware of the cyber risk while basic errors and ignored security best practices emphasize the deep cultural backwardness of most public sector organizations, in particular, with respect to the understanding of the strategic and economic value of information that could be stolen by such information systems.

It is therefore out duty to younger generations, which will live in a digital world where threats will be persistent and ever-increasing, to secure the national cyber space. It is important to remark that this threat could turn out to be a giant economic opportunity for Italy and for our industrial growth. At the moment, in the cyber security domain Italy possesses top expertise at industrial and research level. Such expertise will be lost in a short time (moving out of Italy) if the government does not set up, fund and implement appropriate actions to create a breeding ground and an attractive place for doing research and development in this domain. Eventually, such actions would represent a double advantage in terms of economic and national independence. Today Italy invests zero in this sector. Other nations comparable to Italy have four year investment plans for cyber security which are worth billions of euros.

Nevertheless to implement national plans there is the need for national actors. This is why the Italian research community in cyber security created the Cyber Security National Laboratory under the CINI umbrella. The Cyber Security National Laboratory affiliates 33 Italian Universities, with a total of 250 faculties, which work together to make our digital lives more secure. We hope that the opportunity offered by the National Laboratory will be supported by the Italian government as a strategic way of funding research and education vital for the country.

Let me finally thank all the authors of this report, the Agency for Digital Italy(AgID, Agenzia per l'Italia Digitale) and the Security Intelligence Department for their collaboration and support. A special thank goes to the three public organizations that acted as case studies for this report, namely INPS, Corte dei conti and Regione Friuli-Venezia Giulia[1]. Thanks also to all the public organization that filled out the questionnaire. The help and comment of Claudio Ciccotelli, Federico Lombardi, Antonella Dal Pozzo and Daniele Ucci was instrumental in improving the content of this report. Finally, it is important to remark that the realization of this report was possible thanks to the generous contribution of MICROSOFT, HP, FireEye and Finmeccanica.

This work is a part of the research activities funded by the Italian Prin project TENACE and by the EU projects Panoptesec, Cockpit-CI e T-NOVA.

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

Roma, 22 Dicembre 2014

[1] Case studies are only present in the Italian version of the report.

Contents

List of Recommendations

CHAPTER

1 Introduction

In the nineties, the Italian government introduced an important plan aimed at introducing IT tools into every level of the public sector. This plan commits to employing IT as a basic element for the execution of every process within the public sector with the three-fold goal of i) fostering the simplification of the procedures, speeding up their execution, and thereby improving the quality of the services and how such quality is perceived by citizens, ii) making the provision of these services more economical so as to reduce the impact of administrative machinery on the national budget and, finally, iii) reaching citizens more easily by fostering their interaction with public bodies thanks to the employment of the most modern IT means, which citizens are able to handle much more quickly than the public bodies can. Many processes so far have been based on the use of hardcopy documents and on the direct interaction among employees. The effort of transforming them into highly computerized processes where documents are totally dematerialized takes time. Although remarkable, results are still heterogeneous today within the public sector. Electronic invoicing is a nationwide example of good practice, whereas, at a local, the spread of IT (and the computerization of processes) has been heterogeneous and with results mainly subjected to the vision of local managers or to the initiative of individuals having advanced IT backgrounds. Such progressive modernization, which we hope will change sharply in speed and scale, will lead to an ever increasing interaction between citizens and their institutions through IT channels. Such a vision is already partially present today. Processes like electronic invoicing, verification of citizens' tax status, and online legal procedures and cases, are relevant examples of this modernization. This evolution entails several advantages, but it will surely make citizens rely much more on IT tools during their everyday lives, which in turn renders the public sector IT infrastructure even more of a critical infrastructure for Italy.

Therefore the great opportunities provided by this evolution also come with the risks deriving from an increasing exposure to cyber attacks. These kind of illegal activities already impact on citizens during their everyday interactions *online*, and will impact their everyday lives even more negatively by damaging the preferential and trusted connection between citizens and public bodies. In particular, from this point of view, public entities pay the price of thier own identity by becoming key targets for demonstrative attacks (hacktivism). The main goal of these attacks is the reduction of a country's capabilities to directly interact with its citizens by preventing or undermining such interaction, or by intercepting and modifying its contents so as to transmit propagandist messages through a channel that has so far been considered "reliable".' In addition to hacktivism, the sector becomes a favorite goal for reconnaissance and spying activities, directly or indirectly carried out by foreign agencies interested in obtaining confidential information that the sector itself should protect. It is indeed important to note that, as well as a country defending its own geographical borders against undesired intrusions by foreign elements, it should also identify and protect cyber borders where direct and widespread control can be enforced. Such borders should comprise and preserve all the information and services relevant for the country, and thus should include all public sector IT services.

The recent publication of the *Quadro strategico nazionale per la sicurezza dello spazio cibernetico* (National Strategic Framework for Cyber Space Security) has explained this aspect, but its implementation will need sig-

nificant effort over the next years. Meanwhile, threats don't stop and today the status of public secor protection from attacks is very fragmented. Indeed, especially for organizations of minor size, such protection has relied on the good will of local managers who, because of their skills or thanks to good advice, became aware in time of the dangers citizens were exposed to because of an inaccurate protection of their services and data. Only public sector operators of major size and relevance, having at their disposal appropriate means and budgets, have been able to address the problem systematically, but even in this case the approaches have been heterogeneous and consequently led, in the best scenario, to an extreme or at least avoidable waste of resources.

By operating in a situation of extreme fragmentation, without any institutional reference point except for traditional police authorities, during the last years the Italian public sector has experienced a situation in which security culture has not depended on the government, but rather on the skills of single managers. Since laws or regulations at this level do not exist, it is thus obvious that only the entities that are aware and economically strong have been able to develop a proper awareness of the problem. Up till now, all smaller size public bodies like municipalities, provinces, local health boards and hospitals are in a critical situation. Yet, these are often responsible for directly managing citizens' data and providing their main services.

This all takes place in a time when cyber crime has radically changed, because the attacker himself has radically changed. In less than 10 years, we have moved from a lot of isolated and disorganized attackers, composed of fanatics looking for a few hours of frivolous glory, to big groups of organized and professional hackers, funded sometimes by governments, sometimes by crowdfunding, and sometimes by organized crime. Anonymous is a relevant example, operating very intensively in the Italian territory. There has been an increase in the availability of powerful hardware and of *malware* that are more complex than in the past. These malware install daemons, which appear as idle, into single devices (e.g., domestic PCs, smartphones, servers and NASs). These daemons can act simultaneously even on a global scale, thus enabling even small groups of attackers to launch big attacks.

It is indeed a recognized idea within the cyber security community that the effects of a cyber attack, led accurately and towards specific targets, would be the same as a military attack, in economic terms. It is not possible to estimate with certainty the damage large attacks could cause, just as it is not possible to estimate the damage military attacks could cause. For instance, consider the consequences of a one week total blockage of the Italian stock market, or the unavailability of registry services in the biggest cities like Rome or Milan for one week. Or a large local health body serving thousands of persons that cannot provide its services anymore. Delays would accrue, people would be forced to use their vacation days to come back again to ask for these services, with all the consequences that this would entail, for example this increased movement of people would have implications on the traffic and so on. Another example is the National Institute for Social Welfare (INPS, Istituto Nazionale Previdenza Sociale): consider the effects of an attack lasting for two weeks against such an organization, with millions of people unable to get their public welfare on time. It would be chaos.

Up till now, no cyber attack of such size has been documented in Italy, nevertheless it would be wrong to assume that the Italian public sector cannot be a target for spying or attacks funded by other countries. On the contrary, latest events regarding Regin malware [1] lead to the supposition that the public sector is already being targeted by spying activities. All of this suggests that in terms of security the possibility that the enemy is already among us should be taken into account. Nevertheless other reports, in particular CLUSIT 2014 [2], document a long list of attacks carried out against public authorities between 2013 and the beginning of 2014.

In this context, the Research Center of Cyber Intelligence and Information Security "Sapienza" University of Roma, in collaboration with AgID and the Security Intelligence Department, has carried out research aimed at a detailed understanding of public sector awareness of the cyber threat and its present defense capability. With this aim, between June and August 2014, *441* questionnaires were delivered to the same number of public authorities at national, regional, provincial and municipal (where there are more than 1,000 citizens resident) level, as well as to local health boards and hospitals. The questionnaire was organized into 61 questions on topics related to

[1] Regin was discovered by KAspersky Lab on November 2014 and is a sophisticated malware able to steal and gather information of distinct types: file, voice, data, etc. It is suspected that it was developed by the United Kingdom and the United States of America with the aim of monitoring European Commission buildings through Belgacom, a telco provider for several structures within the European Commission.

[2] `https://www.clusit.it/`

the entity's awareness, defense and organization, and was delivered with the fundamental support of the highest managerial levels of AgID. The answers were analyzed in order to produce a realistic picture at the national level.

Positive and negative aspects emerged from this analysis, resulting in an overall picture which, as mentioned above, can been defined at the very least as heterogeneous. The results clearly highlight that some public sector organizations at a national level are better prepared than local ones. In the latter the situation is extremely fragmented, presenting few cases of excellence and many critical cases. *However, it is fundamental to highlight that the results reported in this document must not be interpreted as a guarantee that those public bodies with high scores are safe*; quite the opposite. Having been exposed to major risks, they have undertaken for a longer time the path that smaller public operators will necessarily have to undertake. The sooner this step is taken, the fewer the risks will be for the citizen and for the country.

Chapter 3 shows the results using three *Key Performance Indicators (KPI)*, specifically *awareness*, *organization* and *defense*. The first evaluates public sector awareness of cyber issues, the second assesses how it is prepared in terms of policy and management, and the third ponders the technological defenses employed against cyber threats.

Besides the absolute values for each category, results are presented based on the size of the entity, geographical location and number of attacks experienced. Finally, a statistical analysis of the answers is presented which highlights the characteristics of organizations that have similar scores in the three KPI.

Some conclusions are drawn from these results and presented as a list of recommendations. Besides technical recommendations for the public sector aimed at improving their security levels, further relevant concepts have been deduced, among which:

- the process of rationalizing the informational assets of the public sector in terms of data, process and infrastructures, and the management of security are an inseparable pair. Only by reducing the attack surface can the security of a national infrastructure be said to be effectively managed. This can be done today by means of appropriate data centers, for instance employed on a regional base, which can also result in huge saving for the public treasury;
- the framework of expertise and responsibilities, deriving from the strategic plan for national cyber security concerning prevention, management and response to cyber attacks, is large and irregular. It is thus advisable to move to a centralization of such expertise and responsibilities so as to make the chain of command faster and more coordinated.

The document is organized as follows: research methodology is presented in Chapter 2, Chapter 3 describes the results and Chapter 4 concludes the report by presenting and explaining a series of recommendations. The graphs representing the answers to the questionnaire can be found in the Appendix.
The english version of the Italian Cyber Security Report 2014 does not contain three case studies, namely Corte dei conti, Friuli-Venezia Giulia region and INPS. Interested readers may refer the Italian version available at `www.cis.uniroma1.it/csr2014`**.**

CHAPTER

2 Survey Evaluation Methodology

In order to provide an objective value that consicely describes the public sector's level of preparation with respect to cyber security, three Key Performance Indicators (KPI) have been identified. The answers to the survey's questions affect, through a weighted mechanism, the score achieved in each of the KPI.

In the following, we describe the KPIs and the survey. Next we explain the association between the survey questions and the affected KPIs. Finally we provide some details on the scores computation.

2.1 Key Performance Indicator

A Key Performance Indicator is an index used to monitor the performance of a business process. We have identified three KPIs measuring three different aspects of public sector preparation when facing cyber security events: *Organization* KPI, *Defense* KPI, *Awareness* KPI.

The *Organization* KPI covers all those organizational aspects that directly affect the response capabilities to cyber attacks. As is known, an organization that pays attention to security issues is most likely to have better proactive and/or reactive response capabilities.

On the other hand, the *Defense* KPI covers all the technical aspects related to the capability of the organizations to defend themselves from cyber attacks. This KPI covers the presence or absence of proper security technical measures, such as firewalls, intrusion detection systems, antivirus and secure communication protocols for the provided services, as well as the use of obsolete technologies which are widely known to be vulnerable.

Finally, the *Awareness* KPI covers organizations' awareness levels with respect to cyber security issues. Notice that, in general, awareness is one of the most relevant aspects as it enables an organization to improve its capability. This is particularly true when we talk about cyber security. Indeed, not being aware of the threats often leads to paradoxical situations in which an entity thinks it is safe, and not under attack, whilst being *constantly* attacked.

2.2 Survey and questions

The survey was submitted to various arms of the public sector and is composed of 61 questions which are structured as follows:

- the first 15 questions identify the role of the respondent within the public sector, the type of organization, its size (in terms of number of branches, number of users served, number of employees, number of data centers), the type of processed data and the possible level of criticality of the provided services;
- questions 16 to 28 are related to the techniques used by for data protection, the technologies used for authentication and remote access, and the web technologies;

- questions 29 to 42 are related to cyber attacks and their prevention, data protection measures and employee training;
- questions 43 to 47 are devoted to software and its updating;
- questions 48 to 61 are devoted to organization and security policy.

All questions are reported in the appendix, each one with the related results aggregated by category.

2.3 Questions-KPIs association

Table 2.1 shows the association between questions and KPIs. Saying that a question is associated with a KPI means that the question affects the computation of the score of that KPI. Notice that size, i.e., the number of employees, branches and registered users, is taken into account for the evaluation of the *Organization* and *Defense* KPIs and is deduced from questions no. 4, 5 and 14, as highlighted in the *Size* column of the table. The size assessment is important for showing some critical aspects of the infrastructure: we believe that for bad practices it is fair to penalize smaller organizations less than larger ones. Similarly, one should be more demanding of public entities that manage a larger amount of data and assets. In order to take into account the size within the identified KPIs, we have defined two multiplicative factors, fm and fp (more details below), affecting respectively the *Defense* and the *Organization* KPIs.

Table 2.1: Association between questions and KPIs.

Questions		KPI		Size
	Organization	Defense	Awareness	
4,5,14	✓	✓		✓
16,20,25,30,31,34-37,43,45		✓		
12,21,23,26,28,29,32,33,44		✓	✓	
22,27,38,40	✓	✓		
15,39,42,46,47	✓	✓	✓	
48,50,52,56-60	✓		✓	
13,49,51,53-55	✓			

2.4 Score computation

The process of scores computation begins with the collection of the answers to each question from each respondent and ends with the production of three values: $< O_i, D_i, A_i >$ within the range $[0,100]$. These values represent, respectively, the score obtained by the operator i for the *Organization, Defense, Awareness* KPIs. According to the association presented in Table 2.1 and the evaluation of the provided answer, each question of the survey may contribute positively or negatively to the computation of the score associated with each KPI. The contributions of the individual questions are totaled and normalized enabling a faster comparison between the various KPIs. In the following we explain the KPIs computation.

Considering the KPI *Defense* and a generic public opertaor a, let:

- S_P be the sum of the positive scores obtained by the operator a for the questions affecting the considered KPI;
- S_N be the sum of the negative scores obtained by the operator a for the questions affecting the considered KPI;

Moreover, let:

- fm be a multiplicative factor calculated from a subset of the answers provided by the operator a.

The sum of the negative scores S_N is multiplied by the factor, thereby obtaining the penalized sum of negative scores:

$$S_{Np} = S_N \times fm.$$

S_{Np} is added to S_P to obtain the total score for the KPI *Defense*:

$$S_D = S_{Np} + S_P,$$

note that $S_N \leq 0$. Let

- Max_D and min_D be, respectively, the achievable maximum and minimum of the sum of the scores associated with all those questions affecting the *Defense* KPI.

