EUROPEAN COMMISSION
DIRECTORATE-GENERAL HOME AFFAIRS

SECURITY LIAISON OFFICER

FINAL REPORT

SECURITY LIAISON OFFICER PROJECT 2014

Printed in June 2014

Agreement Number: HOME/2012/CIPS/AG/4000003747

With the support of the “Prevention, Preparedness and Consequence
Management of Terrorism and other Security-related Risks Programme”
European Commission - Directorate-General Home Affairs

EXECUTIVE SUMMARY

Who is the "***Security Liaison Officer***"?

Article 6 of the Council Directive 2008/114/EC imposes to the European Critical Infrastructure operators to designate a Security Liaison Officer (SLO), but no specific indication has been provided to characterize the competences, roles and background of this professional figure. Hence it remains an extremely fluid concept.

To overcome such a drawback the European Commission co-funded the SLO project in the "Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risk Programme" of the Directorate-General Home Affairs.

From June 2013 to June 2014 the SLO project team analyzed the technical literature and acquired information from more than 350 experts via questionnaires, interviews and Workshop Cafés. The experts belong to more than 30 countries, including both EU Member and non-Member States, coming from both the private and public sector.

From the collected data it emerges the interest and relevance of a figure such as the SLO who might concretely contribute to promote information sharing, facilitate Public-Private Partnership and shape more effective strategies and solutions. Consequently there is a strong motivation to establish a standard profile of the SLO figure, and to introduce a more cogent and specific regulation on the subject of the SLO.

Specifically the SLO primarily serves as an interface between the Critical Infrastructure (CI) organization and the Public Authority (PA) or other operators, acting as a link between the organization and both National/European PA and other CI. SLO activities should be focalized in the preparedness and prevention phase, and not during a critical situation. To effectively perform his/her work, the SLO should be familiar with all the threats that are impacting the organization. Hence it is a largely shared opinion to appoint a person already within the organization because he/she already has a deep knowledge of the corporate processes and activities.

The general sentiment is that it is not necessary to have a dedicated Critical Infrastructure Protection (CIP) department inside a CI company. The majority of the answers identified a good position of the SLO inside the Security Department or as member of the Board of Directors. From the collected data it is preferable for the SLO and Chief Security Officer (CSO) to be two separate figures.

The SLO should have a strategic view in order to guarantee the continuous protection of the Infrastructure, with experience in management, but not necessarily former experience in law-enforcement or the military field. It is mandatory that he/she maintains a continuous training program and has an adequate academic background.

It is important to stress that in order to operate effectively, the PA should also introduce a figure similar to the SLO in order to facilitate exchange of information.

TABLE OF CONTENTS

INTRODUCTION

> “As the security function becomes increasingly critical, the industry must be poised to enhance its professionalism and define critical standards that will set security apart as a distinct field of study. Instituting professional standards can help to crystallize the understanding of emerging risks, and of security professionals’ responsibility for mitigating and managing them”[1].

While the security field continues to grapple with a myriad of challenges (cyber security, mobile technology, globalization, crime, natural disasters, etc.), the need for strategic thinking is ever growing.

In 2005, the Justice and Home Affairs Council called on the European Commission to focus on improving the protection of Critical Infrastructures (CIs) throughout Europe. The result was the creation of the European Programme for Critical Infrastructure Protection (EPCIP): an all-hazards approach to help Member States (MSs) to increase the level of protection and resilience of their CIs starting from those which failure may have pan-European consequences[2].

Indeed European CIs, due to the large integration and the presence of several interdependencies, are becoming a very complex system of systems where any single failure might trigger domino consequences affecting several Countries[3].

These exponential increases in inter-sectorial relationships and the introduction of new vulnerabilities reinforce the relevance of a figure such as the Security Liaison Officer able to operate as an interface between Public Authorities and private CI owners.

Now because the strength of any chain is no greater than its less robust link, the EU calls for a guarantee of minimum level robustness to all the Infrastructures deemed critical for Europe. The Council Directive 2008/114/EC represents a cornerstone element of such a strategy[4]. The Directive focuses on how to identify and designate a European Critical Infrastructure and subsequently require them to set-up an Operator Security Plan (OSP) and designate a Security Liaison Officer (SLO).

Specifically, article 6 comma 2 specifies “*Each Member State shall assess whether each designated ECI located on its territory possesses a Security Liaison Officer or equivalent*”. This is to facilitate information sharing and allow a more effective Public-Private Partnership with the aim to share ideas/opinions/facts which can harden CI assets and help to implement strategic plans.

The designation of a Security Liaison Officer, although mandated by the Directive, has proven more difficult than perhaps originally anticipated by the EU Commission. Critics argue that ambiguous language, such as the use of “or equivalent”, has left the definition of the SLO open-ended and confusing. Additionally, MSs and CIs, both public and private, have determined independent roles for the Security Liaison Officer leaving an obvious gap in interpretation and execution of the position.

[1] Enterprise Security Risks and Workforce Competencies; Findings from a Security Roundtable on Security Talent Development. University of Phoenix, ASIS; 2013.

[2] On a New Approach to the EPCIP; Making European Critical Infrastructures more secure. Commission Staff Working Document; EU – 28 August, 2013.

[3] R. Setola, S. De Porcellinis, and M. Sforna “Critical Infrastructure Dependency Assessment Using Input-output Inoperability Model”, Int. J. Critical Infrastructure Protection (IJCIP), Vol. 2, n. 4, pp. 170 - 178, 2009.

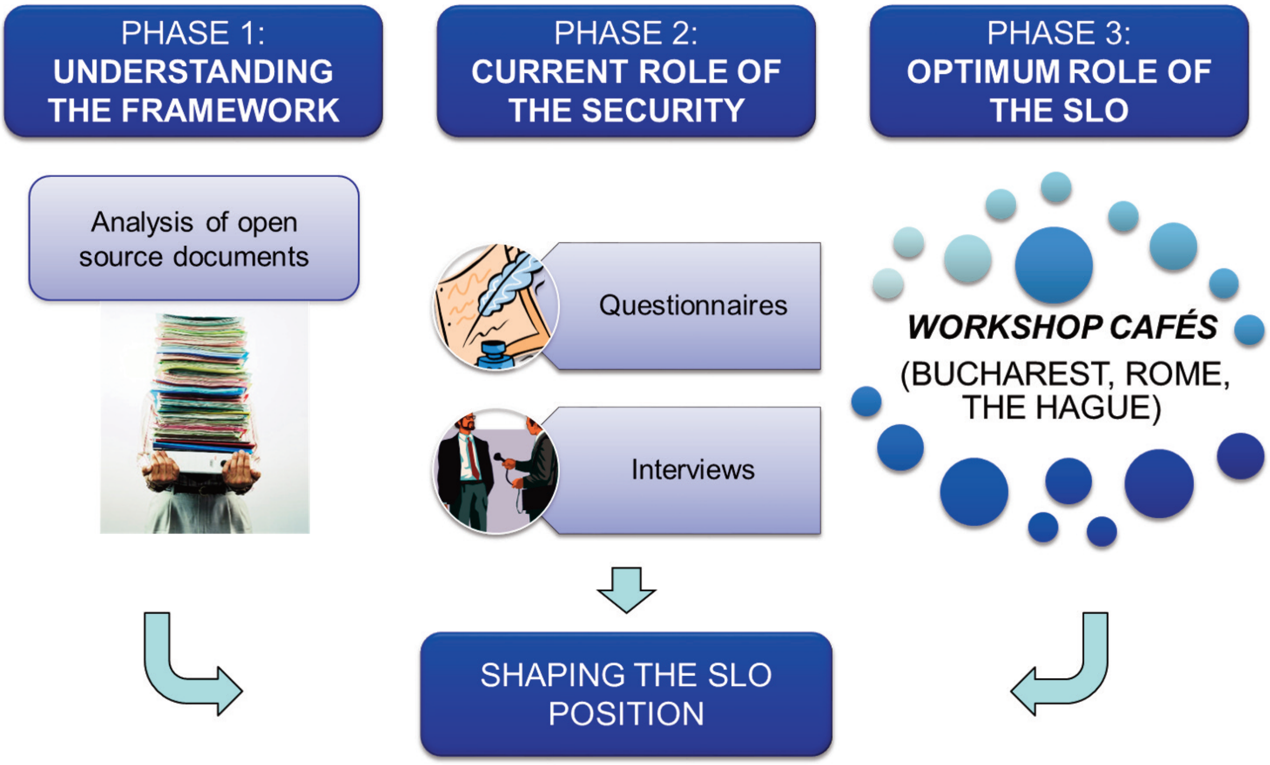
[4] Council Directive 2008/114/EC; 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection.

The European Commission – Directorate-General Home Affairs – co-funded the project "Security Liaison Officer" (SLO project) to better define this role, responsibilities and background.

The SLO project has utilized a three-pronged approach to help identify the SLO role. Via open-source documents, the dissemination of a tailor-made questionnaire to experts in the field of CIs, and three Workshop Cafés (meetings designed to spur discussion surrounding CIP and provide best-practice to SLO-related issues). Although the end-goal is to deliver a product for the European Union, experience outside Europe (United States, Australia, New Zealand, etc.) was analyzed to provide a more complete vision about such a professional figure.

The SLO project was built upon a myriad of informed opinion/statistical data/operational success/forward thinking approaches and gap analysis research. The goal was to provide a "European vision" of the SLO in terms of his/her background, competences and roles with the aim to support a standardized process, so the SLO can be an effective interface amongst, public-private, and private-private actors. The results of the project are intended to be both a starting point for the definition of a regulatory standardized framework for such a professional figure, and a guideline for technicians to better interpret the role of the Security Liaison Officer.

Three-phase structure of the SLO project activities.


PHASE 1:
UNDERSTANDING THE FRAMEWORK
PHASE 2:
CURRENT ROLE OF THE SECURITY
PHASE 3:
OPTIMUM ROLE OF THE SLO
Analysis of open source documents
Questionnaires
Interviews
WORKSHOP CAFÉS
(BUCHAREST, ROME, THE HAGUE)
SHAPING THE SLO POSITION

This report only summarizes the results of the project. Further details and information about SLO project outcomes can be requested to the SLO team using the contact details indicated at the end of this report.

STATE OF THE ART

Critical Infrastructures are no longer separate systems but are physically and logically interdependent and the update of their resilience accordingly is mandatory. Advances in technology and globalization have obviously aided in the intertwining of these CIs, increasing their efficiency but also exposing new vulnerabilities. Further, given that the European Union (EU) currently consists of 28 Member States (MSs), there are as many different cultures, approaches and needs.

In this framework, the European Commission promoted the European Programme for Critical Infrastructure Protection (EPCIP) within the issuing of the Council Directive 2008/114/EC.

Over the years, due to the changes in the geopolitical status worldwide and to the different initiatives implemented at the European level, several MSs consider a comprehensive review essential for both the whole EPCIP, concerning the underlying logistic, assumptions, objectives, and approaches of the Programme and of the Council Directive as a legal instrument[1]. In response to this, the Commission Staff Working Document SWD(2013)318, released in August 2013 by the European Commission (EC), details a more practical implementation of EPCIP. It is worth to notice that this new approach also takes into account the interdependencies between CIs, industry, and state actors[2]. As stated in the SWD (2013)318 less than 20 European CIs (ECIs) have been designated and consequently very few new Operator Security Plans (OPS) have been produced. Although the EPCIP has not completely fulfilled its intended goals, it is still relatively young and has succeeded in raising CIP awareness throughout the EU community (for more details see Table 1).