In particular, Max_D is the sum of all achievable positive scores and min_D is the sum of the negative scores. Max_D and min_D are computed a priori and are, therefore, independent from the answer of the individual entity. The score D_a associated with the *Defense* of the operator a is computed as follows:

$$D_a = \left(\frac{(S_D - min_D)}{(Max_D - min_D)} \right) \times 100,$$

namely, applying the well known *min-max normalization* formula to S_D. The process is easily generalizable to the other KPIs through the same procedure. Notice that the maximum and minimum values are different for each KPI and that the fm factor exists only for the *Defense* KPI. With regard to the *Organization* KPI, a different multiplicative factor, fp, is applied to the sum of the positive scores. The total score for the KPI *Organization* is:

$$S_O = S_N + S_{Pp},$$

where $S_{Pp} = S_P \times fp$. Such a multiplicative factor is used to understand the increased complexity in the organization of larger public operators, therefore it rewards larger entities that use good practices. Regarding the other KPIs, large entities are penalized for bad practices.

2.5 Scores, qualification threshold and charts interpretation

To ease the interpretation of the results obtained from the survey, we have defined a threshold above which a public sector entity can be considered sufficiently careful about the issues arising from cyber threats. Such a threshold is meant as a qualification threshold, meaning that those obtaining a higher score have implemented basic devices, both technological and organizational, suitable with respect to the state of the art. Obtaining a score above such a threshold does not guarantee that the organization is immune to successful attacks. Rather, obtaining a score above the threshold translates into being able to detect, for instance, data leaks or other kinds of high probability attacks, and being able to solve such problems as quickly as possible.

The qualification threshold has been calculated by taking into account the individual questions of the survey, the influence of each possible answer on each KPI and the presence or absence within the organization of the minimal measures that an organization should provide to consider itself reasonably safe from generic threats. It is worth stressing again that a public body obtaining a score above the threshold cannot consider itself safe, but rather being on the right track. It should also be noted that such an entity cannot consider itself safe from threats specifically tailored against the organization (for instance, APT attacks). Conversely, an organization that obtains a score below the qualification threshold must consider itself at high risk.

In the charts of the following chapters, the areas above the identified threshold are highlighted in green. The areas highlighted in yellow are border areas, with substantial room for improvement, but to be considered at medium/high risk. Finally, the areas with white background are to be considered as areas of severe insufficiency.

CHAPTER

3 Data analysis

This chapter will present the aggregated results of the survey so as to ensure the anonymity of the respondents.

3.1 Sample analyzed and methodology of data collection

The sample analyzed has been gathered in collaboration with AgID. The public sector has been divided into 5 different tpes:

- national authorities, including governement ministries and agencies, which operate at a national level (PAC, Pubbliche Amministrazioni Centrali);
- the 117 municipalities which are the administrative centers of Italy's provinces;
- regions and regional organizations;
- hospitals;
- local health boards (ASLs, aziende sanitarie locali).

During May and June 2014, AgID sent communications, asking for a contact person able to fill in the survey. The communication was sent to:

- 42 PACs;
- 117 municipalities;
- 19 regions, asking them to forward the communication to ASLs and hospitals.

The first result of this report shows the number of contact persons received from AgID, and also the number of organizations that were not able to either receive the communication or to find a contact person within its organization:

- of the 117 municipalities contacted by AgID, 83 provided a contact person. Of these 83, 79 answered the survey. This represents 71% of municipalities.
- all the 42 PACs contacted provided a contact person and all of them answered the survey;
- all the 19 Italian regions contacted provided a contact person and filled out the survey.

It is not possible to know exactly the number of hospitals and health boards that received the communication as this was forwarded by the regions. However, the following considerations about the representativeness of the sample hold:

- 43 of the 140 ASLs in Italy provided a contact person and received the survey. 34 filled it in. This is around 25% of the total.
- 34 of the 645 hospitals in Italy provided a contact person and received the survey. 29 filled it in. This is 4.5% of the total.

All of the contact persons provided by AgID to CIS received the survey. Table 3.1 shows the number of surveys sent and received, with the percentage of reception, according to its category.

Table 3.1: Number of surveys sent and received for each category

	PAC	Municipalities	Regions	Hospitals	ASL	Tot.
Sent	42	83	30	34	43	232
Received	42	79	25	29	34	209
Perc. Reception	100 %	95,2 %	83,3 %	85,3 %	74,4 %	90,1%

The public sector organizations are distributed throughout the territory according to what Figure 3.1 shows. The PACs are excluded from this representation as they are all located in the city of Rome. The only region with no contact person was Molise.

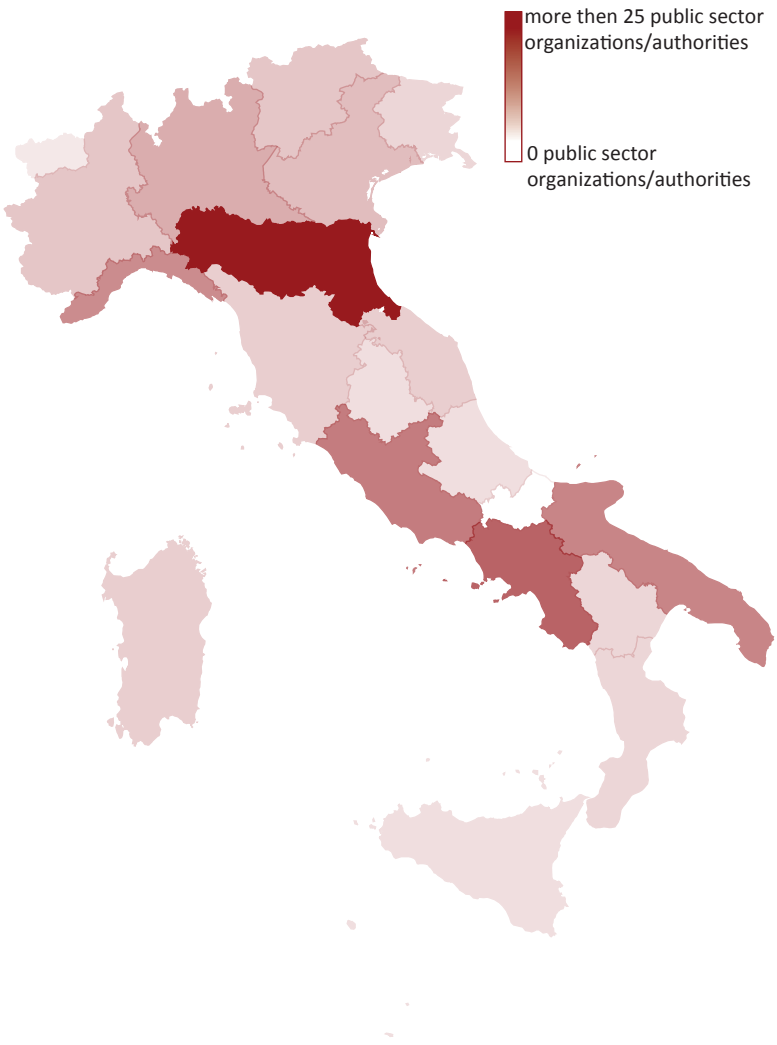


Figure 3.1: Distribution of public sector organizations/authorities across Italy.

3.2 Comparison between the mean values of all categories

The first result presented compares the 5 different categories examined. The mean value of the KPIs for each category is shown in Figure 3.2. It is possible to note the mean value is not close to the eligibility threshold for any category. The figure shows that the PACs and the regions perform better than municipalities, ASLs and hospitals, moreover the latter three categories have very similar results. In Figure 3.2, the error bars represent the standard deviation of considered sets. It is possible to note that the latter rarely surpasses 10 units.

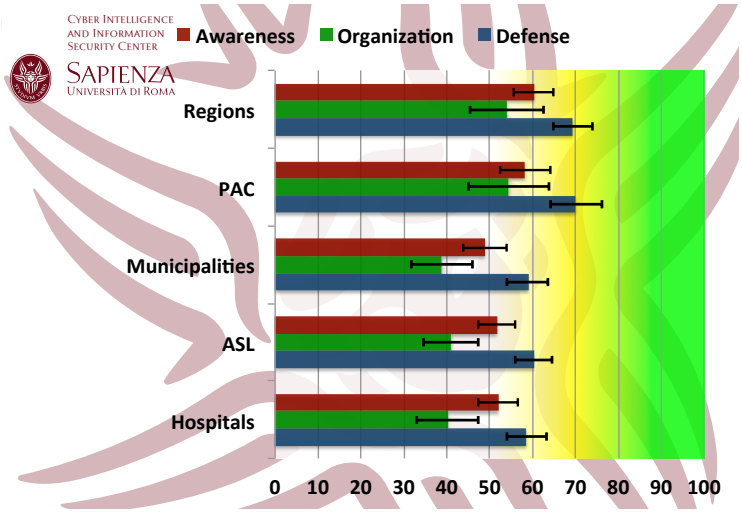


Figure 3.2: Average results for categories, where the error bars represent the standard deviation.

3.3 Comparison between the absolute values of the entire public sector

Figures 3.3, 3.4 and 3.5 show the placement of each organization in terms of *Defense*, *Organization* and *Awareness*. Specifically, the figures show the situation by considering on the axis all the possible KPI pairs: *Defense-Organization*, *Defense-Awareness* and *Organization-Awareness*. Each point in figures represents a public organization/authority and its color represents the relative category. It is possible to notice a high level of correlation between the KPIs (the set of the points is grouped in the plane) which suggests that high levels of *Organization* imply high levels of *Awareness* and *Defense*. It can be seen that few operators are in the green zone (i.e., surpass the

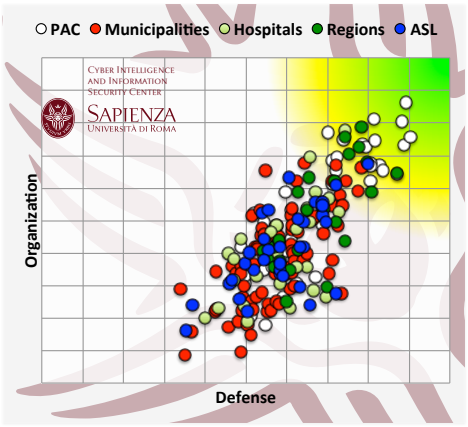


Figure 3.3: Comparison Defense-Organization for each category.

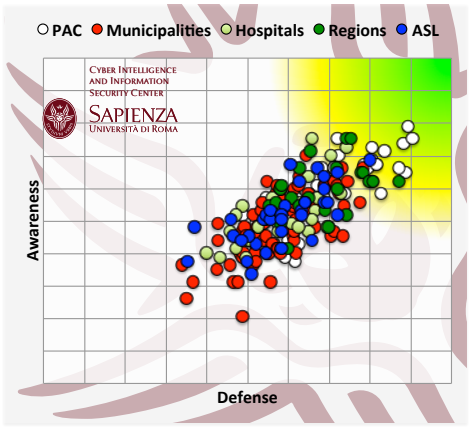


Figure 3.4: Comparison Defense-Awareness for each category.

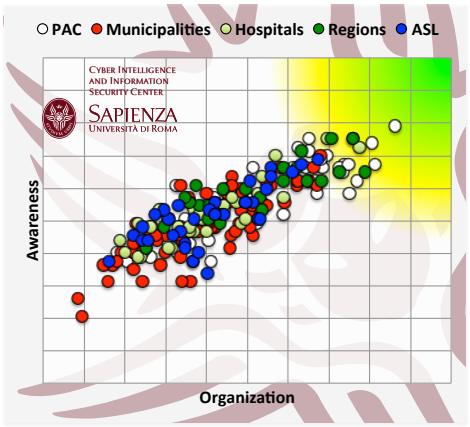


Figure 3.5: Comparison Organization-Awareness for each category.

eligibility threshold) and all of them belong to the PAC category, while the majority of the others are in the white zone i.e., they are seriously unprepared in terms of cyber security.

3.4 Results for single categories

In this section the results obtained from each category of the public sector are shown by comparing *Defense-Organization*, *Defense-Awareness* and *Organization-Awareness*.

3.4.1 National authorities/PACs

The results of the PACs range in the interval [50,90] regarding the KPI Defense, [40,80] regarding the KPI Organization and [50,75] regarding the KPI Awareness. Although the situation of the PACs is basically better than the other categories, few of them score moe than 80, specifically 12 out of 42 for the KPI Defense. Regarding the KPI Organization, only 3 have a score of 80 and the majority of the others are far from this threshold. A similar, but slightly worse, result regards *Awareness*. It can be noted that in general a much more serious situation for 22 of the national bodies (i.e., 50% of the sample) with very low levels of *Organization* and *Awareness*, and *Defense* at less than 70.
These results are presented in Figure 3.6 which shows the values of *Defense* in relation to the values of *Organization*, in Figure 3.7 which shows the values of *Defense* in relation to the values of *Awareness* and finally in Figure 3.8 which shows the values of *Organization* in relation to the values of *Awareness*. By analyzing Figure 3.6, it possible to note how the points are clustered into two distinct groups. The first group contains the points with Organization and Defense greater than 70, while the second group contains those with lower points. In Section 3.8 this situation will be investigated in more detail and will show the reasons that cause a division of the set into two parts (see Figure 3.42).

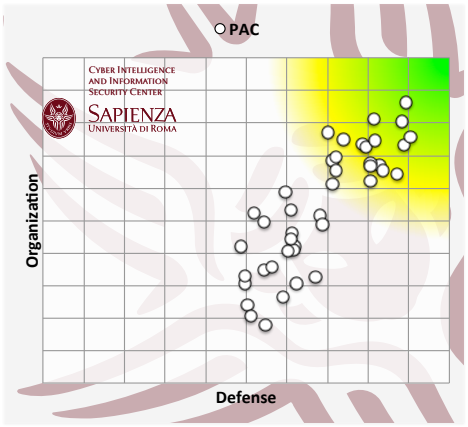


Figure 3.6: Comparison Defense-Organization for the PACs.

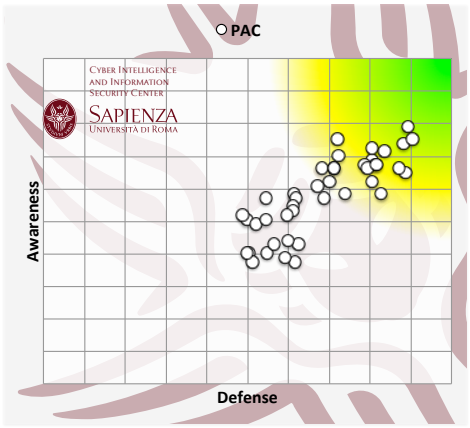


Figure 3.7: Comparison Defense-Awareness for the PACs.

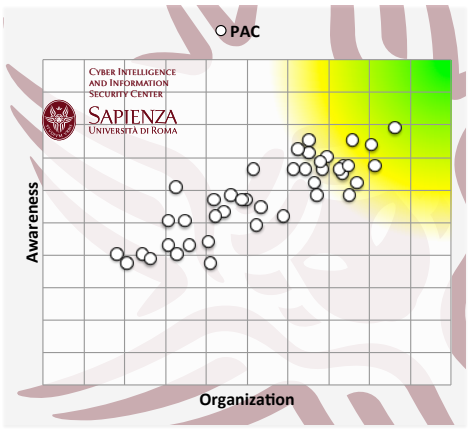


Figure 3.8: Comparison Organization-Awareness for the PACs.

3.4.2 Regions

The results of regions and regional organizations range in the interval [54,87] regarding the KPI Defense, [40,64] regarding the KPI Organization and [50,62] regarding the KPI Awareness. The Figures 3.9, 3.10 and 3.11 show respectively the trend of the KPI pairs*Defense-Organization*, *Defense-Awareness* and *Organization-Awareness* for regions and regional organizations. It is possible to notice how these results are lower than the results obtained by the PACs, specifically regarding the maximum values of all three KPIs. In this case, only 3 regional organizations surpassed the score of 80 for the KPI *Defense*, 2 surpassed 80 for the KPI *Organization* and 2 surpassed 80 for the KPI *Awareness*. It is evident how none of them are in the green zone and how a considerable number of the organizations (14 out of 25) does not surpass both the score of 50 in *Organization* and 70 in *Defense*.

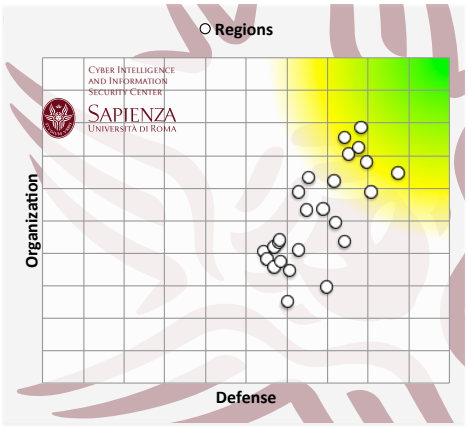


Figure 3.9: Correlation Defense-Organization for the regions.

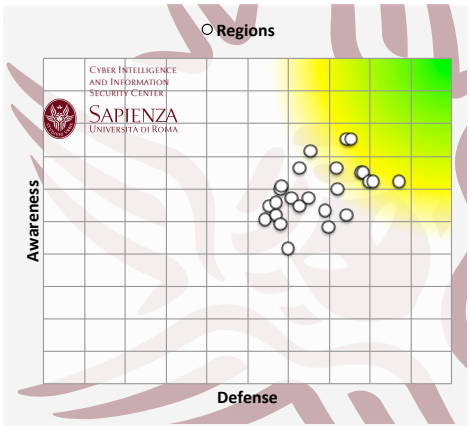


Figure 3.10: Correlation Defense-Awareness for the regions.

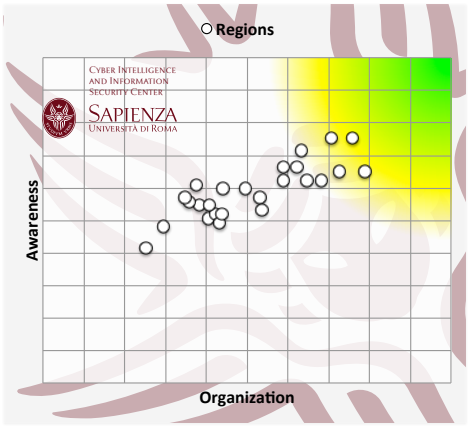


Figure 3.11: Correlation Organization-Awareness for the regions.

Single regions and regional organizations

In Figures 3.12, 3.13, 3.14 the situation of all the categories belonging to three single regions are reported as examples. It is possible to notice how there is always an organization that acts better than the others. This means that the fragmentation of IT among the regional authorities and bodies leads to to conflicting results. The aforementioned three regions are examined in Section 3.8 so as to work out the connection between the organizations that show better regional results.

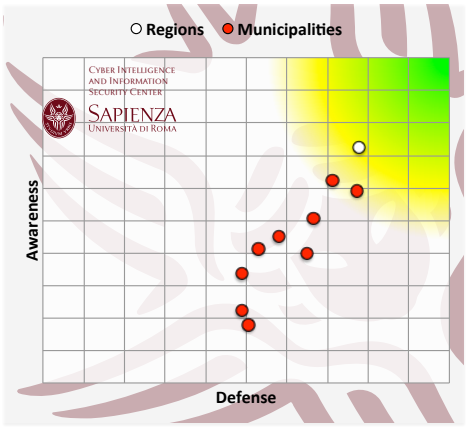


Figure 3.12: Situation of a single region (Region 1).

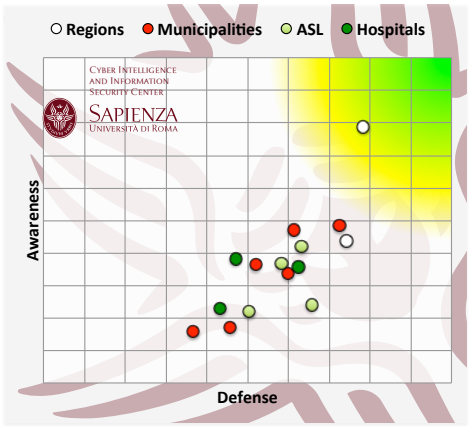


Figure 3.13: Situation of a single region (Region 2).

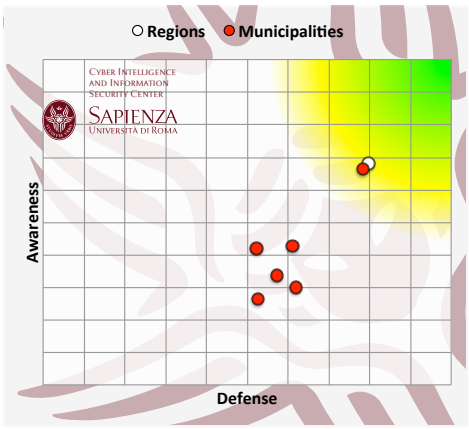


Figure 3.14: Situation of a single region (Region 3).

3.4.3 Municipalities

The results of municipalities range in the interval [33,78] regarding the KPI Defense, [28,68] regarding the KPI Organization and [36,70] regarding the KPI Awareness. None of the municipalities has achieved a score of 80 or more for the KPI *Defense* and only 11 out of 79 of them have a score greater than 70. For the other KPIs the situation is worse. In general the municipalities are the category that on average perform worse than the others (see the results shown in Figure 3.2) regarding the KPI *Awareness* and *Organization*, even though they have similar behaviour to ASLs and hospitals regarding the KPI *Defense*. The Figures 3.15, 3.16 and 3.17 show such results.

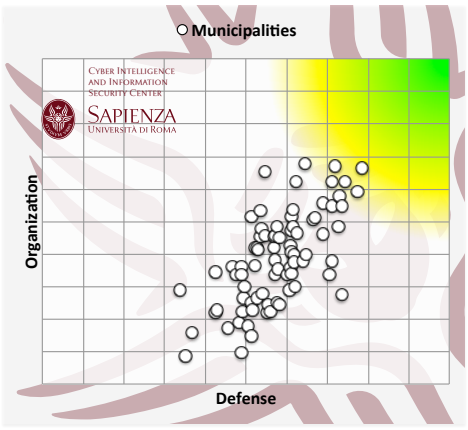


Figure 3.15: Correlation Defense-Organization for the municipalities.

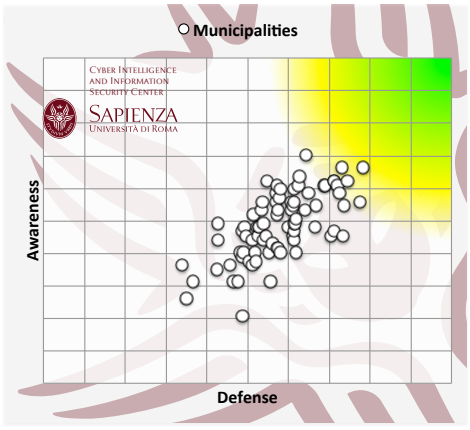


Figure 3.16: Correlation Defense-Awareness for the municipalities.

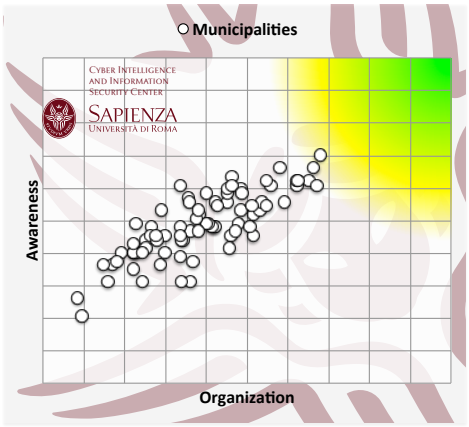


Figure 3.17: Correlation Organization-Awareness for the municipalities.

3.4.4 Local health boards/ASLs

The ASLs range in the interval [35,80] regarding the KPI Defense, [16,67] regarding the KPI Organization and [37,68] regarding the KPI Awareness, whish illustrates very similar behaviour to municipalities. Such results are shown in Figures 3.18, 3.19 and 3.20.

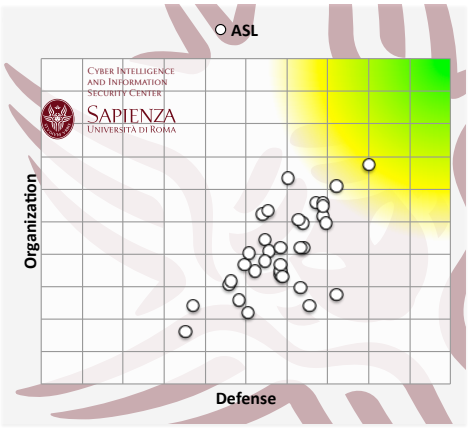


Figure 3.18: Comparison Defense-Organization for the ASLs.

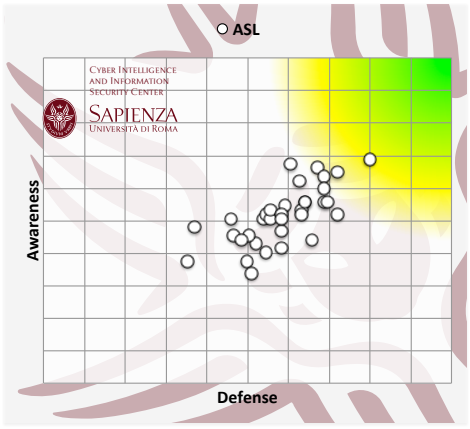


Figure 3.19: Comparison Defense-Awareness for the ASLs.

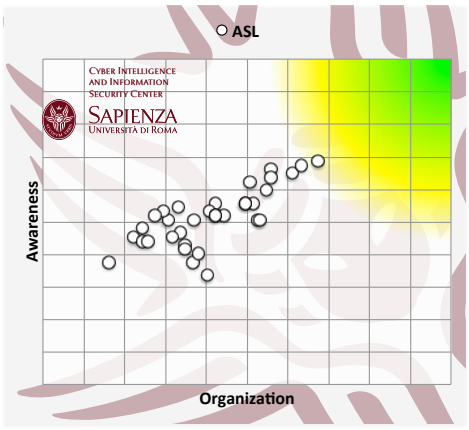


Figure 3.20: Comparison Organization-Awareness for the ASLs.

3.4.5 Hospitals

Hospitals range in the interval [40,74] regarding the KPI Defense, [20,77] regarding the KPI Organization and [40,72] regarding the KPI Awareness, thus showing a slightly better result than municipalities and ASLs. In this instance, like for the ASLs, there are cases where *Organization* is far from the value obtained in the KPI *Defense*. The Figures 3.21, 3.22 and 3.23 compare the KPI and show such cases. It is possible to notice how on average hospitals and municipalities are far from the eligibility threshold. In this case, the correlation value is slightly less.

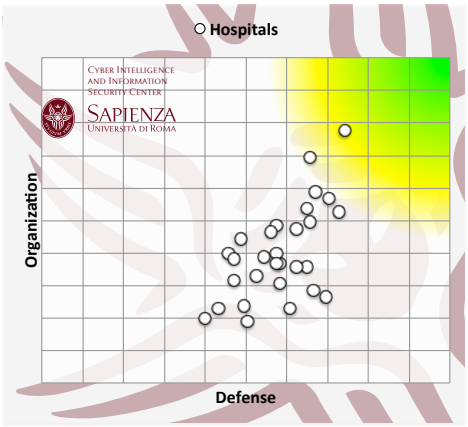


Figure 3.21: Comparison Defense-Organization for the hospitals.

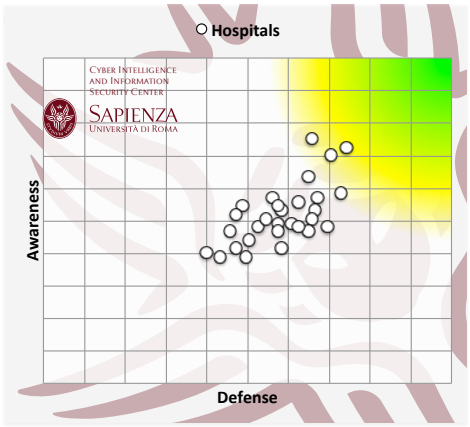


Figure 3.22: Comparison Defense-Awareness for the hospitals.

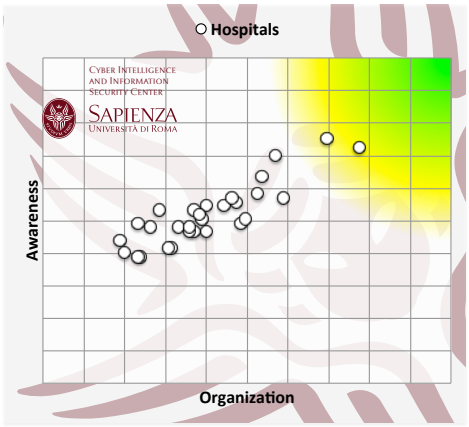


Figure 3.23: Comparison Organization-Awareness for the hospitals.

3.5 Results based on organization size

In the following section average results are reported. These depend on one of the survey size parameters, namely the number of customers served by the organization. In Figure 3.24, an ordering of the results can be seen: those serving a greater number of citizens get, on average, higher values for the three KPIs.

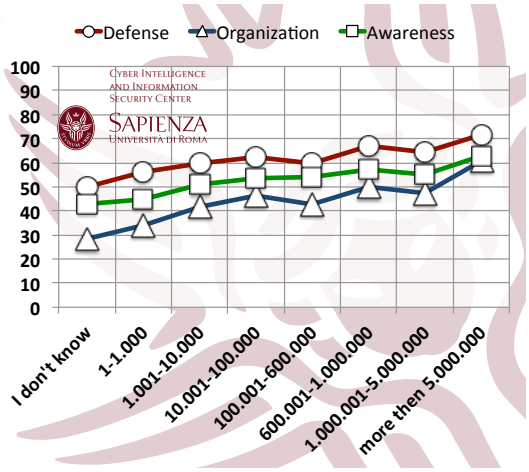


Figure 3.24: Comparison among organizations based on the number of customers served.

If average results are filtered, by analyzing the ones related only to PACS in regard to the number of customers served, the graph depicted in Figure 3.25 is obtained. Although the results are slightly worse than PACs which supply services to up to 1000 customers, they do not show a real correlation between size and results. The same analysis is valid for ASLs (Figure 3.27) and regions (Figure 3.28). Municipalities and hospitals (Figures 3.26 and 3.29, respectively) reveal a size-results correlation. It is worth noting that the organizations which have answered "I don't know" to the question regarding the number of customers served have on average the worst results.

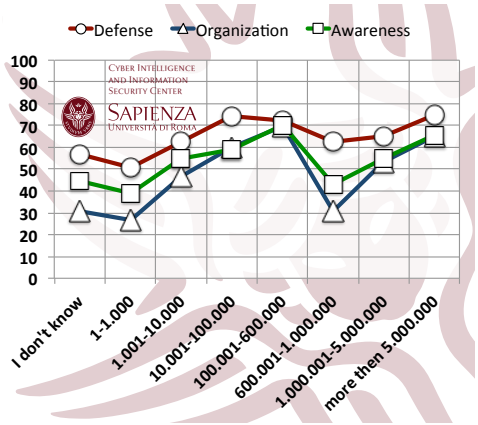


Figure 3.25: PACs results based on the number of customers served.