Concerning the SLO figure the SWD(2013)318 does not provide any input and it is not clear if any of the designated ECI's currently have a SLO. To further compound the situation, there is information about the SLO indicated by companies which are not included in the ECI list.

Some more elements about SLO were specified in the green paper "on a European Programme for Critical Infrastructure Protection" COM(2005)576. Specifically in article 8.1 it was specified that operators designed as ECI or as National CI have to nominate "a senior representative(s) to act as Security Liaison Officer (SLO) between the owner/operator and the relevant MS CIP authority. The SLO would take part in the development of security and contingency plans. The SLO would be the main liaison officer with the relevant CIP sector body in the MS and where relevant with the law enforcement authorities". But in the following legislative acts several aspects, including the responsibilities of the SLO, have been largely updated, hence it is questionable the coherence of such vision with the actual legislation framework. Consequently, currently there are no specific roles, responsibilities and tasks affiliated with the SLO position in the EU, thus the role can be molded into a desired product built upon a wide variety of skillsets and backgrounds. For example, although all Security Managers in Europe must not have a criminal record, thus far only Spain has mandated that the SLO should be a qualified Security Manager. Further, some countries (Hungary, Romania) require agreement with the CIP authorities to appoint the SLO. Although the Security Manger, Chief Security Officer and Security Liaison Officer fulfill roles, there are overlapping desired knowledge/skillsets in all of them. Can the SLO coincide with one of the preexisting figures inside an organization? Moreover, since there are already ISO standards, which define in detail the duties and responsibilities of the Security Manager, why would there be a need to explicitly define

[1] Study to support the preparation of the review of the Council Directive 2008/114/EC on the "identification and designation of European critical infrastructures (ECI) and the assessment of the need to improve their protection" contracting authority: European Commission; prepared by: Booz & Company GmbH - 05 March 2012

[2] On a New Approach to the EPCIP; Making European Critical Infrastructures more secure. Commission Staff Working Document; EU – 28 August, 2013

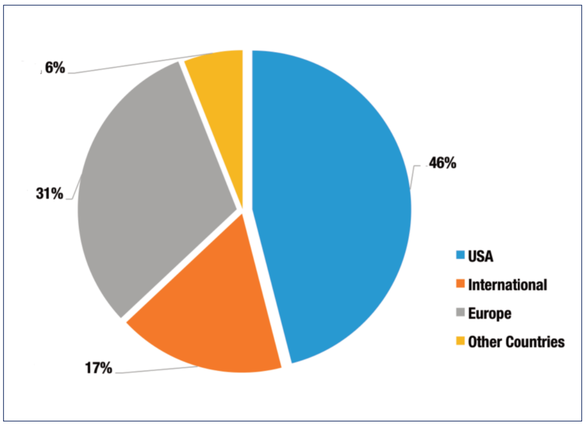
TABLE 1: Current operating status within Europe regarding Council Directive 2008/114/EC as reported in SWD(2013)318

Implementation has been largely successful	• 26 Member States (MS) have implemented the Council Directive through legal or policy/procedure means - Largely driven by MS authorities with minimal private sector participation • A few MS claimed it helped formalize a national CIP program • MSs with consultative national approach would prefer a non-obligatory instrument • There were no major issues faced by MS in transposing the Council Directive
The ECI process should be reviewed to validate that the outcome (20 ECI) reflects the reality	• Questions have been raised about the appropriateness of sectorial criteria • Cross-sector dependencies have not been included in the assessment process • Lack of uniformity in interpretation of acceptable “alternatives” • Very few new OSPs seem to have been created as a direct result of the Council Directive (most MS had OSP-equivalent requirements already in place for operators) • The added value of the Council Directive on its core objective of improved protection is debatable • MS viewpoints on improvement of security levels are intuitive as no direct measurement was undertaken
There is a lack of consensus with regards to expansion of scope	• Opinion is divided about inclusion of ICT in scope among MSs and Operators • Many MSs are interested in considering expansion of scope to cover the Space and Finance sectors • Evidence of impact in Energy and Transport are important to build support for a decision on scope expansion
Many MSs would like to evaluate alternative assessment approaches to improve effectiveness	• Many MSs point out the need for an additional “Top down” component of the Identification / Designation process
Opportunities exist for strategic alignment of Council Directive objectives with other initiatives	• Review original EPCIP objectives and role of Council Directive • Streamline initiatives with other Directorate-General’s and MSs.

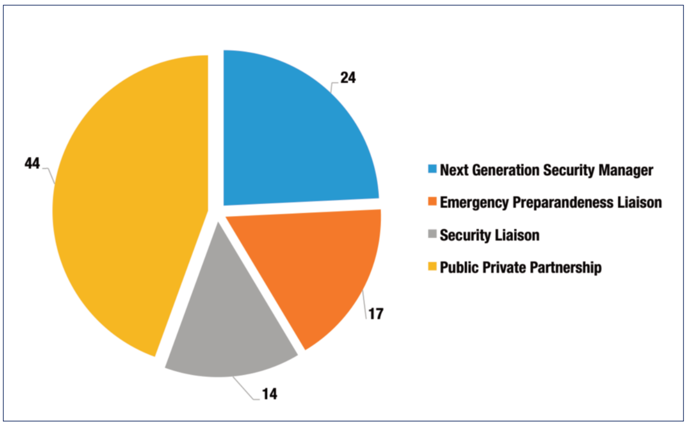
the Security Liaison Officer? These are just some of the questions that arose from the research and that the SLO project is trying to address.

To this purpose, we considered more than 100 documents, mainly from the United States, where the Liaison Officer figure has been historically associated to the military field, although our analysis covered a broad scope of domains.

Document source.



Document type.



In general, the term Liaison Officer (LO) is most commonly associated with the military. In this capacity, the LO serves both to exchange information/ideas and act as diplomatic representative of his/her respective country. The definition provided by CSA[3] is that "*a liaison officer is a person that liaises between two organizations to communicate and coordinate their activities by serving as an official go-between for senior official of both organization*".

Consequently, the term Security Liaison Officer (SLO) indicates a LO which operates specifically in the security field. The term SLO can also assume different meanings, for example for the Canadian government Security Liaison Officers are posted inside embassies to gather security-related intelligence from other nations, and the MIS UK secret service also utilizes field officers for the same purpose.

The United States Coast Guard released a "Liaison Officer Manual" (see the box). The language used in the manual is quite ambiguous. Specifically, the "qualifications" section of the manual leaves much to interpret. This intentional obscurity is required because emergency situations are not necessarily tailored to a typecast responder. However, the regulation of the qualification standards (such as the National Incident Management System courses) allows the ability for Liaison Officers to contain static core competencies and greatly increases their value through the external acknowledgement of their skillsets (e.g. the public can expect a particular level of quality from Liaison Officers) and predictable internal capabilities (e.g. Liaison Officers can exchange information and anticipate the maneuvers of their colleagues).

Although the SLOs share some of the responsibilities of their military counterparts, they fulfill fundamentally different positions. Most notably, the SLO has a completely different command structure; the public and private sectors equally play an important role in CIP and the SLO must seamlessly communicate with all parties involved without being restrained by military tactic/strategy. In fact, the

[3] CSA Cloud Security Alliance – International Standardization Council "Role and Responsibilities for Liaison Officer", 2012.

US COST GUARD “LIAISON OFFICER MANUAL”

The following lists are excerpts from the manual.

Job Description

The LO:

- Is a member of the command staff
- Is designated by the Incident Commander/Unified Command (IC/UC)
- May be a federal, state, local, or responsible party individual
- Reports to the IC/UC
- Is responsible for the information flow between the response organization and other agencies/stakeholder groups

Primary Objectives

- Contribute to the efficiency of the response by ensuring the best use of available assisting agency resources and cooperating agency support
- Contribute to the positive public perception of the response and the attainment of stakeholder objectives by effectively handling stakeholders and their concerns

Qualifications

When considering persons to act as the Liaison Officer for an incident or event, the individual must have superlative interpersonal skills; crisis response experience; be familiar with Incident Command System; be trained in risk communication, consensus building, and public relations; be able to function calmly in a high-stress environment; be able to delegate authority in order to meet liaison objectives.

military LO is so different from the SLO, that the inclusion of the word ’Officer’ in the title of the position has been a matter of strong debate throughout the SLO project.

In addition to the military, the Liaison Officer has, among many other roles, served in the corporate world (coordinating the completion of projects involving several companies), the law enforcement community (serving in schools and community centers to help spread knowledge and awareness) and several agencies and organizations for emergency and disaster management. This is important because the LO should be founded upon the basic intangible elements that can transfer between multiple sectors and all levels of the workforce.

The Resilience Expert Advisory Group from Australia has released a cross sectorial checklist of elements that an organization must deploy in order to strengthen their overall resilience. The list includes a profile for a professional figure similar to SLO: strong leadership with clear, firm decision making; a management attitude (flexible and adaptive); communication skills; good problem solving ability; a culture of cooperation and mutual respect[4]. Similar consideration has been done by the New Zealand government, which identified in the presence of a function as the SLO, a useful contribution to bridge the gap improving the capabilities to transfer information[5].

Critical Infrastructure Protection (CIP) in the United States has transformed over the past fifteen years, stemming from a Presidential Directive in 1998 (PDD 63). Under the National Infrastructure Protection Plan (NIPP)[6], the United States has created a framework to better coordinate the public and private sectors. In short, both the public and private areas have selected representatives from each identified CI. These “Sector Liaison Officials” from the public side and their counterparts in the private sector,

[4] Organizational Resilience; Resilience Expert Advisory Group. Australian Case Studies; 2011.

[5] International Disaster and Risk Conference, Davos. Critical Infrastructure Resilience: Perspective from New Zealand. 28 August 2008.

[6] National Infrastructure Protection Plan; Partnering to Enhance Protection and Resiliency. Department of Homeland Security, 2009.

"Sector Coordinators", worked together to actuate the NIPP. Although the public/private relationship was exploited to create a multifaceted plan, debate continues to swirl around its effectiveness. This is mainly due to the politics associated with the plan; Sector Coordinators have been accused of instilling a "culture of fear" regarding their CI arena in an effort to garner more government funding. Even with these obstacles, the NIPP is widely regarded as, at a minimum, a strong resource for CIP. Along with Sector Coordinators and Sector Liaison Officials, the United States has multiple "Liaison Officers" in operation.

Even though there have been commendable efforts throughout the EU to specifically identify the role of the SLO, only one country within the EU has successfully implemented the SLO position via mandates: Romania (see the box).