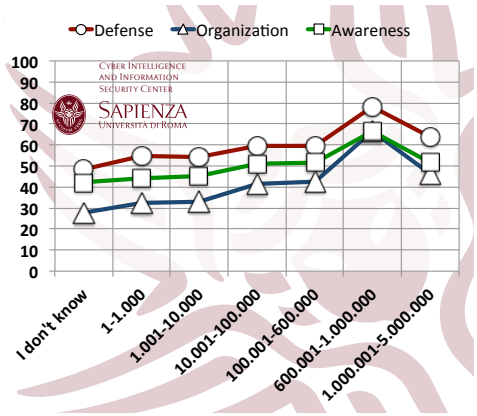


Figure 3.26: Municipalities results based on the number of customers served.

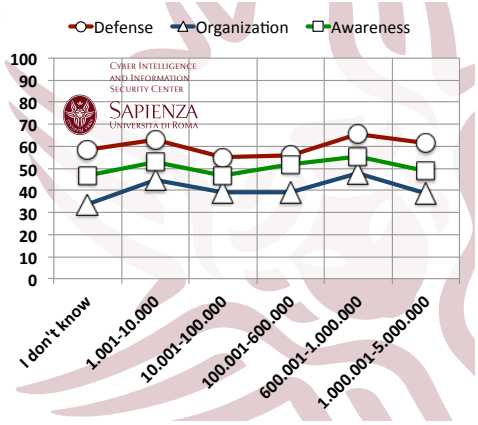


Figure 3.27: ASLs results based on the number of customers served.

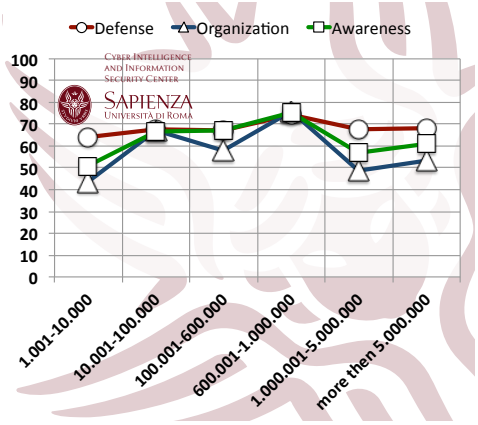


Figure 3.28: Regions results based on the number of customers served.

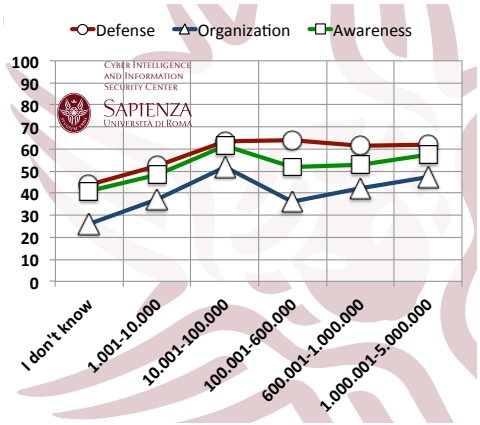


Figure 3.29: Hospitals results based on the number of customers served.

3.6 Results based on geographic location

It is useful to compare results according to the geographic location of public entities. In this regard, municipalities, regions, ASLs and hospitals have been classified according on Table 3.2, which in turn is based on the classification of The Italian National Institute of Statistics (ISTAT, L'Istituto nazionale di statistica). The PAC category is not taken into account because, by definition, every PAC provides services to the entire population.

Table 3.2: Geographic areas - Regions

North	Emilia-Romagna; Friuli-Venezia Giulia; Liguria; Lombardy; Piedmont; Trentino-Alto Adige; Aosta Valley; Veneto;
Center	Lazio; The Marches; Tuscany; Umbria;
South	Abruzzo; Basilicata; Calabria; Campania; Molise; Sardinia; Apulia; Sicily;

The municipalities and hospitals categories reveal strong correlation between geographic location and results: the municipalities and hospitals of northern regions have on average better results than their central conterparts, while these latter ones show better results than southern ones. These values are reported in Figures 3.31 and 3.33. ASLs and regions present contrasting results: there is no well-defined ordering for the different KPIs, based on geographic location. Regarding ASLs, their KPI *Defense* in the s South is better than in the Center and the North; this does not occur for the KPI *Organization*, which is actually ordered. Central regions have the worst results for the KPI *Awareness*. As regards regions, the Center shows on average worse results than the South, while the North obtains better results than the South (Figure 3.30).

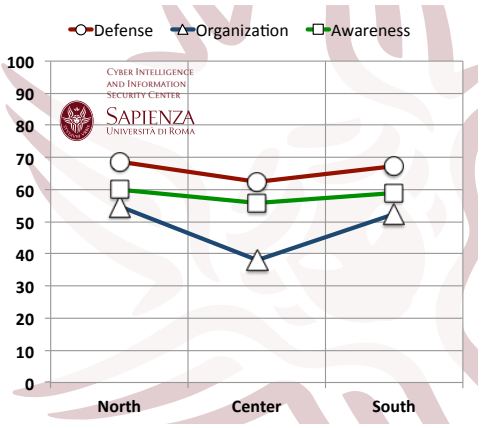


Figure 3.30: Results based on geographic location of regions.

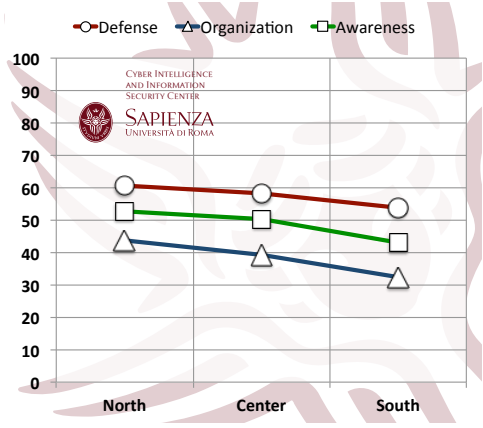


Figure 3.31: Results based on geographic location of municipalities.

Figure 3.31 depicts the average value of the KPIs related to municipalities according to their geographic area. It is worth mentioning the gradual deterioration, from north to south, of all the KPIs.

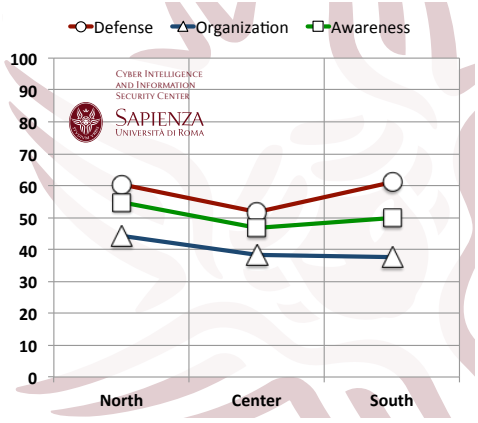


Figure 3.32: Results based on geographic location of ASLs.

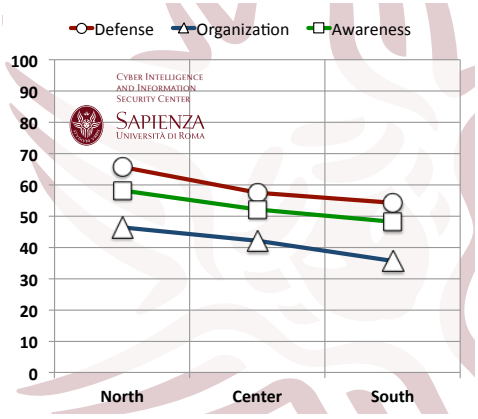


Figure 3.33: Results based on geographic location of hospitals.

Figure 3.33 reports the average values for the three KPIs depending on the geographic location of hospitals. Like municipalities, a degradation of the KPIs based on geographic location occurs.

3.7 Results based on attack attempts suffered

It is important to correlate the number of attack attempts, suffered by the public sector in 2013, to the overall results obtained for the three KPIs. Figure 3.34 reports, on the x- and y-axes respectively, the declared number of attack attempts and the average value of the three KPIs. It is worth noting that on average the organizations

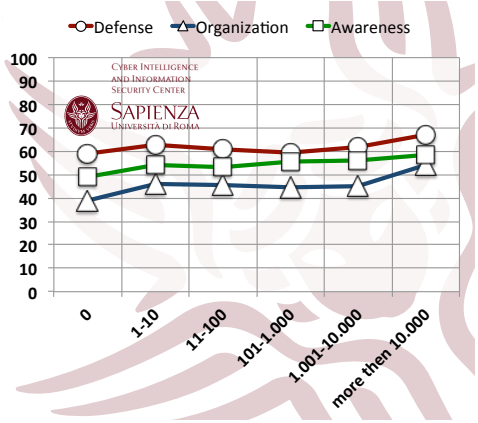


Figure 3.34: Evolution of the KPIs in relation to the number of attack attempts suffered in 2013.

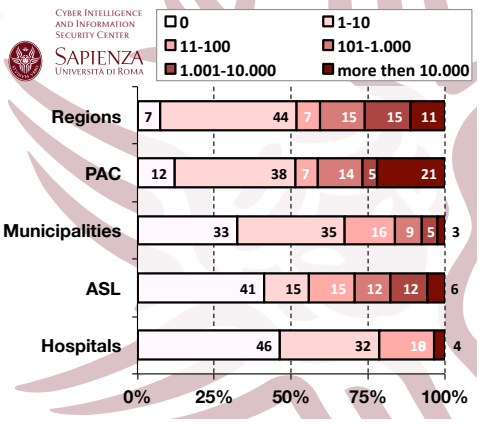


Figure 3.35: Number of attack attempts suffered in 2013 depending on administration category.

claiming to have suffered no attack attempts, are the ones which have obtained the worst results for all the KPIs. This is also shown in Figure 3.35, which shows that hospitals and ASLs have detected a small number of attacks: in fact, over 40% of them (41% of ASLs and 46% of hospitals) declare they have not experienced attack attempts.

Very few PACs, regions and municipalities claim to have not been subject to attack attempts, (12%, 7% and 33%, respectively). PACs detected the greatest number of attempts (21% declared more than 10,000 attempts per year).

3.8 Statistical analysis of survey data

By using algorithms belonging to disciplines like machine learning and information retrieval, it was possibile to study the characteristics common to those public organizations which obtained similar results over the three KPIs. This allowed us to identify the best practices aimed at raising IT security level as a whole, thus evidencing the important aspects that must be considered when there is the intention to significantly improve our own preparedness.

It is important to underline that of each of the 50 plus survey questions contribute to increasing/decreasing each single KPI in a very marginal manner, as such contributions have upper and lower limits independent from every single question. Such independence has allowed us to obtain results that are not influenced in any way by the assigned weights, rather only by the responses provided by the 200 plus organizations involved.

In particular, we studied those areas of the public sector that obtained a score higher than 50 on all KPIs, so to identify the common characteristics of those organizations which pay more attention to the proposed issues. By doing this, we obtained the following criteria:

1. If the organizaton is not doing any risk assessment and contemporarily does not define any response plan to a cyber attack, then it is highly likely that it is in a serious risky state;
2. If the organization is doing risk assessment but does not define any response plan to a cyber attack, it is not necessarily in a good state;
3. If the organization defines a response plan to a cyber attack but is not doing any risk assessment, it is not necessarily in a good state;
4. If the organization contemporarily holds an Information Security Management System (ISMS), a risk assessment activity and has defined a response plan to cyber attacks, then by all means it is very likely that it is in a good state.

Following the definition of such criteria, it has been possible to represent on scatter-graphs those public operators which satisfy this criteria, with their respective scores. In particular, in Figures 3.36, 3.37 and 3.38 we report the comparisons *Defense-Organization, Defense-Awareness* and *Organization-Awareness* respectively, for all operators, evidencing which criteria are satisfied.

In all of the three figures we can note that the areas of the public sector falling in the green zone have in common the following three requisites: (i) a regularly executed aisk assessment activity, (ii) a definition of a response plan to a cyber attack, (iii) the adoption of an ISMS. At the same time, we can note that those entities not doing any of the three aformentioned activities are thus very far from the green zone and even from the threshold (red dots) for qualifying as “safe”. The presence of a risk assessment activity and of a defined response plan to cyber attacks places the organization in the mid-upper part of the scatter graph (green dots), while those satisfying only one out of the three requisites are found in the intermediate zone (white dots).

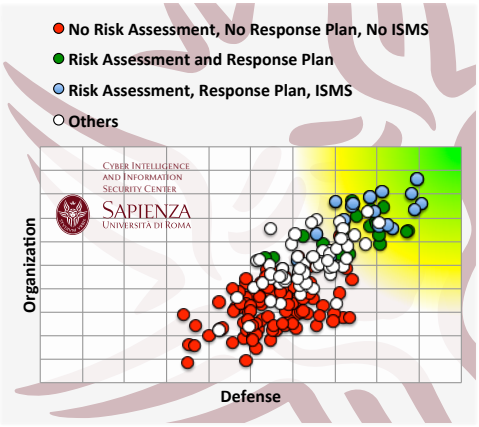


Figure 3.36: Comparison Defense-Organization.

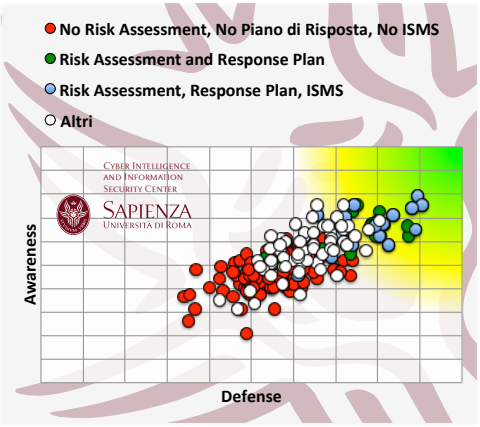


Figure 3.37: Comparison Defense-Awareness.

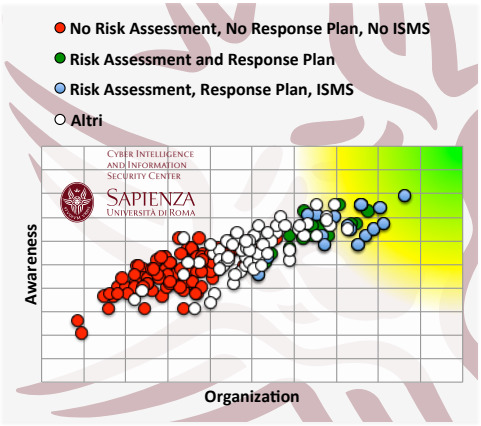


Figure 3.38: Comparison Organization-Awareness.

3.8.1 Three regions and regional organizations

In Section 3.4.2 we reported, as an example, the situation of all categories belonging to three regions (Figures 3.12, 3.13, 3.14). In particular, we noted how there is always a public organization whose general behaviour is always better than the others in the same region. The algorithms we used allowed us to establish what top-scoring public sector organizations have in common, as reported in Figures 3.39, 3.40, 3.41. With reference to Region 2 (Figure 3.39), we can in fact note that the top-scorer is the only organization in that region that puts into action a risk assessment plan, that has defined a cyberattack response plan and that currently has an operational ISMS. In the case of Region 3 (Figure 3.40), there are two entities with a higher score than the other regional public bodies: in this case, none of them have an ISMS but they are the only two who defined a cyber attack response plan and that regularly execute risk assessment activities. Region 1 displays a less clear situation: the two best organizations both operate risk assessment or have defined a response plan, but not contemporarily. Anther two operators, with worse scores, present a similar characteristic.

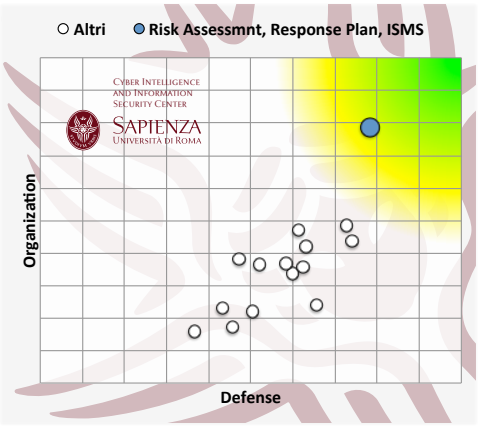


Figure 3.39: Situation of a single region (Region 2).

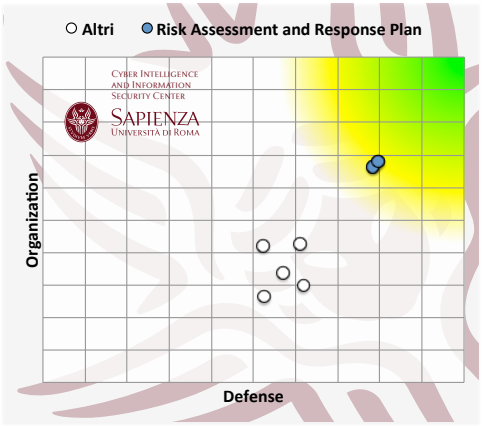


Figure 3.40: Situation of a single region (Region 3).

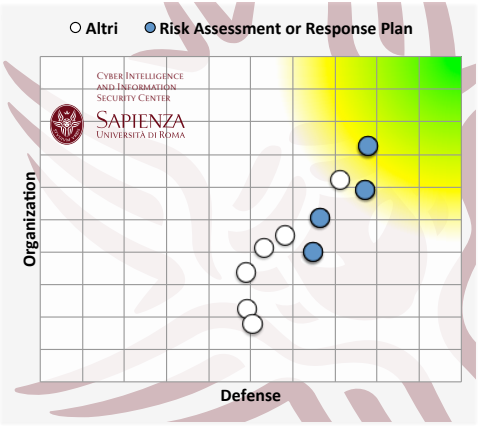


Figure 3.41: Situation of a single region (Region 1).

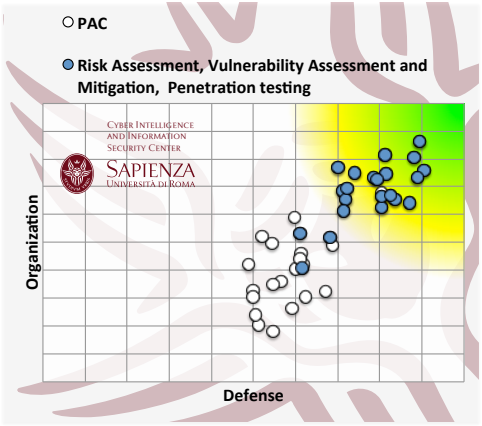


Figure 3.42: Comparison Defense-Organization for PACs with classification.

3.8.2 National authorities/PACSs

As shown in Figure 3.6, with reference to the *Defense-Organization* comparison related to PACs, we identified a well-defined group of public authorities with good scores as well as a well-defined group with worse ones. It seems useful to try understand what are the practices that define such groups and the reasons that lead to such different results. By isolating the scores of such PACs, it has been possible to classify them and it emerged that those PACs that regularly hold risk assessment activities, penetration testing and that follow "vulnerability assessment and mitigation" methodology represent the majority of those with top scores. On the contrary, those not following such practices are the ones showing worse results (such an analysis gave us an error of only 3 PACs out of 42). Figure 3.42 represents this situation, highlighting with different colors the two groups of PACs.

3.8.3 Considerations of the classification procedure

The rules and criteria described above were obtained by analyzing the set of retrieved data, and clearly identifying a small set of questions characterizing certain situations, but it must be interpreted correctly. Note in fact that:

- while responding to questionnaires, an affirmative response to the 3 identified questions impacts for no more than 20% on each KPI;
- the correct positioning of a public body is defined, with certainty, only by the responses to the whole questionnaire, and each question influences the calculation of KPIs in accordance with Table 2.1, according to the methodology already presented into Chapter 2;
- the three questions reported here (risk assessment, response plan and ISMS) are those which most influence the classification of organizations that obtained a score higher than 50 for all KPIs: this result is confirmed by Figures 3.36, 3.37 and 3.38. However, the obtained classification model is way more complex and the various intermediate situations are characterized by a wider subset of questions. A longer list of questions influence most the classification is reported in the next paragraph.

3.8.4 List of high impact questions

The following section reports a list of questions (with their related reference ID and a brief description) which have the most impact on the classification of those public entities that obtained for all KPIs a score higher than 50. Note that such a list represents around 18% of the whole set of questions and that they are not ordered by their impact factor.

- Q. 2: Region to which the organization belongs
- Q.6: Number of users that can avail themselves of the services offered
- Q. 10: Number of employees in the IT sector
- Q.14: Number of registered users for the offered services
- Q. 21: Physical security (access to premises)
- Q.38: Definition of a cyber attack response plan
- Q. 48: Regular risk assessment activities
- Q.49: Risk assessment certified by external organizations
- Q.52: Presence of an operational ISMS
- Q. 53: Presence of an incident response team/committee
- Q. 57: Periodical verification procedures of the correct organization and functioning of ICT security

The interpretation of such questions provides a series of best practices that the public sector should follow in order to bring its own level of preparedness against cyber threats to acceptable levels. In particular, questions 6, 10 and 14 suggest that a proper dimensioning of human resources, adequate to the needs of the sector, is very important. Questions 48, 49, 52, 53 and 57 testify how having a well-structured organization is fundamental in order to be well prepared. Risk assessment (better if certified) allows increasing risk awareness and undertaking of the correct countermeasures. The presence of an incident response team, apart from the undoubted usefulness in case of a crisis, testify a high awareness as well as attention to cyber security issues. Periodical verification procedures of the correct organization and functioning of ICT security allows for reacting in a timely manner to new threats and vulnerabilities. Additionally, the presence of a physical control when accessing the organization's premises is fundamental to prevent intrusions of unauthorized and malicious personnel to those spaces where IT activities are being carried out. Last but not least, we want to stress how in this list there is only one question (38) related to Defense, even if (as shown in Figures 3.36 e 3.37 on the x-axis) the obtained classification places the values of such a KPI in a correct way. This means that the *Defense* KPI is implied by the *Awareness* and *Organization* KPIs: the fact of answering in a certain way to the questions in the list implies that certain *Defense* practices may, or may not, be followed.

3.9 Most commonly ignored practices

It is now useful to identify which characteristics are common to public sector organizations scoring less than 50 for each KPI. This leads to an understanding of which practices are typically ignored by public entities less committed to cyber security issues.

As per what has been discussed and shown in reference to Figures 3.36, 3.37 and 3.38, it appears quite clear that all such public operators are commonly characterized by:

1. lack of risk assessment procedures or irregular risk assessment);
2. lack of cyber attack response plan;
3. lack of an ISMS.

However, the applied methodology allows for the identifcation of other common characteristics among the worst-scoring organizations, in particular:

5. lack of physical access to IT premises control systems;
6. lack of penetration testing or vulnerability assessment mitigation activities;
7. lack of an incident response team;
8. lack of periodical verification procedures of the correct organization and functioning of ICT security;
9. lack of, or non approved, ICT security plan;
10. lack of request to AgID for opinion on the technical feasibility study for disaster recovery and business continuity plans.

CHAPTER

4 Conclusion and Recommendations

Google is a perfect example of the value that citizens' information may have in the world of Internet. Even though in 2013 it spent 7.3 billion dollars to modernize its data centers, both in terms of hardware and network, and considering that most of the applications provided are free, Google was one of the companies with the highest profits in the world. Google's power is all in the information that users grant it, which can then be used to profile users and improve Google's best applications with the final outcome of making a profit from ad-hoc advertisements. Meanwhile users are happy as they perceive the continuous improvements of applications. In essence, this is the magic of Google.

The Italian public sector must be aware that data they possess at local, regional and national level, is of great value. The value of such data may be of a economic type, or of a strategic and national security type, or both. In any case, such value should be exploited whenever possible and protected above all from attacks. Such attacks may, in fact, damage citizens' privacy, make data unavailable, decrease their value due to their diffusion or to their disclosure to third parties.

If such a concept is not acquired by the public sector, it will be difficult to improve the security level. The report has unfortunately highlighted that most of the Italian public sector has very limited defensive capabilities. An improvement of such capabilities needs to progress hand in hand with the possibility of being able to in find security experts who, in turn, have the possibility of working in an organization, and in a coordinated national context, where responsibilities of who is doing what are clearly stated. Thus, the implementation of the national strategic plan plays an important strategic role.

Following is a set of recommendations which starts at the national cyber security strategy level before turning to technical and organizational ones at the individual level:

4.1 Rationalization of public sector information assets and security

You cannot think about securing IT assets of the Italian public sector without reducing its global attack surface. As this report shows, in fact, the huge number of micro- and mini-data centers (or simple server rooms) does not allow for the adequate number of technicians skilled in computer security necessary to guarantee adequate defenses. We are talking about a small number of computer security experts in Italy having to face tens of thousands of potential attack targets. Hence, there is the need for the process of rationalization of the information assets of the public sector and the raising of security levels to to be undertaken together, as described in the following recommendations.

Aggregation of individual public sector operators on a geographic or business basis to raise cybernetic defenses

As the figures related to region performance clearly show, the rationalization of public sector infrastructure goes hand in hand with increased security. The latter can be achieved, in fact, through an aggregation process that will push towards the hosting of local information systems in qualified structures (data centers), probably already present in the same regions. The IT organizations of some regions, often run by in-house companies, can immediately offer answers to different needs, including the presence of physical access control systems (question 21); the presence of an ISMS (reference 52); the presence of a group/committee for incident management (question 53). In addition, this aggregation would increase the number of IT resources with appropriate profiles, typically expert in security. This would require, for example in municipalities, the migration of their level of internal security organization, thus laying the foundations of a virtuous circle that would lead in little time to municipalities having the same levels of security as regions, so making the whole country immediately more resistant to cyber threats.

What we highlighted on a geographical basis for regions and municipalities could also be done for national and local organizations that share the same "business" as well. For example, hospitals, local health boards and the Ministry of Health could be hosted by some nationwide interconnected data centers sharing applications, data and infrastructure. What CINECA[1] did with universities can be an example of this embedding process and, on a smaller scale, what the Court of Auditors did with the advocacy of the state can be one more example.

Consider the IT infrastructure as a strategic national asset

It is important to stress that proper management of an infrastructure based on regional clouds, would not pose obstacles to the property, confidentiality or operational activity of municipalities. However, it would significantly reduce their operating costs through the sharing of applications and infrastructure. Therefore, the rationalization of the public sector technological infrastructure, from the current tens of thousands of centers, to a number closer to fifty, would have the triple benefit of (i) savings in the order of hundreds of millions of Euros, (ii) significantly increasing levels of security and availability of public sector services and (iii) achieving a real infrastructural asset that is strategic for the development of the country. Clearly this cannot be achieved at zero cost, but only through adequate investment from the government, which would make this transition advantageous. Note that such a well structured organization would have the advantage of making employees mobility easier, for example between public entities in the same region as they would find the same IT tools.

Consider public sector data centers as critical infrastructures

Just as already happens in the information systems of companies that manage critical infrastructures (electricity, gas, water, transport, etc.), data maintained by the the public sector may be particularly important, both for security reasons and for the stability of a country. An example is represented by the impact that a malfunction or an attackcould have on applications that manage the public debt of the country, the Inland Revenue, the Land Registry, the National Health Service etc. In a vision close to the one proposed in the previous recommendation, the data centers of the public sector should be considered as critical infrastructures, thus imposing appropriate levels of security and reliability on the structures. The severity level of the infrastructure should be defined according to the criticality of the information it stores. All of this should be specifically regulated at the national level.

A "made in Italy" cloud as an economic driver for small and medium-size businesses

This network of qualified data centers could also be used to host the information systems of small and medium-size businesses. This would lay the foundations for the creation of a "made in Italy" cloud, based on the German model, which allows the development of these businesses, while ensuring the confidentiality of the information processed in accordance with current regulations in Italy. When using foreign cloud service providers, like Amazon, to host

[1] Consortium of Italian Universities `http://www.cineca.it/en`.

data and applications, it must not be forgotten that these suppliers are subject to the Patriot Act. This means that the US government could possibly be granted access to all the data they host.

4.2 Implementation of the national strategic plan for cyber security

This section discusses some recommendations based on the strategic plan for cyber security signed by the President of the Council of Ministers Enrico Letta in December 2013 and published in the Gazzetta Ufficiale in February, 2014.

Centralization of powers and responsibilities in the strategic framework for cyber security

The picture drawn in the national strategic plan for cyber security is distributed and uneven in terms of expertise and responsibility in the prevention, management and response to cyber attacks. Furthermore, in Italy we have a lack of security experts and this means that no further dispersion of these skills among the many actors participating in the national strategic framework should be allowed. Finally, the speed with which attacks unfold requires great coordination between threat detection and response and this goes against a distribution of responsibilities. Therefore, a revision of the strategic plan with the aim of centralizing, whenever possible, competencies and responsibilities would be desirable, if not mandatory. Many countries, such as France, Germany, Israel and the Netherlands, have already concentrated these activities in specific agencies or entities.

CERT operational status and information sharing

Compared to other countries, Italy has expereienced a significant delay in the activation of a national CERT. The operationalization of the system of national CERTs, as defined by the Decree of January 24, 2013, remains a top priority. As for the government, the priority is the organization of a network of regional CERTs headed by a CERT PA and the creation of an appropriate system of information sharing in order to improve prevention and response to cyber threats. In addition, the CERT should establish clear guidelines for the classification of threats, their levels of criticality and their sensitivity.

Promote a security culture: technology vs. the human factor

Figures from this report show that, for all the categories considered, the values obtained in the KPI *Defense* (which is associated to the possession and use of technologies for protection and defense) are bigger, on average, than those for KPIs *Awareness* and *Organization*: this means that more money is spent, on average, in technology, even when it does not necessarily represent the result of joint projects and of strategic visions, while aspects related to the human factor (awareness) and to the organization are not adequately considered. These aspects are the basis for the correct use of these technologies and the basis of their potential yield in terms of effectiveness. This is a well known issue, the result of the distance between the average user's and the "expert's" lexicon and techniques, but it is also the result of a pathological laziness and drag typical of the public sector. It is more and more commonly thought that surplus technological artifacts may compensate for ineffective working practices. All of this falls within the infamous "human factor", which in the field of safety is as important as the ownership and operation of advanced technology. The human factor is further exacerbated by the issue that security and its " policy " are perceived as requirements put in place to delay and monitor the public sector employee. In a nutshell, they are perceived as turnstiles for checking up on employee presence. Furthermore, managers have no instruments (or motivation) to change this perception. It is necessary to improve awareness in the public sector about the importance of information assets that it manages and awareness of how the single employee may be the target of an attack and facilitate, against their will, access to the institutional systems without technologies being able to detect the attacks. Working on this awareness means improving the human factor.

Preparing public sector employees through training and practice exercises is as important as acquiring new technology. Along the same lines, organizational assessment becomes as important as, for example, penetration testing and other technological practices.