SLO POSITION DUTIES IN ROMANIA (AN EXCERPT FROM THE ROMANIAN PRIME MINISTER RESOLUTION No. 166 – 19 MARCH 2013)

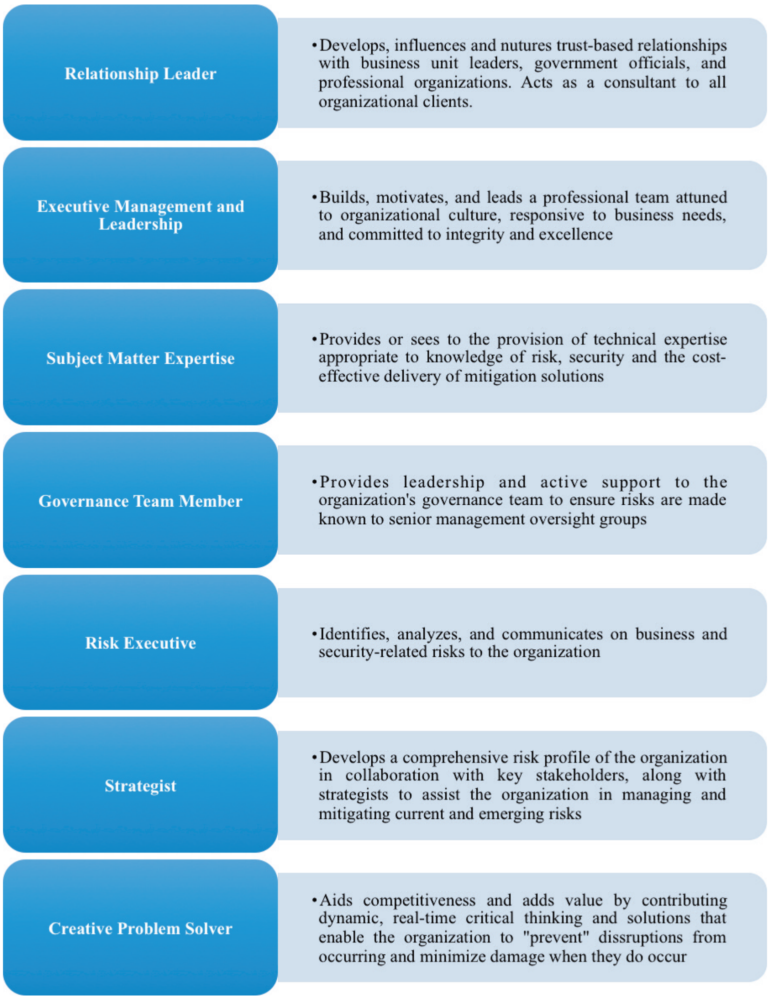
I. *The Security Liaison Officer (SLO)* is the head of the specialized compartment (comprising of at least a three member team) designated at the level of the competent public authorities or the level of the National / European critical infrastructure owner / operator / administrator, and is under the direct authority of the leader of the competent public authorities, respectively that of the National / European critical infrastructure owner / operator / administrator. He is also:

- The person responsible for activities in the field of Critical Infrastructure Protection /head of compartment, at the level of the competent governing body;
- The head of compartment, specializing in National / European Critical Infrastructure Protection, at the level of the National / European critical infrastructure owner / operator / administrator.

III. In the pursuit of his duties, ***the Security Liaison Officer of the National / European critical infrastructure owners / operators / administrators*** must fulfill the following main requirements:

a) Act as the point of contact between the National / European critical infrastructure owner / operator / administrator and the competent public authority, the Centre for Critical Infrastructure Protection Coordination (CCIPC) and the other competent authorities, for all matters relating to Critical Infrastructure Protection;
b) Drafts and/or updates risk assessments and identifies points of vulnerability for the National / European critical infrastructure he is responsible for, or proposes the initiation, within the framework of applicable legislation, of the process for selecting a certified person or company to fulfill the aforementioned tasks;
c) Drafts threat scenarios pertaining to the National / European critical infrastructure under his area of responsibility;
d) Is responsible for the periodic revision / update of documents drafted at the level of the designated specialized compartment of the National / European critical infrastructure owner / operator / administrator;
e) Is responsible for maintaining the up to date status of the database relied upon by the national mechanism for communication in the field of Critical Infrastructure Protection. This includes information related to risks, threats and vulnerabilities which have been identified in relation with the National / European critical infrastructure under his supervision;
f) Provides permanent monitoring of the evolution of risks, vulnerabilities and threats to the National / European critical infrastructure for which he is responsible;
g) Disseminates information to the competent public authorities and other interdependent bodies, regarding the evolution of risks, threats and vulnerabilities to the National / European critical infrastructure under his supervision;
h) Proposes immediate countermeasures whenever risks towards the National / European critical infrastructure under his supervision have materialized;
i) Participates, at the request of the competent public authorities, in the process of establishing the critical thresholds and criteria for the National / European critical infrastructure under his supervision;
j) Is responsible for the evaluation, testing and, if necessary, the update and revision of the OSP for compliance with terms advanced by the applicable legislation;
k) Organizes and conducts exercises and activities specific to the testing of the OSP and of equivalent documents;
l) Ensures the drafting and submission, for review, to the competent public authority, of the OSP generated within the specialized compartment of the National / European critical infrastructure owner / operator / administrator;
m) Plans and ensures, within the framework of the law, the participation of subordinate staff in specialized training activities;
n) Provides the drafting and submission of classified documents, relating to the National / European critical infrastructures under his supervision, ensuring compliance with current legislation regarding access to classified materials;
o) Constantly fulfills the obligations assigned to him as enshrined in the national legislation applicable to his field.

Both the Security Liaison Officer and the Chief Security Officer positions understand that specific considerations and responses must be based on identified risk assessments, intelligence, assumptions and requirements[7]. Some of these characteristics are well codified by the ANSI/ASIS International required skills for the CSO:



Relationship Leader

- Develops, influences and nutures trust-based relationships with business unit leaders, government officials, and professional organizations. Acts as a consultant to all organizational clients.

Executive Management and Leadership

- Builds, motivates, and leads a professional team attuned to organizational culture, responsive to business needs, and committed to integrity and excellence

Subject Matter Expertise

- Provides or sees to the provision of technical expertise appropriate to knowledge of risk, security and the cost-effective delivery of mitigation solutions

Governance Team Member

- Provides leadership and active support to the organization's governance team to ensure risks are made known to senior management oversight groups

Risk Executive

- Identifies, analyzes, and communicates on business and security-related risks to the organization

Strategist

- Develops a comprehensive risk profile of the organization in collaboration with key stakeholders, along with strategists to assist the organization in managing and mitigating current and emerging risks

Creative Problem Solver

- Aids competitiveness and adds value by contributing dynamic, real-time critical thinking and solutions that enable the organization to "prevent" disruptions from occurring and minimize damage when they do occur

These CSO skills can help to build the framework for the SLO position because the challenges and threats are often similar for both positions. However, the two positions have different peculiarities.

It is interesting to note that the idea of designating qualified personnel to operate an interface to improve the management of complex situations gained large attention in several fields, including the Support Liaison Officer concept introduced by the UEFA[8] to serve as a bridge between the fans and the clubs. Similar figures have been introduced for the Port and Homeland Security domains. These examples emphasize the urgency into a world more and more interconnected and complex to identify preferential communication channels, based on the presence of highly skilled personnel able effectively manage unpredictable situations.

[7] Chief Security Officer – An Organizational Model. American National Standards Institute; ASIS International; 2013.

[8] UEFA Supporter Liaison Officer Handbook, 2011
http://www.uefa.com/MultimediaFiles/Download/Tech/uefaorg/General/01/84/35/28/1843528_DOWNLOAD.pdf

QUESTIONNAIRE RESULTS

The activities of security, especially within organizations managing Critical Infrastructures, have changed considerably over the last ten years. The scope of security was once limited to the protection of organizations' people and assets against malicious activities. Nowadays, the security mission embraces further aspects, including service continuity, company reputation, management of crisis situations, etc. This is because companies today must operate in a global market characterized by the presence of a large number of interdependencies, fast dynamics, "new" types of threats and compelling requirements from the end-users. These new security aspects forced companies to adopt new security solutions. Sometimes such solutions are implicit: this is the case, for instance of the All-Hazard approach which aims at both contrasting threats and mitigating negative consequences. Hence the classical aspects of physical and personnel security (e.g., competence, management, soft-skills, etc.) have adapted to include aspects of prevention and preparedness. These new aspects should now be considered mandatory for the definition of plastic and pro-active strategies. This security shift also imposes changes in the organizational chart; the responsibility of the security positions are moving from under the purview of the Director of the Personnel or Legal departments to a staff position of the CEO or equivalent senior position.

To concretely evaluate the relevance of such changes and to perform a snapshot of the current company security context, the SLO project analyzed the security professional domain via questionnaires. The shaping and construction of the questionnaire was a multi-month process based on open source analysis, operational expertise, and continuous feedback from the Advisory Board members. Additionally, the questionnaire was also subjected to criticism from the participants of the First Workshop Café. Ultimately, every single question was critiqued to ensure its added value to the project.

It was determined early in the project that a single questionnaire for such a broad spectrum of expertise would not suffice. The most efficient method for defining the SLO profile would require a specific set of questions for specific roles. Thus, the questionnaire was broken down into 4 distinct categories:

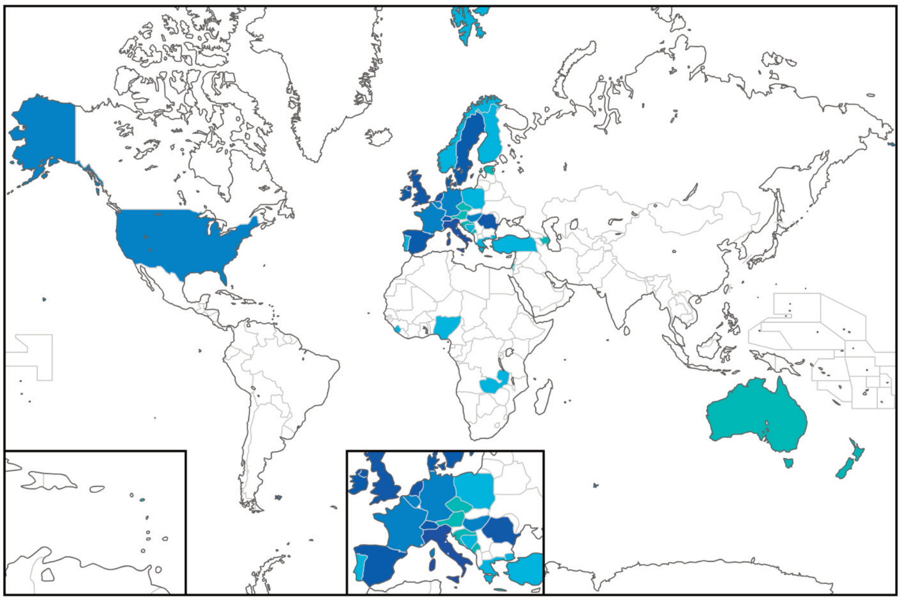
- Public Authority (PA)
- Chief Security Officers (CSOs)
- Security Officer' staff members
- Academia

These four categories encompass the target audience for this project and provide unique perspectives regarding the SLO profile. Prior to beginning the questionnaire, each participant identified his/her appropriate category and was directed accordingly to a set of tailored questions suited to his/her expected knowledge base and exposure. This targeted approach provided four distinct viewpoints of the SLO profile and helped us compile a more accurate set of data.

Specifically, the questionnaires aimed to quantify the security framework, identify how it has changed over recent years and identify the most relevant trends. Moreover, the questionnaires investigated the professional figure of the Chief Security Officer (CSO) and his/her team in terms of competences, role and background.