Research, development and investment in technology

Since the safety of the national cyber space is a strategic objective that impacts the growth and prosperity of the nation, and this is constantly moving due to the nature of the opponent, we can not outsource these skills to other nations, but we must find within our borders methodological, policy, organizational, and technological solutions to the problem and then make them consistent with respect to a framework of international alliances. It is necessary to improve domestic skills and consolidate the existing role of Italy as a key player in this area at the international level as well as stopping the brain drain of those with great security skills who are abandoning Italy.

To make all of this happen we need a plan for a large-scale technological improvement of Italian infrastructure with a clear and direct vision about the development of the country defined in the first recommendations. Rationalization and restructuring of the technological Italian infrastructure would represent a huge economic stimulus for the country. To make this happen we need nationwide actors. On the research side we are trying to do our best to present an organized and compact Italian scientific community. The creation of the National Laboratory of Cyber Security [2] goes in this direction. Financing research and industry in this area through a strategic project is therefore a priority. Everything must be done to achieve, as a country, the maximum possible degree of independence in the prevention and management of risks related to our information assets.

4.3 Recommendations for improving the security levels of the public sector

In this section we list some recommendations, based on the questionnaires results, targeted at public organizations and authorities that want to improve their security levels. The cost-benefit ratio receives particular attention, thus this section mainly targets those which aim at improving their security levels, in a fast and economical fashion.

The importance of a risk assessment process

Cyber security requires investments and these investments may not necessarily lead to a tangible benefit. It is natural that, when security issues arise, operators do not know exactly which activities to devote their efforts to. We believe that the crucial point, concerning cost-benefit ratio, is risk assessment.

The statistical analysis performed in this study highlighted how entities performing risk assessment, especially if certified by external organizations, received a better overall assessment. Performing risk assessment means investigating security problems and unearthing critical issues, in order to understand which are the most promising action points; therefore showing, in a timely and economical fashion, the right direction to follow.

Physical access to IT premises and logical access to all workstations

Cyber security starts with physical access control to IT premises. It makes no sense to implement any security solution if unauthorized people can physically enter the premises hosting the data. Unfortunately, this survey showed up a widespread failure in restricting access to physical premises. This is one starting point for improving security levels. The implementation of restriction systems, to both premises hosting servers and computers accessing relevant data, is mandatory. The ideal solution would be the use of certificates for both logical and physical access to all machines hosting relevant data.

Penetration testing

The main vehicle of cyber attacks is the web. All branches of the public sector provide services through the web. It is obvious that the most exposed and vulnerable access points for the entire public sector information system are its websites. Penetration testing consists in simulating actions of potential attackers, in order to flush out any security flaws of the information system access points. It is a relatively economic activity, compared to an

[2] Cyber Security National Laboratory: `http://www.consorzio-cini.it/lab-cyber-security`.

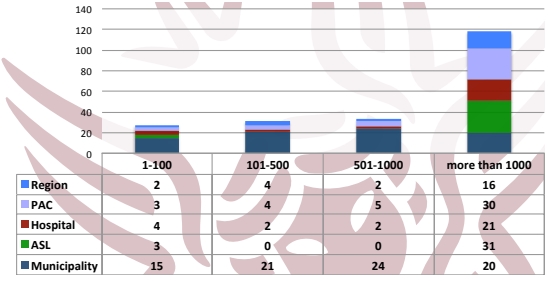
extensive risk assessment. Whoever offers web services must consider periodically running penetration tests, as new vulnerabilities are discovered on a daily basis.

Outsource critical services if it is impossible to protect them

Outsourcing critical services, when it is not possible to properly protect them, may be the most economic solution for significantly improving security. The budget may be the main factor leading to IT system protection practices being put aside. The reason is that the benefit is potential rather than tangible. A good security culture may help in identifying, after a careful risk assessment phase, the main problems and consider the opportunity to rely on security providers to improve services and data security. Moreover, relying on third-party companies can be cheaper than developing in-house solutions. In this investigation we observed that regions and nationwide organizations with a dedicated in-house IT company performed significantly better.

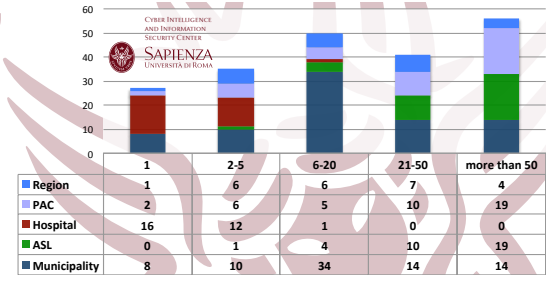
Appendix: Survey and Collected Answers

This appendix provides the survey questions submitted to the public sector organizations and the collected answers aggregated by category. The results are not given in percentages. The survey is implemented with a skip logic: some questions have not been asked since they where excluded by answers to previous questions.



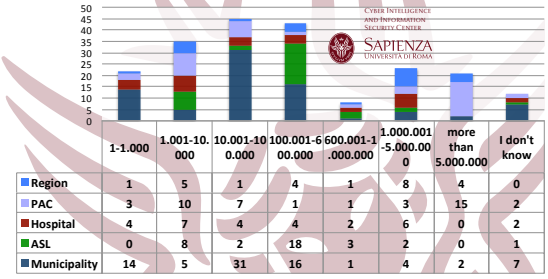
	1-100	101-500	501-1000	more than 1000
Region	2	4	2	16
PAC	3	4	5	30
Hospital	4	2	2	21
ASL	3	0	0	31
Municipality	15	21	24	20

Question n.4: Choose the number of employees.



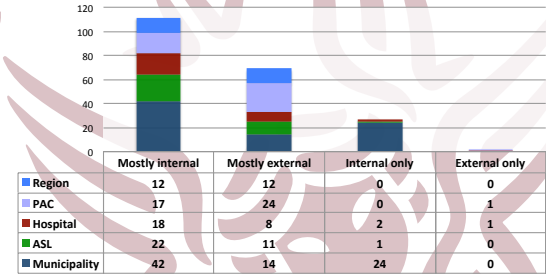
	1	2-5	6-20	21-50	more than 50
Region	1	6	6	7	4
PAC	2	6	5	10	19
Hospital	16	12	1	0	0
ASL	0	1	4	10	19
Municipality	8	10	34	14	14

Question n.5: Choose the number of branches.



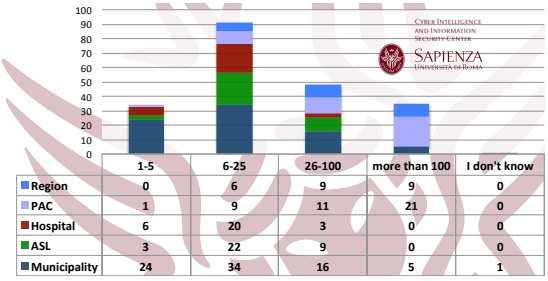
	1-1.000	1.001-10.000	10.001-100.000	100.001-600.000	600.001-1.000.000	1.000.001-5.000.000	more than 5.000.000	I don't know
Region	1	5	1	4	1	8	4	0
PAC	3	10	7	1	1	3	15	2
Hospital	4	7	4	4	2	6	0	2
ASL	0	8	2	18	3	2	0	1
Municipality	14	5	31	16	1	4	2	7

Question n.6: Give the number of users (both internal and external) that can use the services provided.



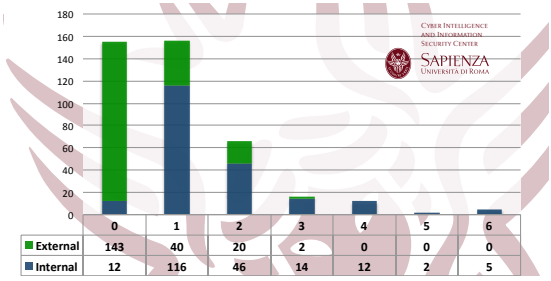
	Mostly internal	Mostly external	Internal only	External only
Region	12	12	0	0
PAC	17	24	0	1
Hospital	18	8	2	1
ASL	22	11	1	0
Municipality	42	14	24	0

Question n.9: Are the IT personnel internal or external employees?



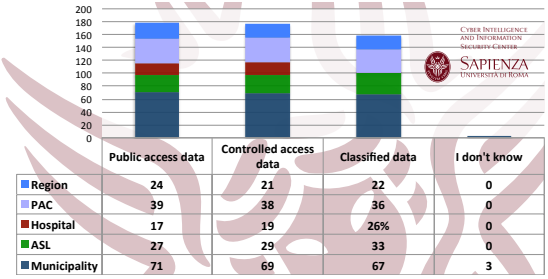
	1-5	6-25	26-100	more than 100	I don't know
Region	0	6	9	9	0
PAC	1	9	11	21	0
Hospital	6	20	3	0	0
ASL	3	22	9	0	0
Municipality	24	34	16	5	1

Question n.10: Choose the number of IT employees.



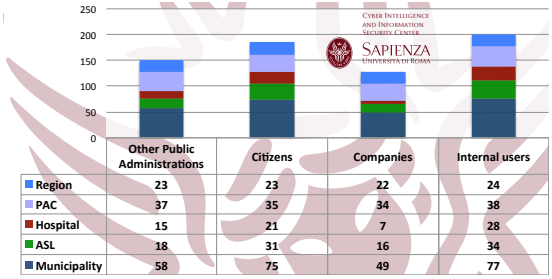
	0	1	2	3	4	5	6
External	143	40	20	2	0	0	0
Internal	12	116	46	14	12	2	5

Question n.11: Choose the number of data centers belonging to the organization/authority.



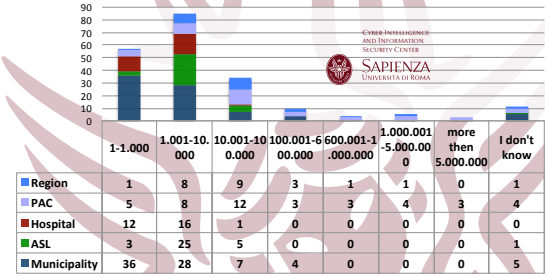
	Public access data	Controlled access data	Classified data	I don't know
Region	24	21	22	0
PAC	39	38	36	0
Hospital	17	19	26%	0
ASL	27	29	33	0
Municipality	71	69	67	3

Question n.12: Choose the type of data handled.



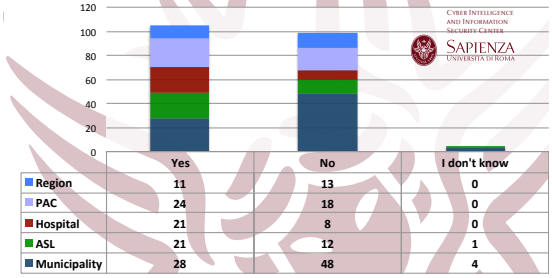
	Other Public Administrations	Citizens	Companies	Internal users
Region	23	23	22	24
PAC	37	35	34	38
Hospital	15	21	7	28
ASL	18	31	16	34
Municipality	58	75	49	77

Question n.13: Choose the IT services user type.



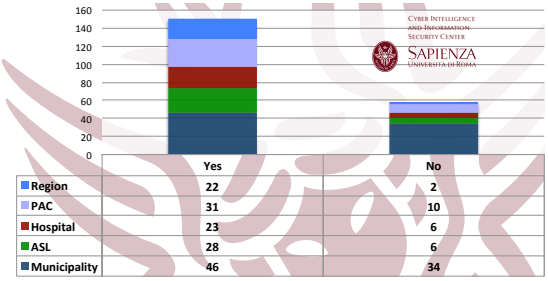
	1-1.000	1.001-10.000	10.001-100.000	100.001-600.000	600.001-1.000.000	1.000.001-5.000.000	more then 5.000.000	I don't know
Region	1	8	9	3	1	1	0	1
PAC	5	8	12	3	3	4	3	4
Hospital	12	16	1	0	0	0	0	0
ASL	3	25	5	0	0	0	0	1
Municipality	36	28	7	4	0	0	0	5

Question n.14: Select the number of registered users using the IT services.



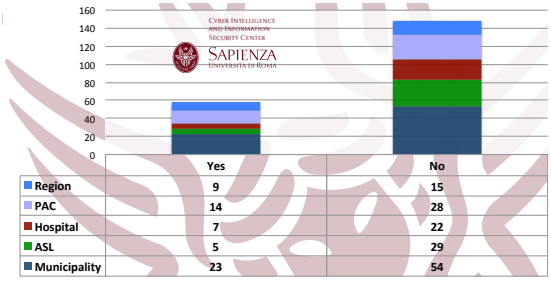
	Yes	No	I don't know
Region	11	13	0
PAC	24	18	0
Hospital	21	8	0
ASL	21	12	1
Municipality	28	48	4

Question n.15: Are critical IT services provided which do not tolerate brief unavailability (up to one hour)?



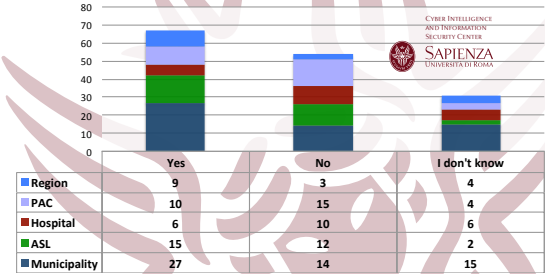
	Yes	No
Region	22	2
PAC	31	10
Hospital	23	6
ASL	28	6
Municipality	46	34

Question n.16: Can employees access the systems or sensitive data from outside the public sector network through a remote login (i.e., ssh, vpn, etc.)?



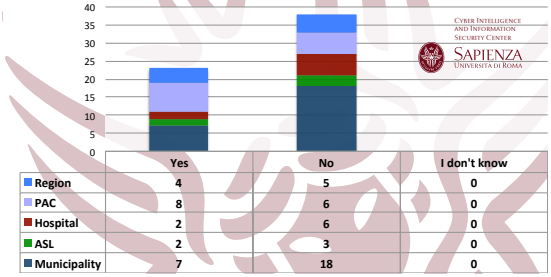
	Yes	No
Region	9	15
PAC	14	28
Hospital	7	22
ASL	5	29
Municipality	23	54

Question n.17: Is cloud computing used?



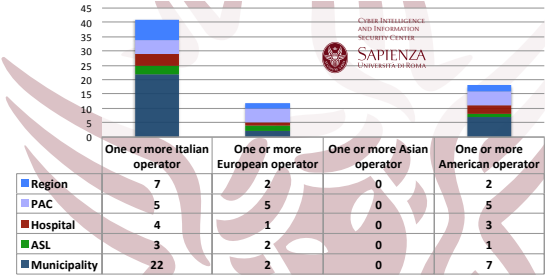
	Yes	No	I don't know
Region	9	3	4
PAC	10	15	4
Hospital	6	10	6
ASL	15	12	2
Municipality	27	14	15

Question n.18: Is there the intention to introduce cloud computing?



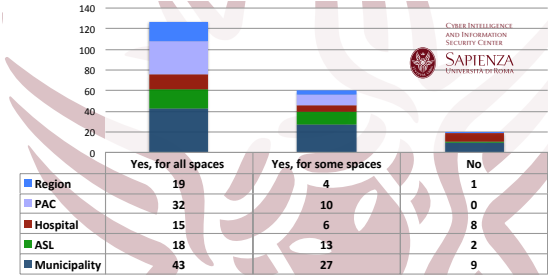
	Yes	No	I don't know
Region	4	5	0
PAC	8	6	0
Hospital	2	6	0
ASL	2	3	0
Municipality	7	18	0

Question n.19: Are any critical IT services provided based on cloud computing?