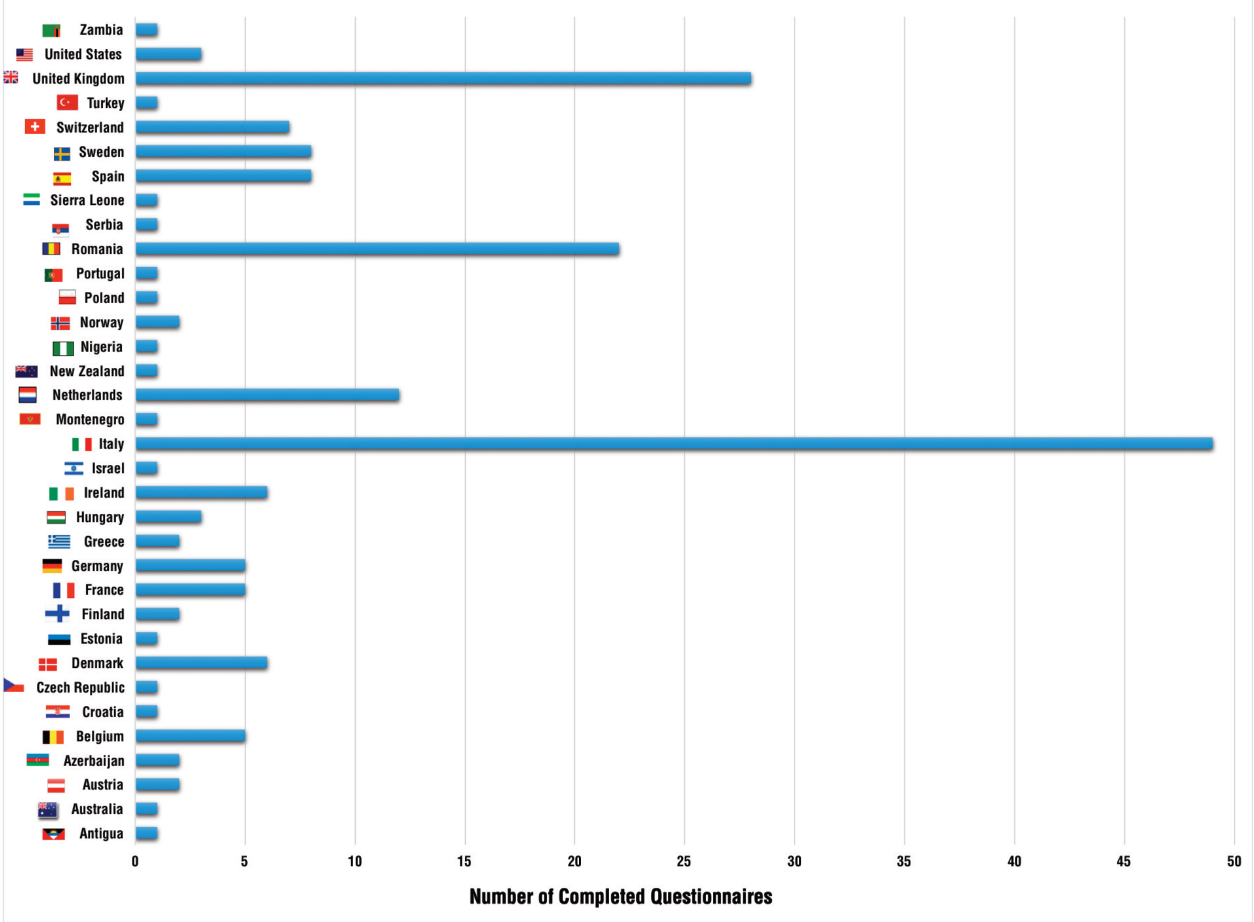
In the period from October 2013 to May 2014 we collected 200 questionnaires from 34 different countries (19 Member States and 15 Non-Member States).

Participation to the SLO survey (a darker blue indicates a higher number of collected questionnaires).



The majority of data stems from EU countries, however, we also collected information from North America, Australia and Africa. This wide spectrum of diversity has ensured that the collected data are not biased towards one region (e.g. Northern Europe, Western Europe, Africa, North America, etc.) or category (Public Authority, Chief Security Officers, Staff Security Officers, Academia). The following graph provides a detailed breakdown of the questionnaire participants per nationality.

SLO survey participants origin.

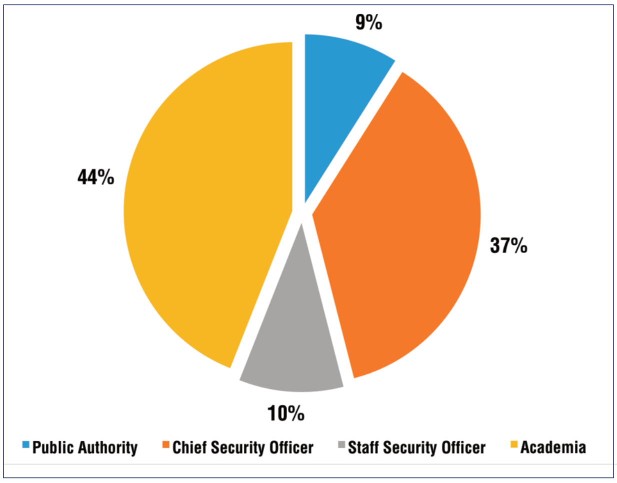


A large portion of the completed questionnaires was from personnel working in the security field and academia. An important note regarding the questionnaires is that some of the questions tailored for the academia community queried what the responder would "want" vice what their organization actually "has". Although this may be perceived as a limitation, we interpreted it as an advantage. We have used this data to help balance the actual happenings of the SLO with the desired role.

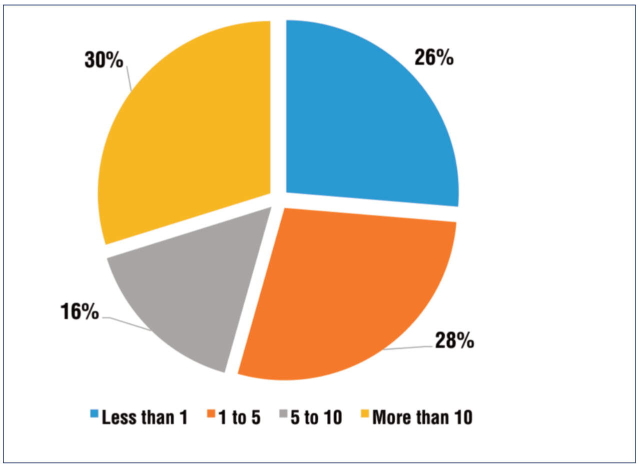
The smallest set of data was derived from the Public Authority category: 17 questionnaires were collected from Italy, UK, Romania, Sweden, Germany and The Netherlands.

From the collected data, it appears that the security budget for the next five years will be aligned with those experienced in the past. Given the current budgetary constraints within the EU and abroad, this continuing upward trend of funding is further evidence of the sizeable attention that security is garnering. According to the data, more than 30% of the CSOs foresee an annual security budget greater than 10 M€ for the next five years. Further, roughly half of all the CSOs are predicting a budget of more than 5 M€/year over the next five years. Having said that, our data concludes that Public Authorities are spending less than others in the security field.

SLO survey participants per category.

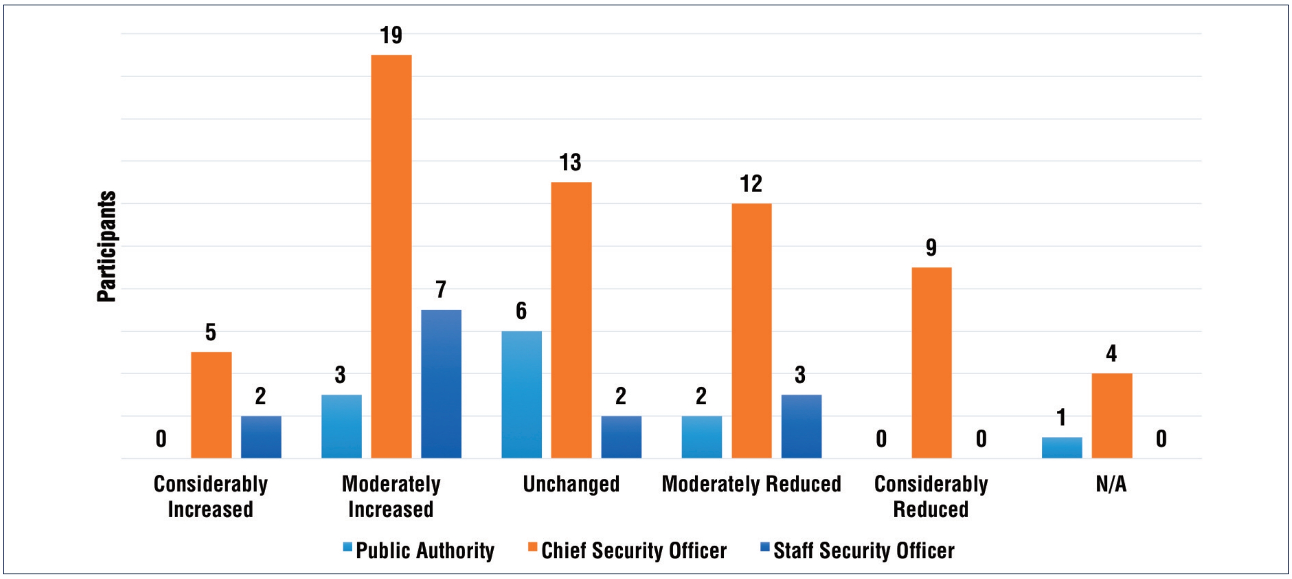


Chief Security Officer Annual Security Budget (EUR Million) for the next 5 years.



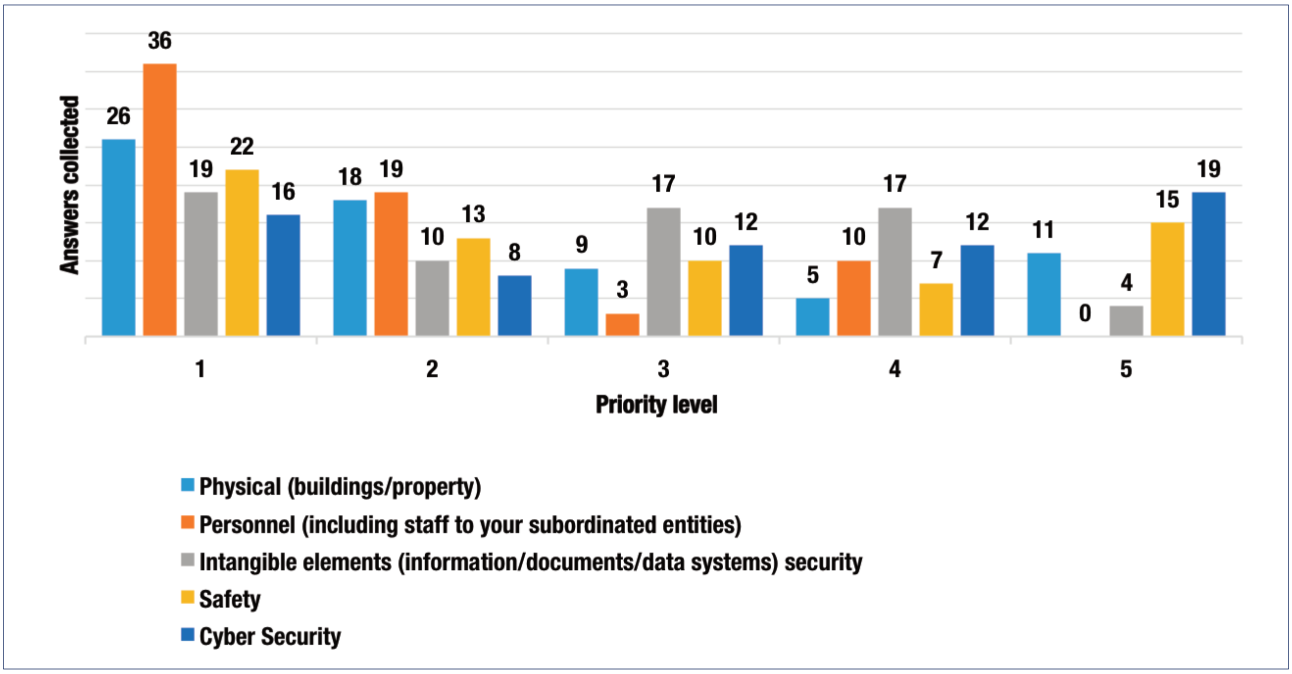
The increase in attention towards security is further emphasized by the incremental growth in the number of persons involved within the security division.

Has the number of Security Personnel within your organization changed within the past 5 years?



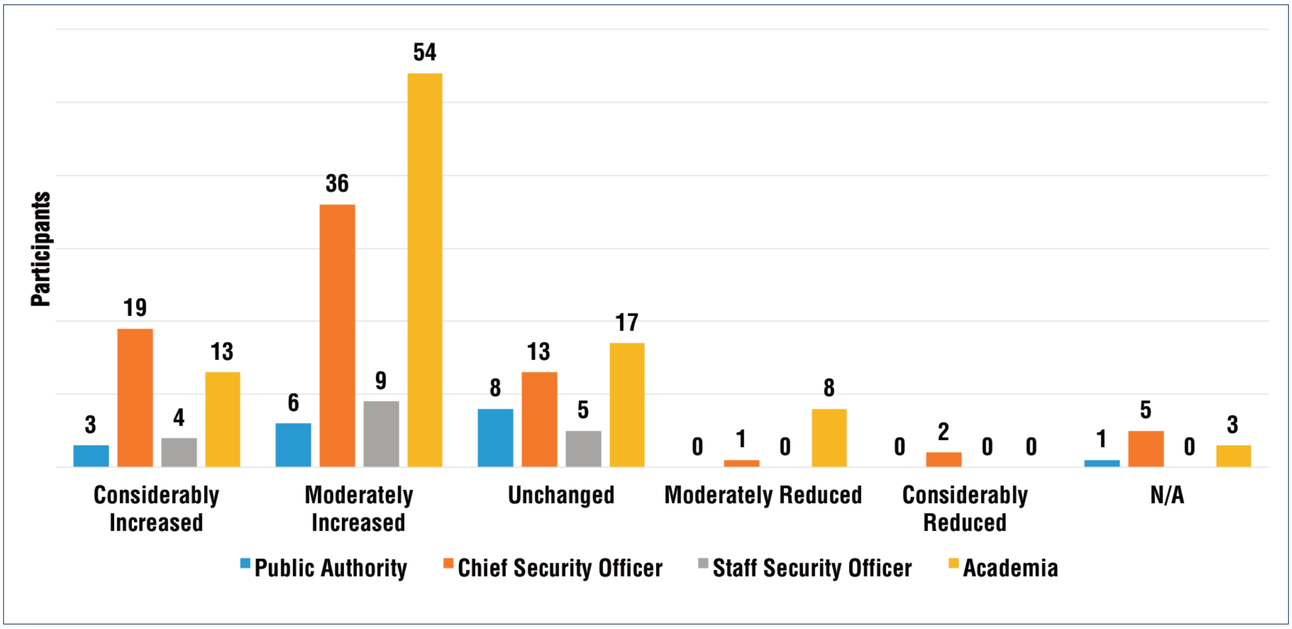
Concerning the varying focal points of security, the most important aspect is personnel security: nearly a quarter of respondents considered personnel security as the most essential domain, stressing the utmost importance attributed to the personnel inside a company (notice also the large relevance attributed to safety).

How do you rank the relevance of the different security domains (1= top; 5=less important)?

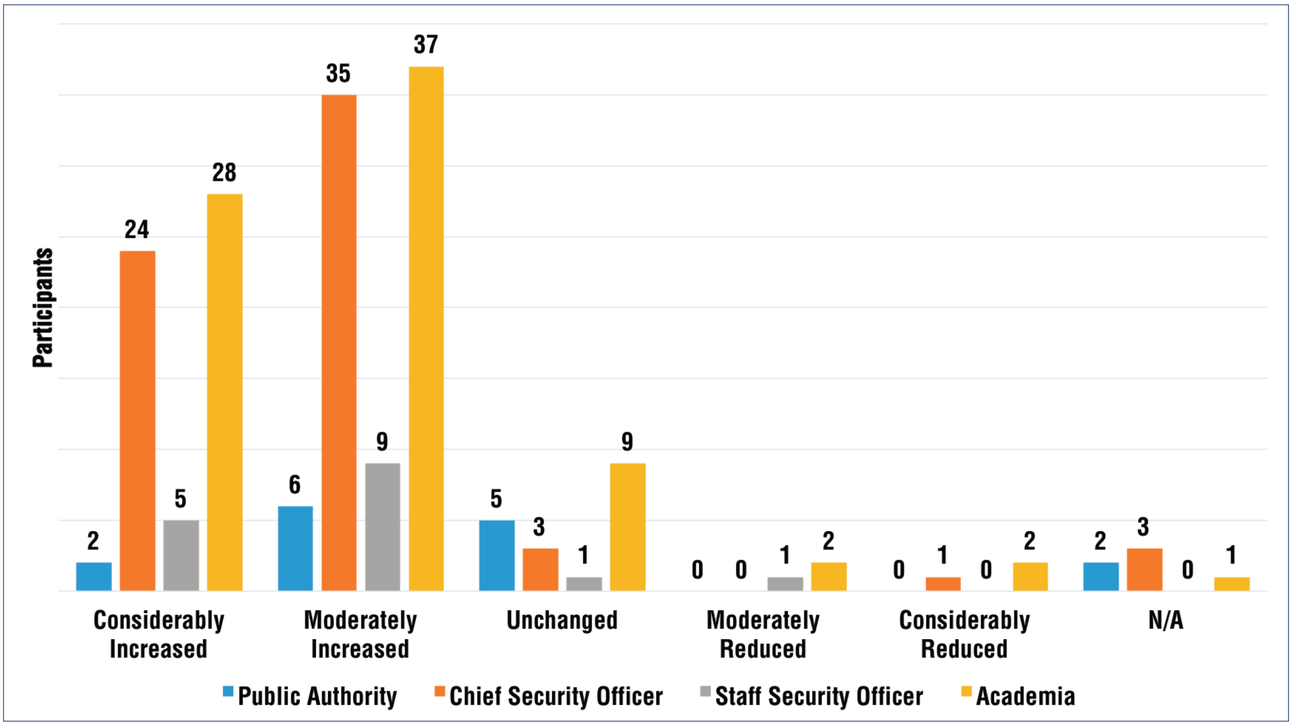


However, our data shows that in the last five years there was a considerable boost in the security standards for the physical and cyber security domains, while personnel security standards received much less attention. The increased relevance of the physical and cyber aspects can be one of the reasons that justify the augment of the number of persons involved within the security division.

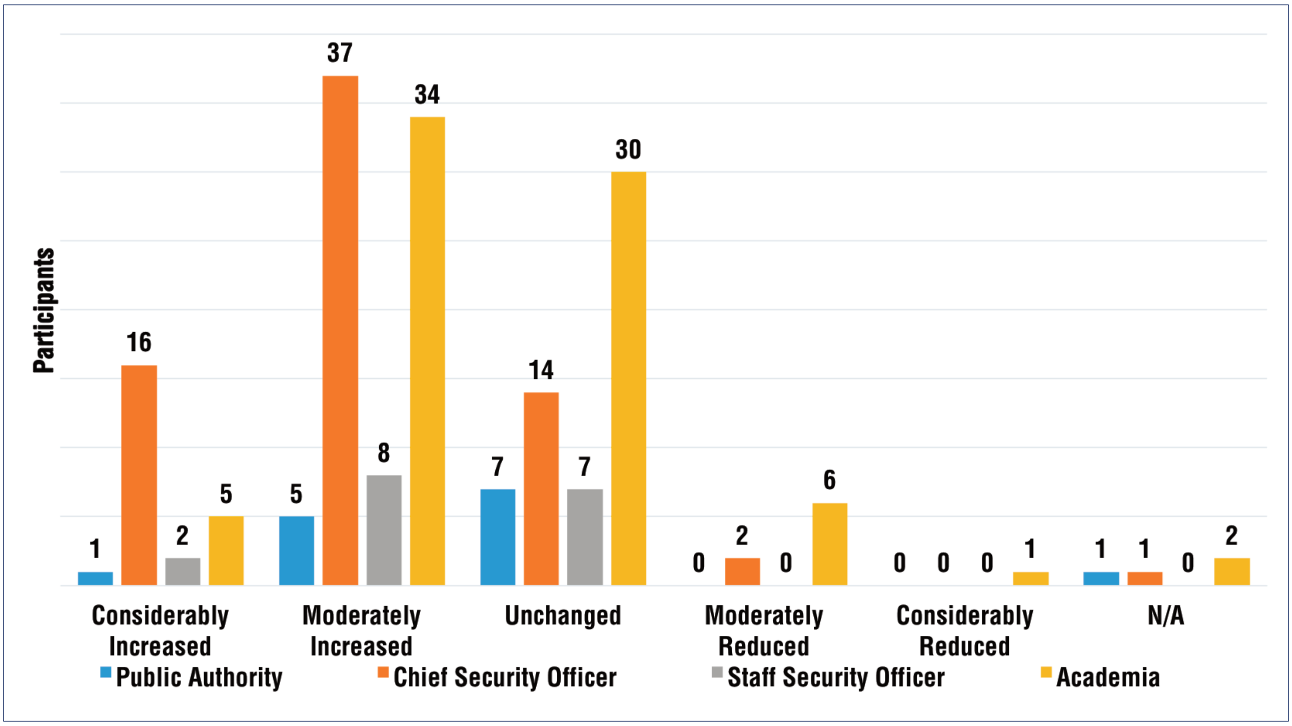
Physical Security Standards.



Information Security Standards.



Personnel Security Standards.