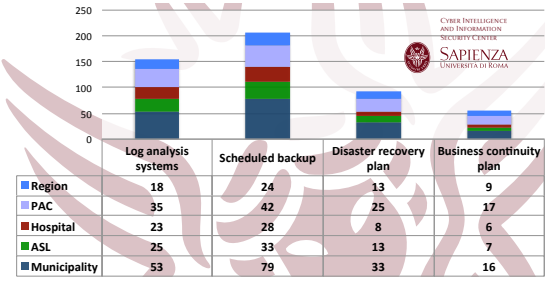
	One or more Italian operator	One or more European operator	One or more Asian operator	One or more American operator
Region	7	2	0	2
PAC	5	5	0	5
Hospital	4	1	0	3
ASL	3	2	0	1
Municipality	22	2	0	7

Question n.20: What operator is used for cloud computing?



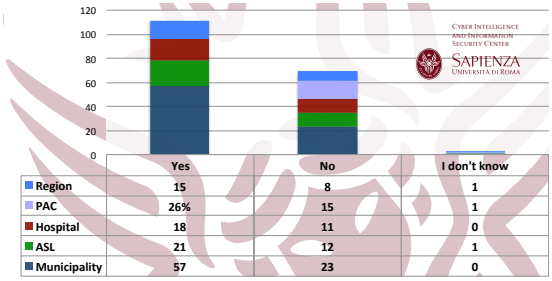
	Yes, for all spaces	Yes, for some spaces	No
Region	19	4	1
PAC	32	10	0
Hospital	15	6	8
ASL	18	13	2
Municipality	43	27	9

Question n.21: Are there any physical access control systems protecting the rooms hosting computational, storage or network resources (excluding personal workstations)?



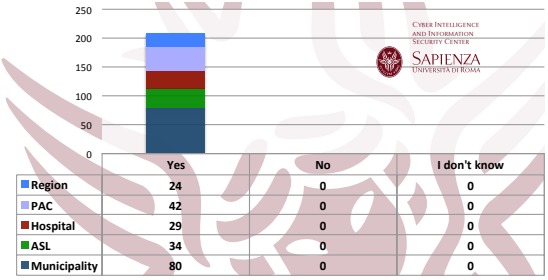
	Log analysis systems	Scheduled backup	Disaster recovery plan	Business continuity plan
Region	18	24	13	9
PAC	35	42	25	17
Hospital	23	28	8	6
ASL	25	33	13	7
Municipality	53	79	33	16

Question n.22: How are data and digital documents controlled and protected?



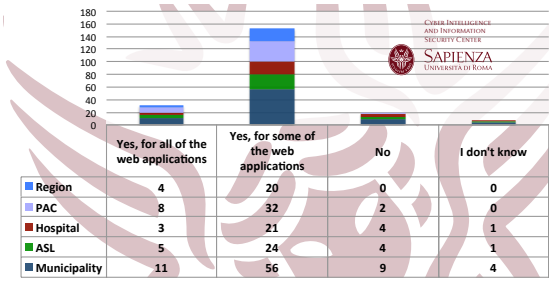
	Yes	No	I don't know
Region	15	8	1
PAC	26%	15	1
Hospital	18	11	0
ASL	21	12	1
Municipality	57	23	0

Question n.23: Are the backup data storage support devices located in a different physical site?



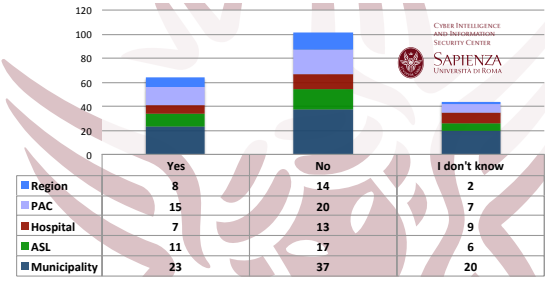
	Yes	No	I don't know
Region	24	0	0
PAC	42	0	0
Hospital	29	0	0
ASL	34	0	0
Municipality	80	0	0

Question n.24: Does the organiziation/authority use and/or provides services based on web technologies?



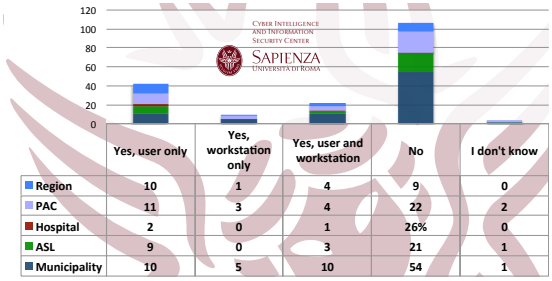
	Yes, for all of the web applications	Yes, for some of the web applications	No	I don't know
Region	4	20	0	0
PAC	8	32	2	0
Hospital	3	21	4	1
ASL	5	24	4	1
Municipality	11	56	9	4

Question n.25: Do the web applications provided and/or used by the organization/authority use the SSL/TLS protocol?



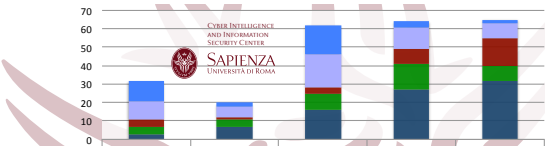
	Yes	No	I don't know
Region	8	14	2
PAC	15	20	7
Hospital	7	13	9
ASL	11	17	6
Municipality	23	37	20

Question n.26: Regarding the web applications provided and/or used which employ the https protocol, are the corresponding digital certificates issued according to the Extended Validation (EV) criteria?



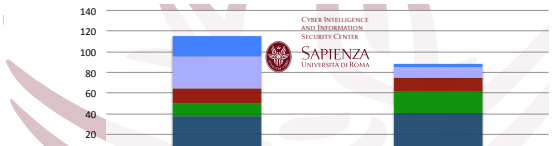
	Yes, user only	Yes, workstation only	Yes, user and workstation	No	I don't know
Region	10	1	4	9	0
PAC	11	3	4	22	2
Hospital	2	0	1	26%	0
ASL	9	0	3	21	1
Municipality	10	5	10	54	1

Question n.27: Is there any digitally certified authentication procedure for users and workstations?



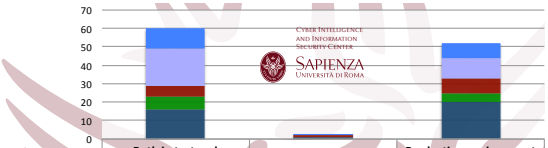
	Prior to 1.0.1	1.0.1 to 1.0.1f	1.0.1g or later	I don't know	OpenSSL not used
Region	11	2	16	3	2
PAC	10	6	18	12	8
Hospital	4	1	3	8	15
ASL	4	4	9	14	8
Municipality	3	7	16	27	32

Question n.28: If a service is provided which is based on the open SSL library, which version is used?



	Yes	No
Region	20	3
PAC	31	10
Hospital	14	14
ASL	13	20
Municipality	37	41

Question n.29: Have you ever performed vulnerability assessment and mitigation, or penetration testing activities?



	Both in test and production environments	Test environment only	Production environment only
Region	11	1	8
PAC	20	0	11
Hospital	6	1	8
ASL	7	0	5
Municipality	16	1	20

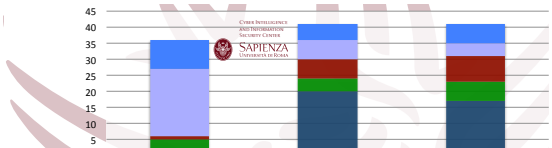
Question n.30: Ref. Question 29, in which environment are these tests performed?

	Each six months at least	At least annually	At least each two years	Not regularly	After being attacked	After that new vulnerabilities are discovered
Region	6	6	2	6	6	6
PAC	11	6	0	14	4	10
Hospital	1	1	2	11	0	0
ASL	3	3	2	4	1	2
Municipality	2	8	3	23	4	5

Question n.31: Ref. Question 29, how often are they performed?

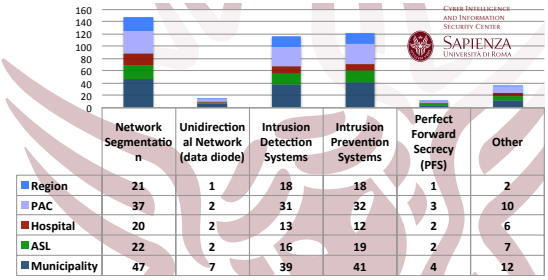
	Yes	No	Sometimes	I don't know
Region	15	2	2	1
PAC	17	2	12	0
Hospital	13	1	1	0
ASL	10	0	2	1
Municipality	21	10	8	0

Question n.32: Ref. Question 29, are the tests outsourced?



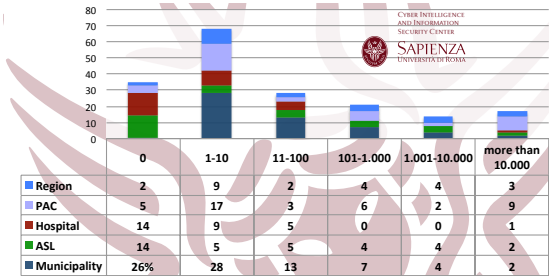
	Yes	No	I don't know
Region	9	5	6
PAC	21	6	4
Hospital	1	6	8
ASL	3	4	6
Municipality	2	20	17

Question n.33: Ref. Question 29, are the web applications tested with the OWASP methodology?



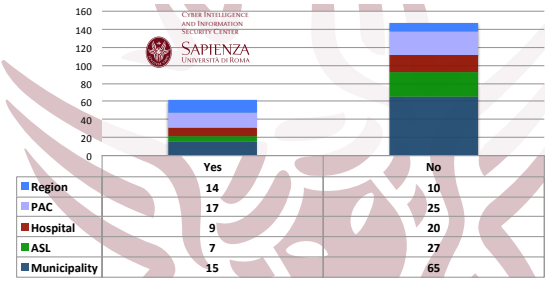
	Network Segmentation	Unidirectional Network (data diode)	Intrusion Detection Systems	Intrusion Prevention Systems	Perfect Forward Secrecy (PFS)	Other
Region	21	1	18	18	1	2
PAC	37	2	31	32	3	10
Hospital	20	2	13	12	2	6
ASL	22	2	16	19	2	7
Municipality	47	7	39	41	4	12

Question n.34: Which of the following measures are taken to prevent the spread of a possible cyber attack?



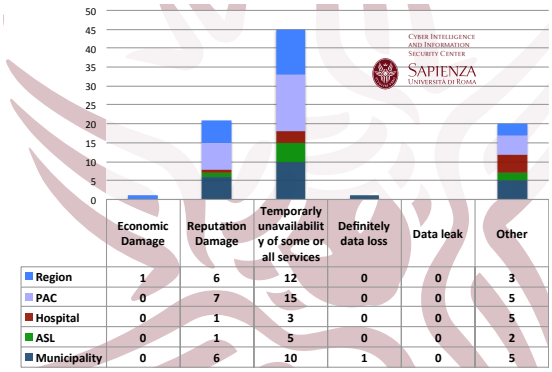
	0	1-10	11-100	101-1.000	1.001-10.000	more than 10.000
Region	2	9	2	4	4	3
PAC	5	17	3	6	2	9
Hospital	14	9	5	0	0	1
ASL	14	5	5	4	4	2
Municipality	26%	28	13	7	4	2

Question n.35: How many attack attempts were recorded during 2013?



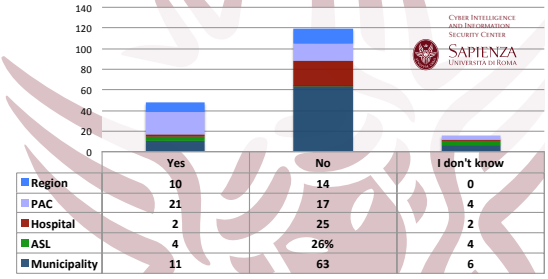
	Yes	No
Region	14	10
PAC	17	25
Hospital	9	20
ASL	7	27
Municipality	15	65

Question n.36: Were there any known successful cyber attacks targeting the organization/authority?



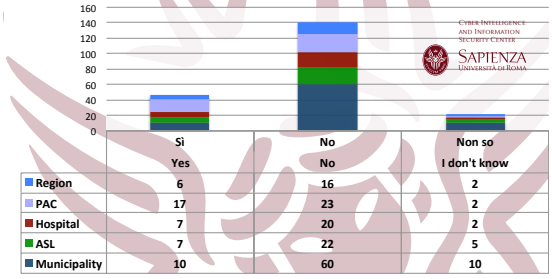
	Economic Damage	Reputation Damage	Temporarily unavailability of some or all services	Definitely data loss	Data leak	Other
Region	1	6	12	0	0	3
PAC	0	7	15	0	0	5
Hospital	0	1	3	0	0	5
ASL	0	1	5	0	0	2
Municipality	0	6	10	1	0	5

Question n.37: Which type of loss/damage caused by successful attacks has been recorded?



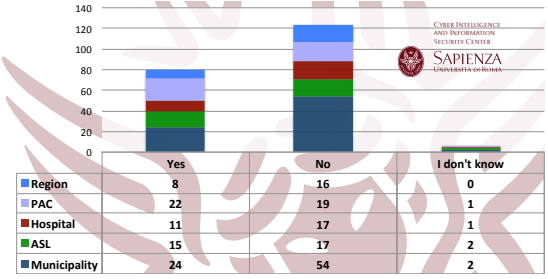
	Yes	No	I don't know
Region	10	14	0
PAC	21	17	4
Hospital	2	25	2
ASL	4	26%	4
Municipality	11	63	6

Question n.38: Does the organization/authority have a response plan or procedure to be followed when a cyber attack is detected?



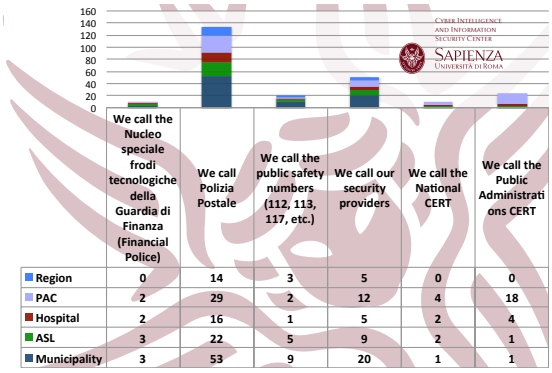
	Si	No	Non so
	Yes	No	I don't know
Region	6	16	2
PAC	17	23	2
Hospital	7	20	2
ASL	7	22	5
Municipality	10	60	10

Question n.39: For the daily management of IT security events is a Security Information and Event Management (SIEM) system used?



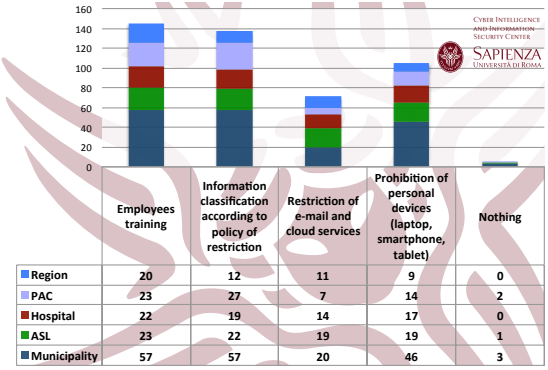
	Yes	No	I don't know
Region	8	16	0
PAC	22	19	1
Hospital	11	17	1
ASL	15	17	2
Municipality	24	54	2

Question n.40: Does the organization/authority have an agreement with some IT security service provider?