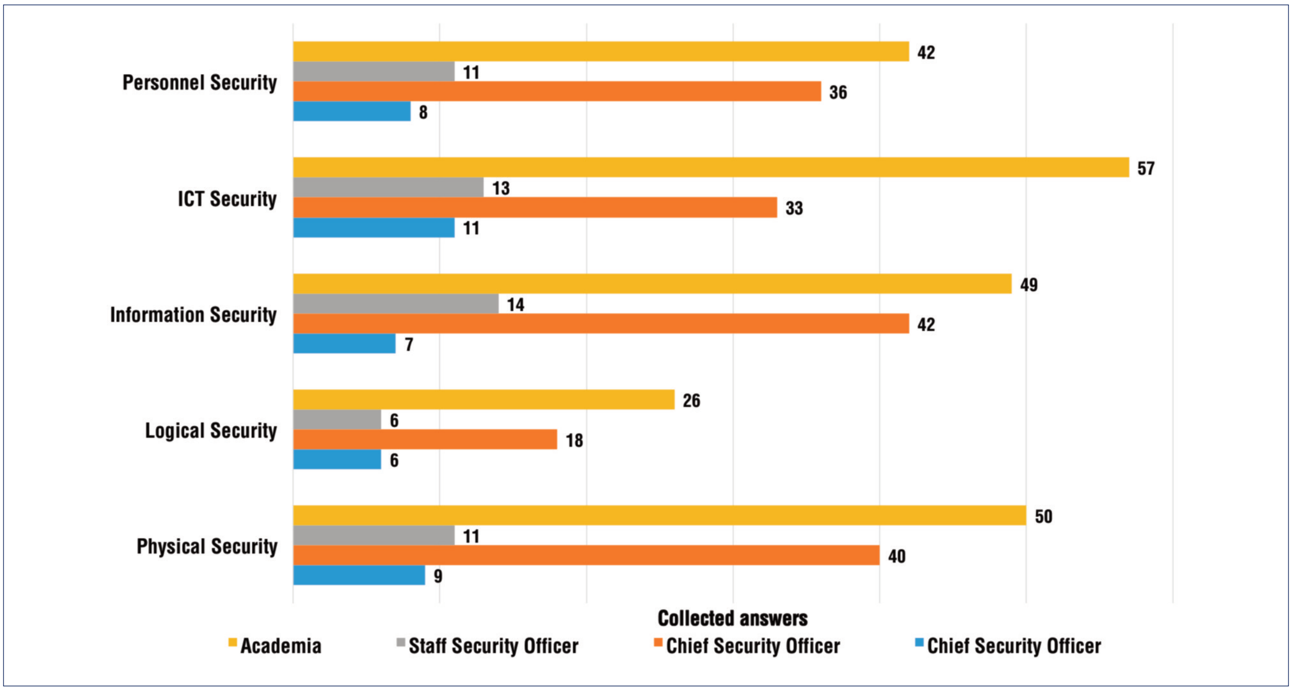


Overall, the majority agree that security requirements increased, although this feeling is more evident in the private sector rather than in PA. This increased relevance of the private sector in the security of CIs is a direct consequence of the elimination of national monopolistic operators and, consequently, of the absence of direct PA resposability vice a more market-oriented management of CI. Subsequently, there is a larger amount of attention towards prevention rather than prosecution and repression.

Notice that although “Personnel Security” was considered the “most important” domain within an organization, more stakeholders marked “Unchanged” for personnel security than any other type of security domains.

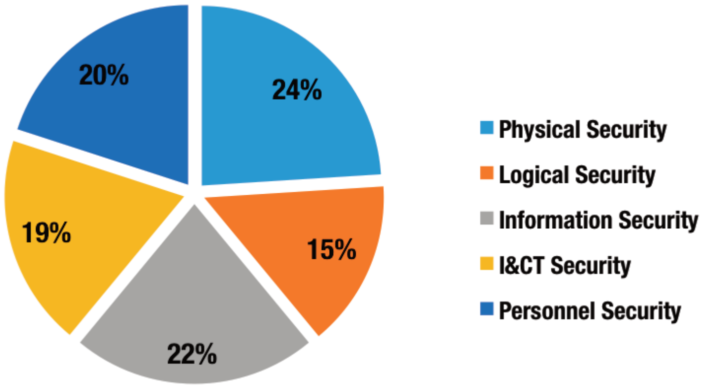
The overall increase in security budgets, personnel and standards promotes the relevance of the different dimensions of security for each category (Public Authority, Chief Security Officers, Staff Security Officers, Academia). The data shows that all security fields (Physical Security, Logical Security, Information Security, IC&T Security and Personnel Security) are receiving a balanced amount of attention, stressing the relevance of All-Hazard approaches.

Where is the focus for differing roles?



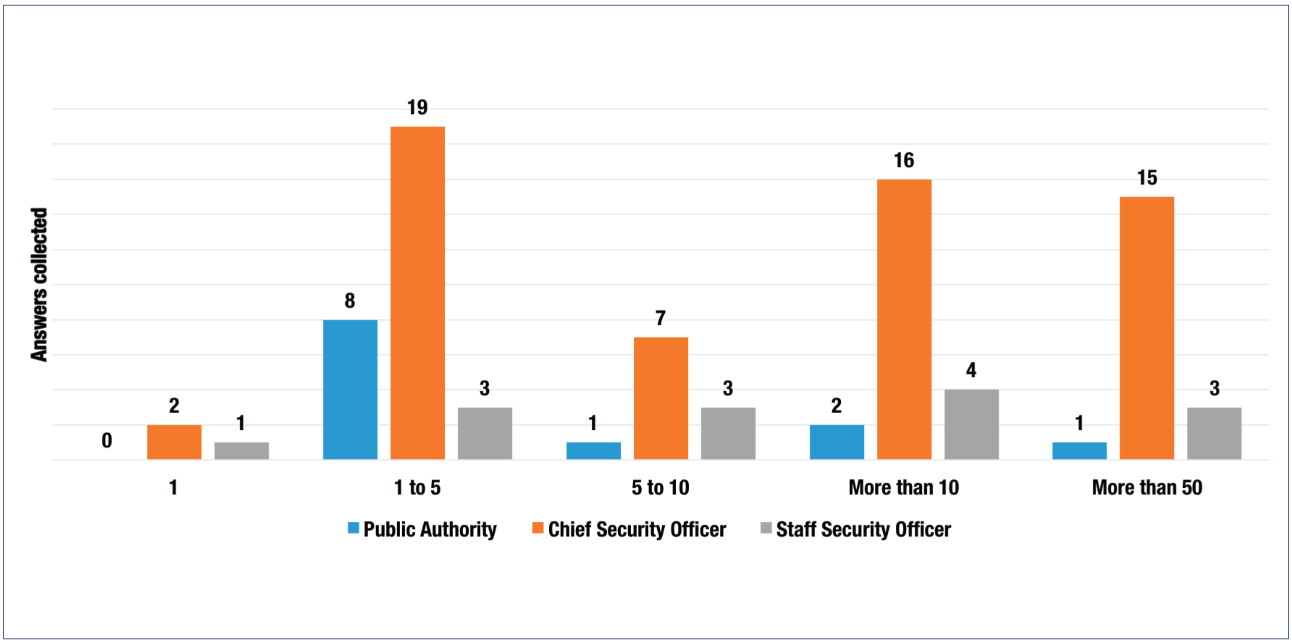
This balanced approach towards security is further confirmed by the CSO category answers regarding resource allocation. From the related graph one can notice that resources will be allocated quite uniformly on all the different aspects of the security domain. Similar indications also come from the answers provided by the other categories, with the only difference being that Public Authorities allocated a moderately higher attention towards ICT security (about 26%).

CSO Budget Allocation.



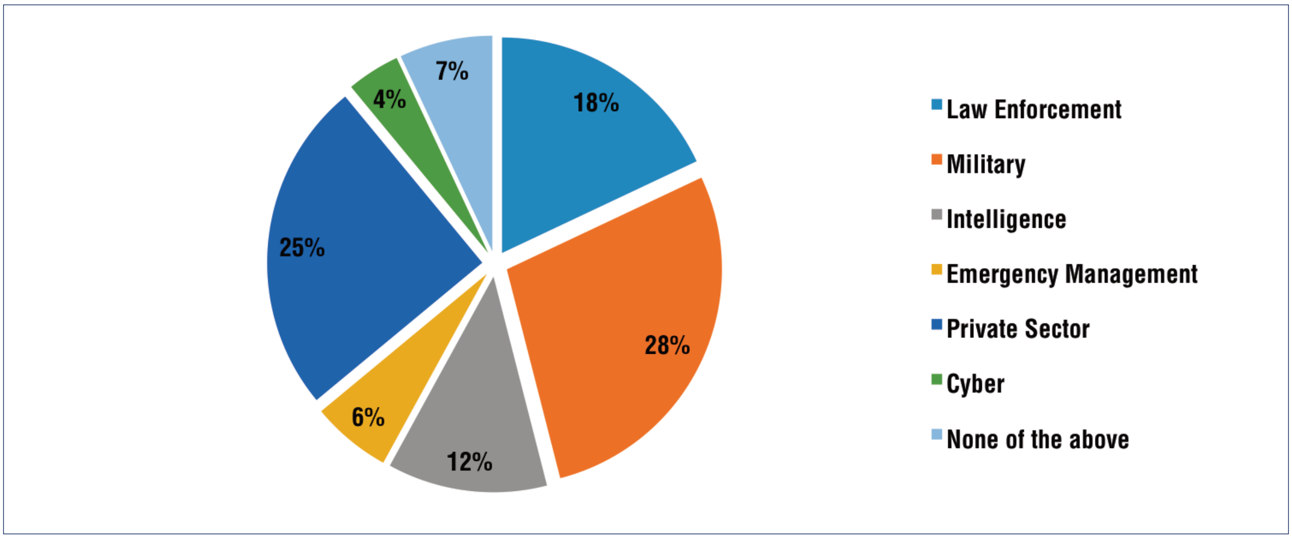
The need to adequately manage such a broad spectrum of topics is reflected by the composition of the security team. According to our data, the majority of companies have a team of 10 or more persons involved in security, even though there is still an important quota of companies who employ a small security team (less than 5).

People currently comprised in the responders' security component (excluding outsourced resources).

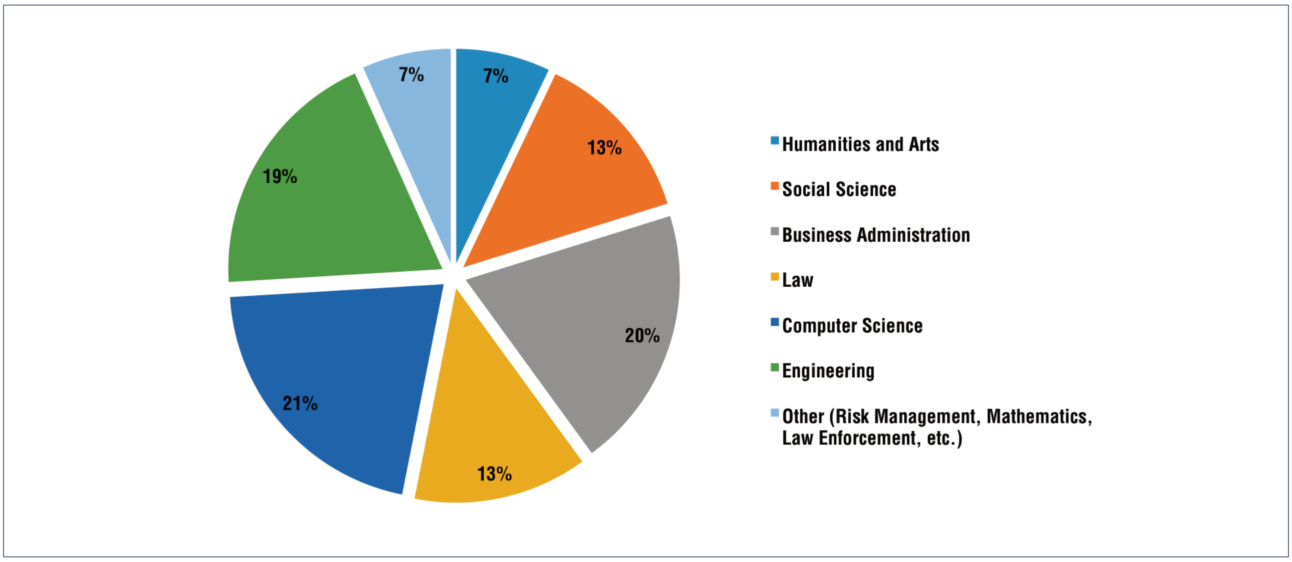


This aspect is more evident when we analyze the background of the people involved in security. Indeed, even if 46% of the CSOs have a background in the law enforcement or military fields, the actual composition of a security team is more articulated with a prevalence of competence in Computer Science, Business Administration and Engineering. This stresses the imposed complexity from complementing the education with managerial and process-based competencies.

Background of Chief Security Officers.

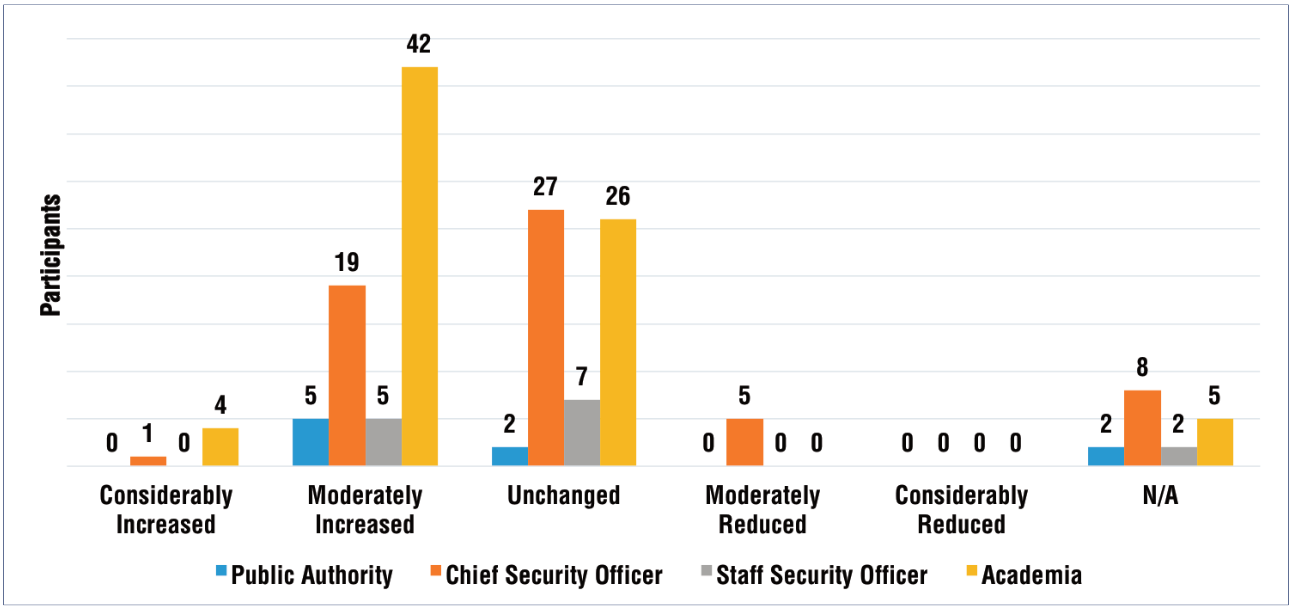


Background of Security Officer' staff members.



In this analysis, it is interesting to stress that, even if no female CSOs filled out the questionnaire, the data suggests the presence of female personnel inside the security division has moderately increased in the last five years. Such an increment is more evident from those outside the company structure (e.g. PA and Academia), perhaps because female personnel are mainly involved in front-end situations.

Female staff in security divisions.

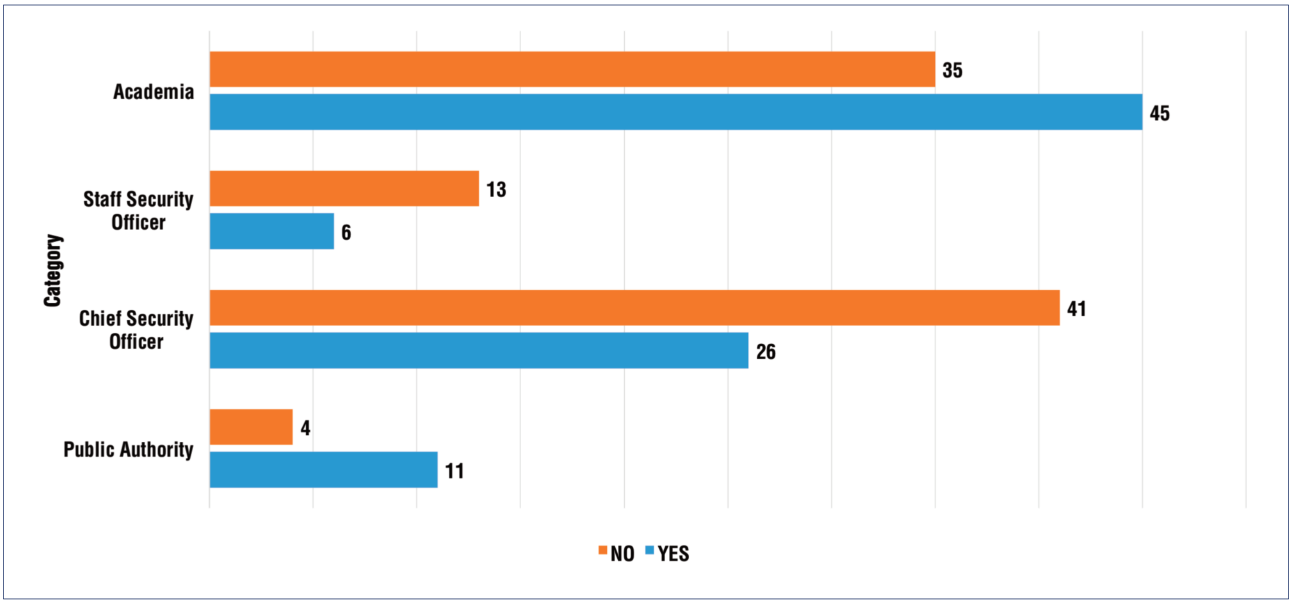


Going more in-depth on the aspects directly related with Council Directive 114/08/EC, one notices that there is only moderate familiarity with it (less than 50% of CSO's have knowledge of the EPCIP programme). Even more resounding is our analysis regarding the CIWIN network[1], which was evaluated

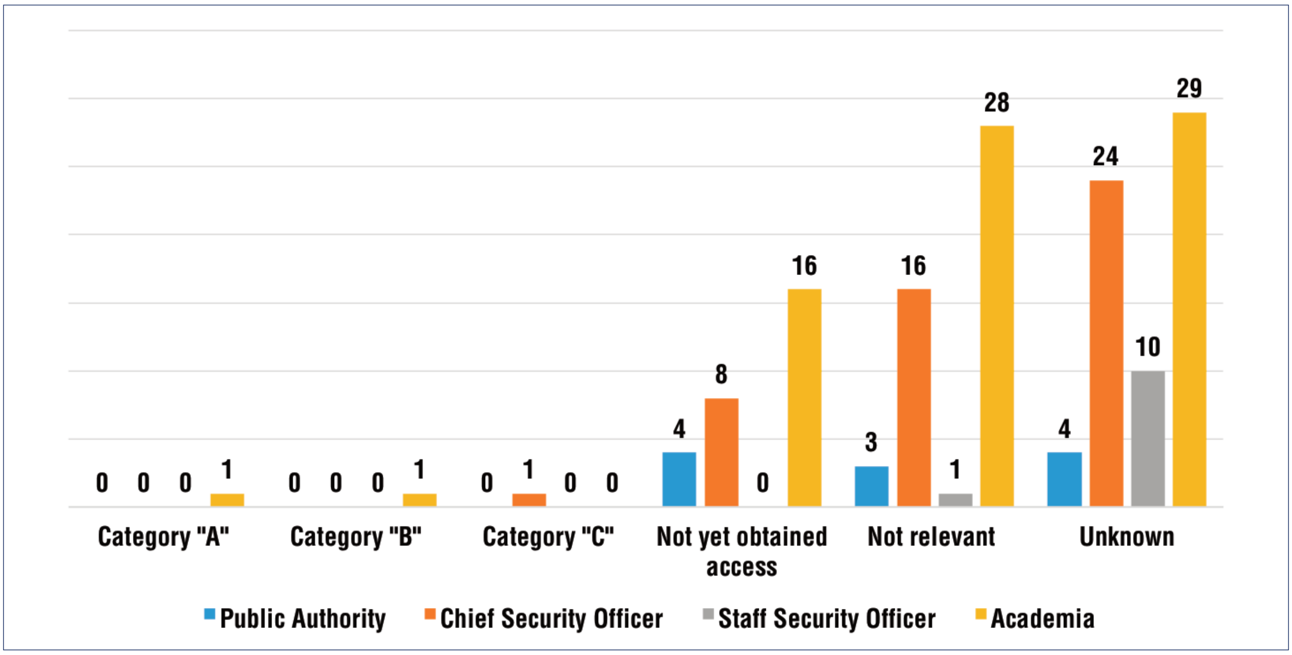
[1] CIWIN is a Critical Infrastructure Warning Information Network created by EU Commission SEC(2008)2701.

as "unknown", "not relevant" or simply unused by the majority of responders (the figure below reports the category of membership to CIWIN). This limited knowledge regarding the EPCIP programme represents a partial contradiction with respect to the conclusions of the EU Commission Working Document SWD(2013)318. This discrepancy can be partially explained taking into account that our questionnaires were mainly oriented toward private sector, while the primary customers for the EU Commission are the governments (notice that the PAs involved in the questionnaire have a discrete knowledge of the programme).

Familiarity with EPCIP framework.

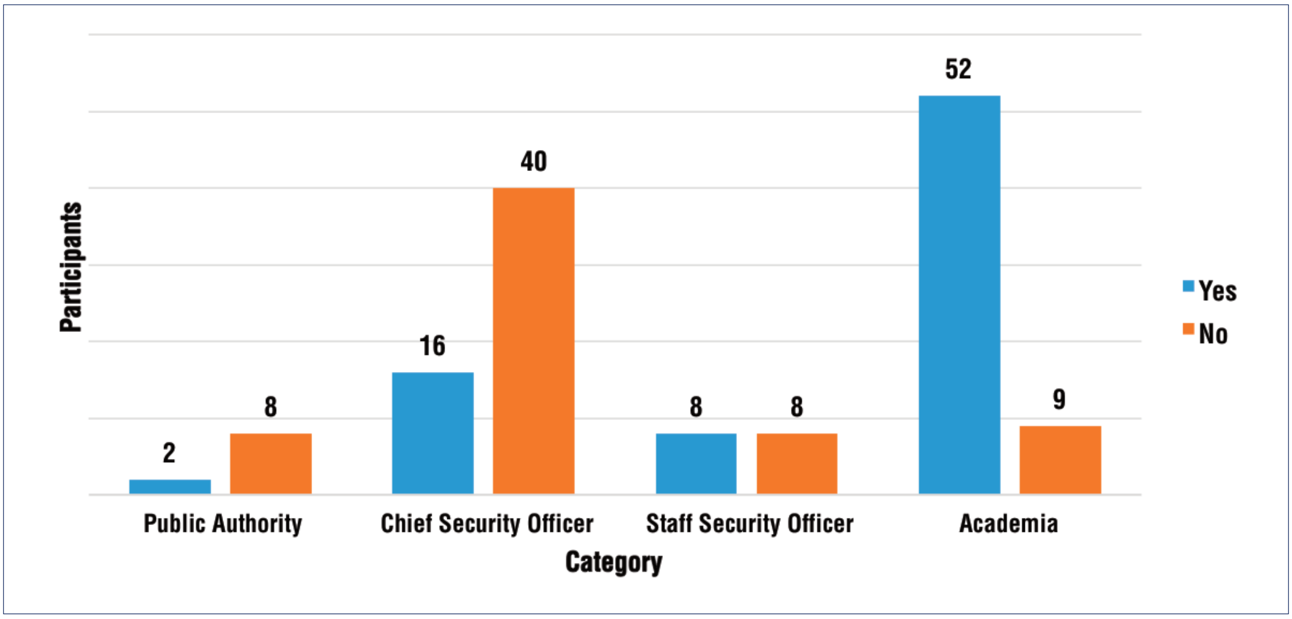


CIWIN Membership.