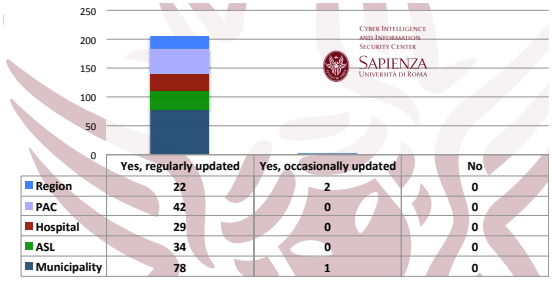
	We call the Nucleo speciale frodi tecnologiche della Guardia di Finanza (Financial Police)	We call Polizia Postale	We call the public safety numbers (112, 113, 117, etc.)	We call our security providers	We call the National CERT	We call the Public Administrations CERT
Region	0	14	3	5	0	0
PAC	2	29	2	12	4	18
Hospital	2	16	1	5	2	4
ASL	3	22	5	9	2	1
Municipality	3	53	9	20	1	1

Question n.41: If a cyber attack is detected, which external bodies/authorities are informed?



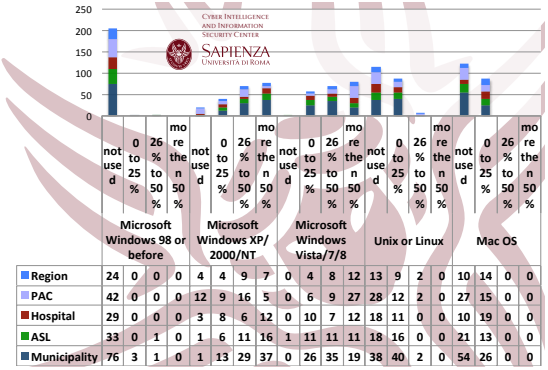
	Employees training	Information classification according to policy of restriction	Restriction of e-mail and cloud services	Prohibition of personal devices (laptop, smartphone, tablet)	Nothing
Region	20	12	11	9	0
PAC	23	27	7	14	2
Hospital	22	19	14	17	0
ASL	23	22	19	19	1
Municipality	57	57	20	46	3

Question n.42: Which of the following security measures are implemented to protect data and systems against misuse by employees?



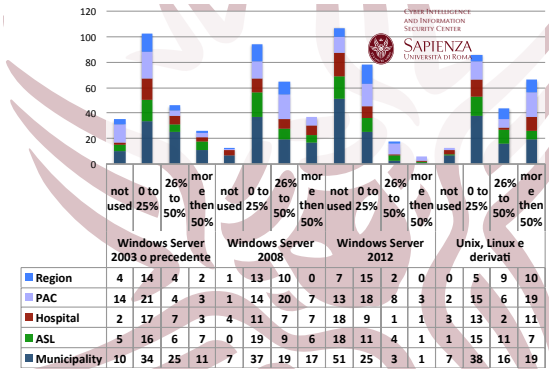
	Yes, regularly updated	Yes, occasionally updated	No
Region	22	2	0
PAC	42	0	0
Hospital	29	0	0
ASL	34	0	0
Municipality	78	1	0

Question n.43: Has an antivirus deployment been planned within the organization/authority?



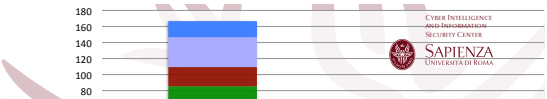
	Microsoft Windows 98 or before				Microsoft Windows XP/ 2000/NT				Microsoft Windows Vista/7/8				Unix or Linux				Mac OS			
	not used	0 to 25%	26% to 50%	more then 50%	not used	0 to 25%	26% to 50%	more then 50%	not used	0 to 25%	26% to 50%	more then 50%	not used	0 to 25%	26% to 50%	more then 50%	not used	0 to 25%	26% to 50%	more then 50%
Region	24	0	0	0	4	4	9	7	0	4	8	12	13	9	2	0	10	14	0	0
PAC	42	0	0	0	12	9	16	5	0	6	9	27	28	12	2	0	27	15	0	0
Hospital	29	0	0	0	3	8	6	12	0	10	7	12	18	11	0	0	10	19	0	0
ASL	33	0	1	0	1	6	11	16	1	11	11	11	18	16	0	0	21	13	0	0
Municipality	76	3	1	0	1	13	29	37	0	26	35	19	38	40	2	0	54	26	0	0

Question n.44: Choose the percentage of deployed operating systems on the CLIENT systems operating within the organizaton/authority network.



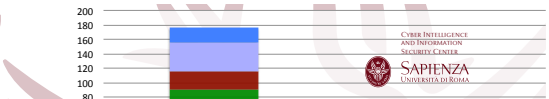
	Windows Server 2003 o precedente				Windows Server 2008				Windows Server 2012				Unix, Linux e derivati			
	not used	0 to 25%	26% to 50%	more then 50%	not used	0 to 25%	26% to 50%	more then 50%	not used	0 to 25%	26% to 50%	more then 50%	not used	0 to 25%	26% to 50%	more then 50%
Region	4	14	4	2	1	13	10	0	7	15	2	0	0	5	9	10
PAC	14	21	4	3	1	14	20	7	13	18	8	3	2	15	6	19
Hospital	2	17	7	3	4	11	7	7	18	9	1	1	3	13	2	11
ASL	5	16	6	7	0	19	9	6	18	11	4	1	1	15	11	7
Municipality	10	34	25	11	7	37	19	17	51	25	3	1	7	38	16	19

Question n.45: Choose the percentage of deployed operating systems on the SERVER systems operating within the organization/authority network.



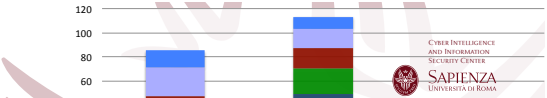
	Yes	No
Region	20	4
PAC	38	4
Hospital	23	5
ASL	28	6
Municipality	58	19

Question n.46: Is there a update policy for the CLIENT systems OS?



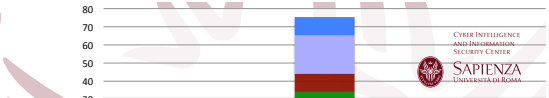
	Yes	No
Region	21	3
PAC	40	1
Hospital	24	5
ASL	27	7
Municipality	64	15

Question n.47: Is there a update policy for the SERVER systems OS?



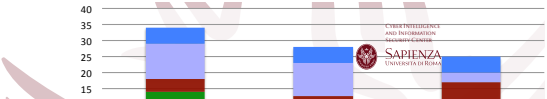
	Yes	No	I don't know
Region	14	10	0
PAC	24	16	2
Hospital	10	17	2
ASL	10	21	3
Municipality	27	49	4

Question n.48: Does the organizaiton/authority perform risk assessment of the IT systems?



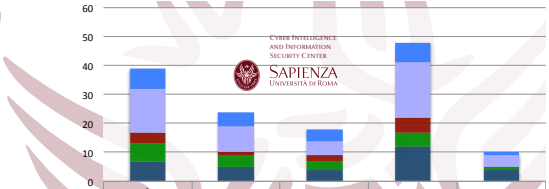
	Yes	No	I don't know
Region	5	10	0
PAC	2	21	1
Hospital	1	10	0
ASL	1	9	0
Municipality	3	25	0

Question n.49: Is the risk assessment evaluation certified by an external organization?



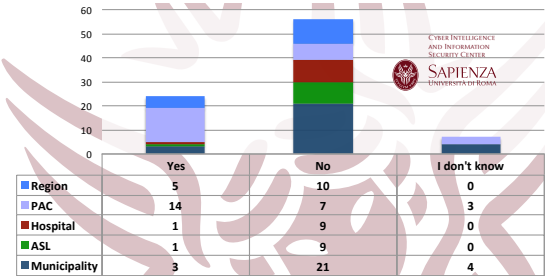
	Yes, defined and approved	Defined but not approved	No
Region	5	5	5
PAC	11	10	3
Hospital	4	1	5
ASL	4	3	3
Municipality	10	9	9

Question n.50: Has an ICT security plan, describing the security organizational chart, the roles and the responsibilities, been defined?



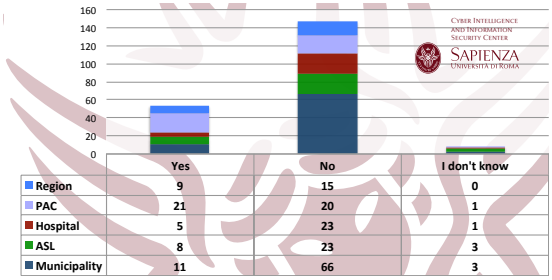
	Produce, disseminate and manage security documentation	Stock up services and products	Alienate products or to provision services	Report anomalies	Other
Region	7	5	4	7	1
PAC	15	9	5	19	4
Hospital	4	1	2	5	0
ASL	6	4	3	5	1
Municipality	7	5	4	12	4

Question n.51: Does the ICT security plan define the procedures to follow in order to undertake the following actions?



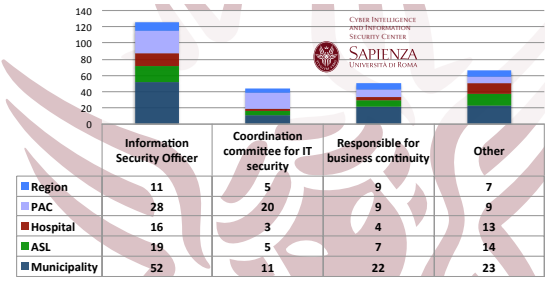
	Yes	No	I don't know
Region	5	10	0
PAC	14	7	3
Hospital	1	9	0
ASL	1	9	0
Municipality	3	21	4

Question n.52:Is an Information Security Management System (ISMS) used?



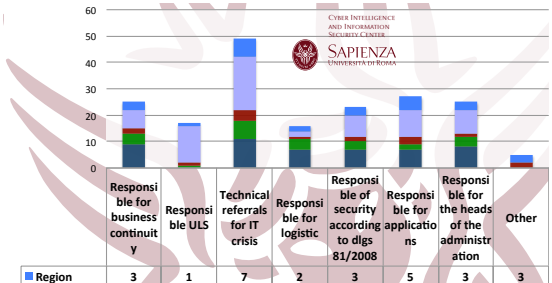
	Yes	No	I don't know
Region	9	15	0
PAC	21	20	1
Hospital	5	23	1
ASL	8	23	3
Municipality	11	66	3

Question n.53: Has a group/committee been created to manage security incidents?



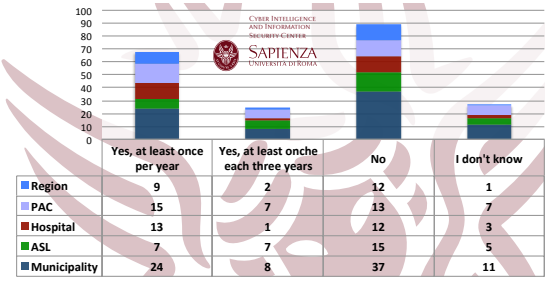
	Information Security Officer	Coordination committee for IT security	Responsible for business continuity	Other
Region	11	5	9	7
PAC	28	20	9	9
Hospital	16	3	4	13
ASL	19	5	7	14
Municipality	52	11	22	23

Question n.54: Which of the following roles have been identified (and assigned to employees) within your organization/authority?



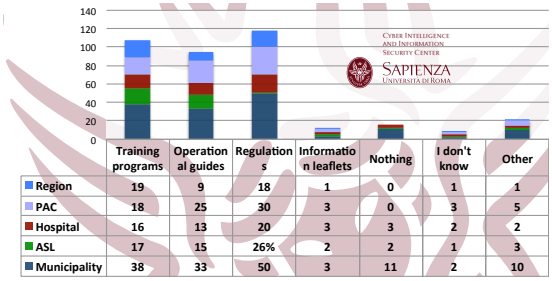
	Responsible for business continuity	Responsible ULS	Technical referrals for IT crisis	Responsible for logistic	Responsible of security according to dlgs 81/2008	Responsible for applications	Responsible for the heads of the administration	Other
Region	3	1	7	2	3	5	3	3
PAC	7	14	20	2	8	10	9	0
Hospital	2	1	4	1	2	3	1	2
ASL	4	1	7	4	3	2	4	0
Municipality	9	0	11	7	7	7	8	0

Question n.55: Which of the following roles are considered within the group/committee that has been created to manage security incidents?



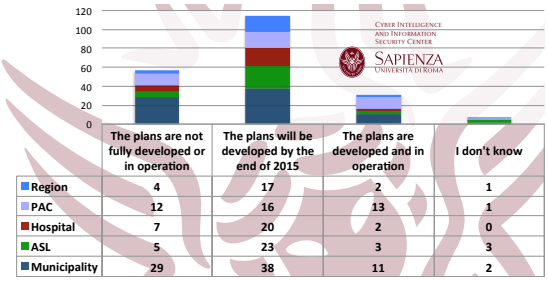
	Yes, at least once per year	Yes, at least onche each three years	No	I don't know
Region	9	2	12	1
PAC	15	7	13	7
Hospital	13	1	12	3
ASL	7	7	15	5
Municipality	24	8	37	11

Question n.57: Are the organization and operation of the ICT security regularly verified?



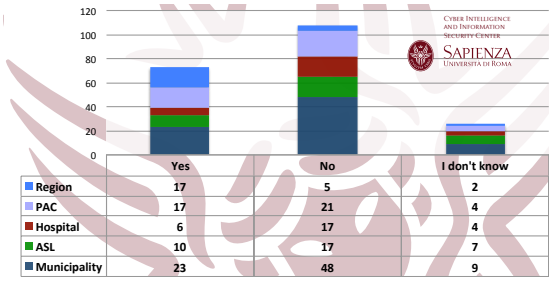
	Training programs	Operational guides	Regulations	Information leaflets	Nothing	I don't know	Other
Region	19	9	18	1	0	1	1
PAC	18	25	30	3	0	3	5
Hospital	16	13	20	3	3	2	2
ASL	17	15	26%	2	2	1	3
Municipality	38	33	50	3	11	2	10

Question n.58: Which of the following measures have been adopted to make staff aware of IT security issues?



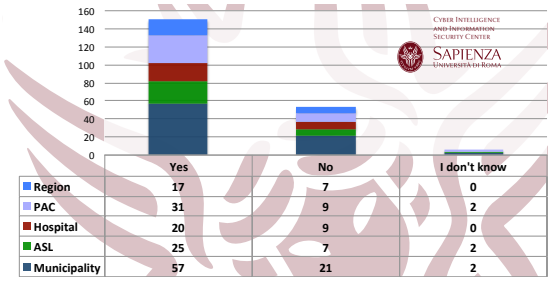
	The plans are not fully developed or in operation	The plans will be developed by the end of 2015	The plans are developed and in operation	I don't know
Region	4	17	2	1
PAC	12	16	13	1
Hospital	7	20	2	0
ASL	5	23	3	3
Municipality	29	38	11	2

Question n.59: According to the "Codice di Amministrazione Digitale" (CAD) regulating e-government, it is mandatory to have a disaster recovery and business continuity plan. Within your PA:



	Yes	No	I don't know
Region	17	5	2
PAC	17	21	4
Hospital	6	17	4
ASL	10	17	7
Municipality	23	48	9

Question n.60: CAD makes it compulsorily for public sector bodies to ask AgID for an advisory opinion regarding their disaster recovery and business continuity plans feasability study. Is this requirement observed?



	Yes	No	I don't know
Region	17	7	0
PAC	31	9	2
Hospital	20	9	0
ASL	25	7	2
Municipality	57	21	2

Question n.61: Is it possible that a problem in the ICT system of one or more outsourcers will have a significant impact on the operational continuity of the organization/authority?

Acronyms

ASL Local Health Boards

PAC Nationwide administrations

AgID Agenzia per l'Italia Digitale

CAD Codice di Amministrazione Digitale

ISMS Information Security Management System

ISTAT Istituto Nazionale di Statistica

INPS Istituto Nazionale della Previdenza Sociale