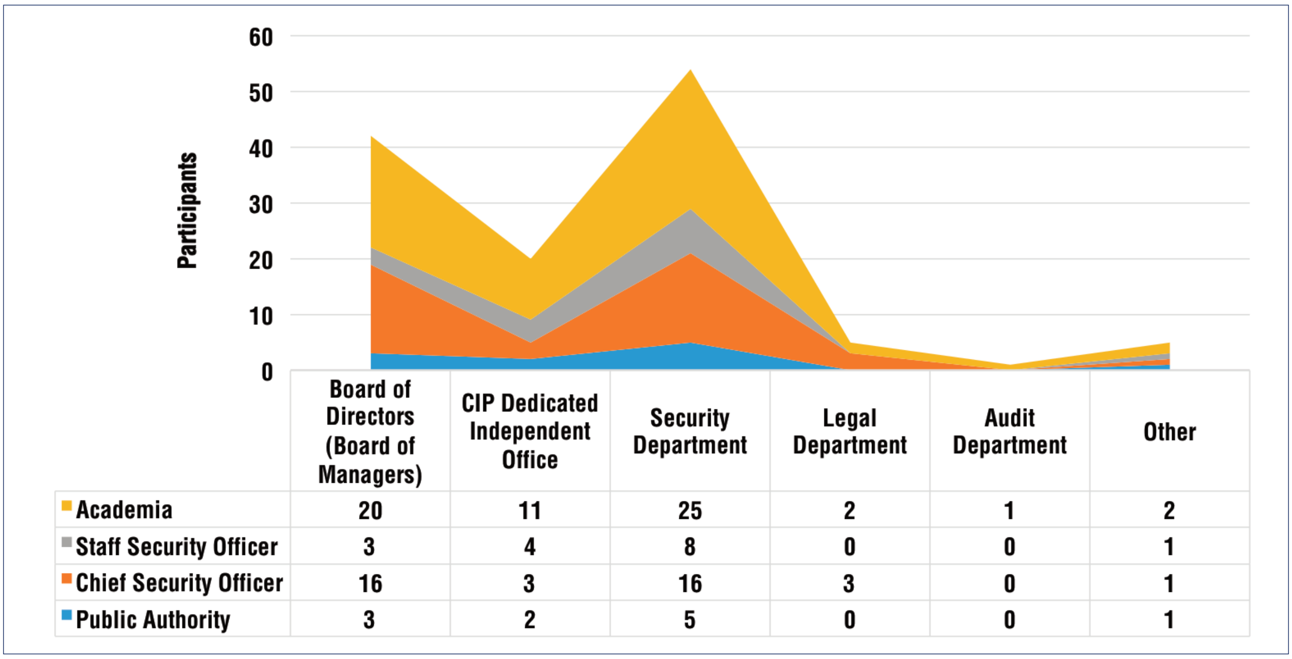
Consequently, a very few organizations have a dedicated CIP office. Notice that the Academia question was posed as "*should your organization have a dedicated CIP office*" hence it express a desiderata, while for the other categories it refers to an actual situation.

Organizations having a dedicated CIP office.



It's interesting that there is a general sentiment which doesn't think it's necessary to have a dedicated CIP department inside a CI company. The majority of the answers identified a good collocation of the SLO inside the Security Department or as member of the Board of Directors: it's noteworthy that for the CSO these two positions have quite the same appeal, while Academia prefers the SLO to fall under a more technical level.

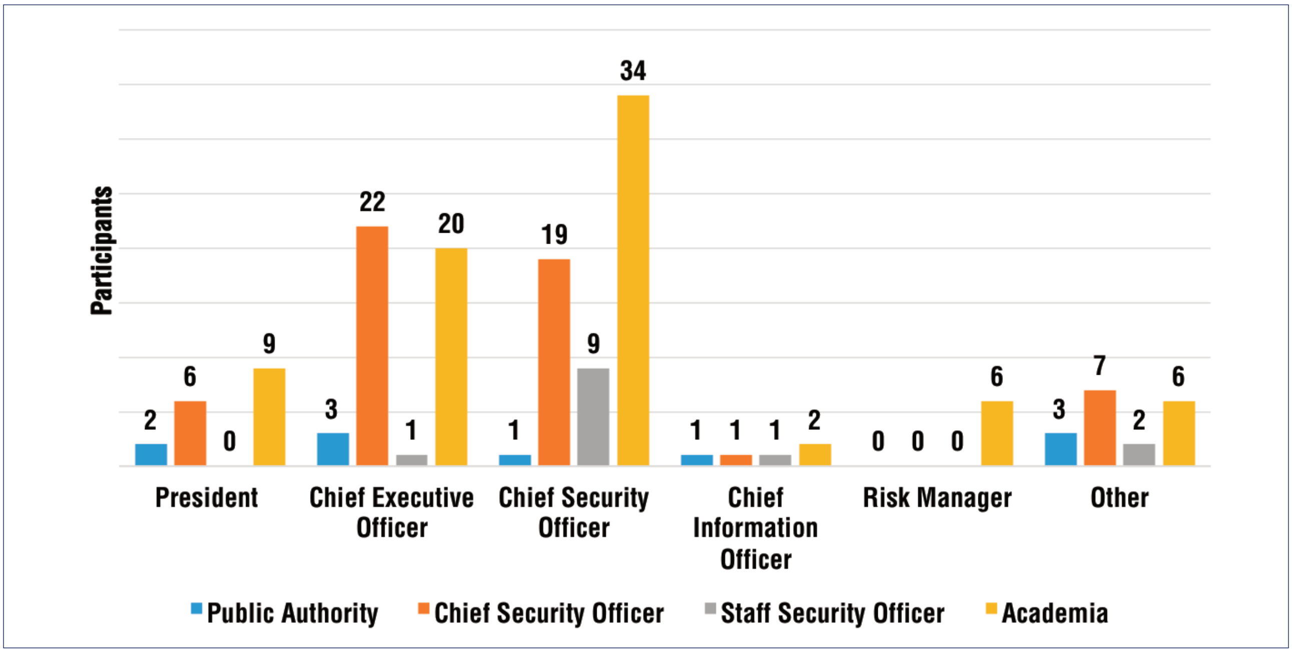
Who should SLO belong to?



	Board of Directors (Board of Managers)	CIP Dedicated Independent Office	Security Department	Legal Department	Audit Department	Other
🟨 Academia	20	11	25	2	1	2
⬜ Staff Security Officer	3	4	8	0	0	1
🟧 Chief Security Officer	16	3	16	3	0	1
🟦 Public Authority	3	2	5	0	0	1

Analogously, the large majority of respondents concurred that the SLO belong to a hierarchy where they report directly to the CEO or eventually to a CSO. This is in agreement with the results of our Workshop Cafés where participants overwhelmingly agreed that the SLO should have an executive level position or report directly to the CEO.

Who should SLO refer to?



WORKSHOP CAFÉS

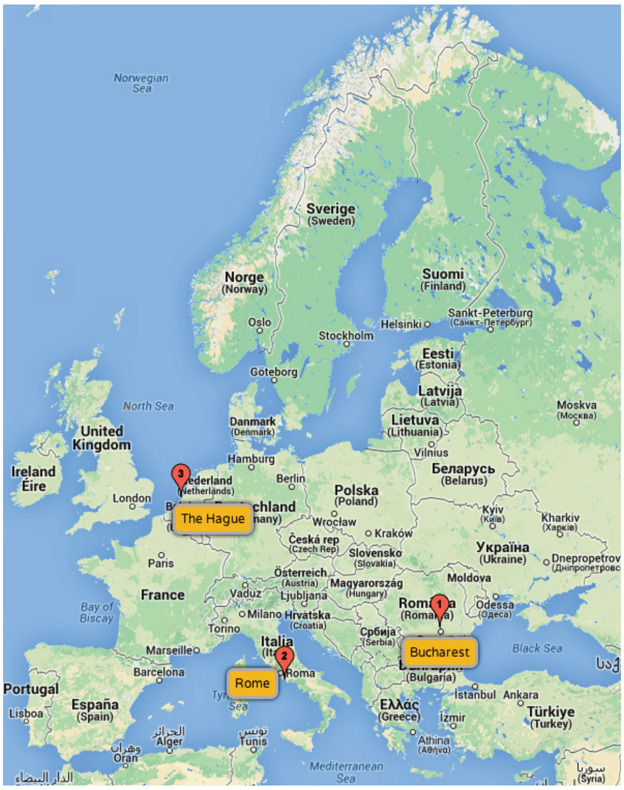
Within the SLO project, three Workshop Cafés (WSC) have been organized, with the aim to stimulate discussion among Security experts regarding what the SLO *should be* and which tasks he/she should perform in the European scenario.

Following the example of “Knowledge Cafés”, the Workshop Cafés were designed to elicit information and opinions from security experts, dividing the attendees into small groups and stimulating the discussion via open questions.

The WSCs were held in three different European Countries, in order to collect different opinions which reflect Member States’ regulations and cultural business schemes.

The SLO should have visibility on ALL security aspects.

SLO Workshop Cafés.



During each WSC, after a short introduction session, the attendees were divided into smaller groups, each one supervised by a facilitator who helped to raise the discussion regarding the questions emerged during the introduction; the conversations lasted for about an hour. Afterwards the groups met again for the plenary session, in order to match the collected ideas and express subsequent conclusions.

The WSCs focused on three separate elements of the SLO profile: Skills, Role and Tasks. These elements were analyzed and resulted in numerous innovative ideas and future elements for considerations. These results have been achieved thanks to the participation in the WSCs of about 100 security experts from Academia, Public Authorities and Critical Infrastructure Companies from different countries.

In particular, besides the citizenship diversity, a common opinion among the participants was that it is fundamental to initially focus on the SLO tasks in order to define his/her professional figure. A great effort regarding this subject came from the WSC in Bucharest, the unique European country where legislative act defines the specific duties of the Security Liaison Officer.

In this section, a summary of the results and common ideas characterizing the WSC activities is presented. First of all, according to most of the WSC attendees, the SLO must have the function of connecting not only structures (main reason of the “liaison” denomination), but also tasks and persons, playing a fundamental role to integrate the company activities and coordinate the personnel. The tasks attributed to the SLO figure are mainly carried out at a strategic level, thus the SLO is not appointed for an operational position. One of the most cogent opinions among the WSC attendees was that it is essential for the Security Liaison Officer to be aware and familiar with all the potential threats that are impacting the organization and to suggest solutions to the board who is entitled to the final decision. He/she must be able to communicate to all directions within the company and to connect all the divisions/departments of the company. Additionally, the SLO must also be in contact with the Security Liaison Officers of other CIs, authorities and law enforcement officers. The SLOs must monitor events within their CI (with the intent to prevent incidents or crisis). Their main role must be, therefore, a link between the organization and both the National and European Public Authorities and other Critical Infrastructures.

The SLO must have a very good knowledge of the company.

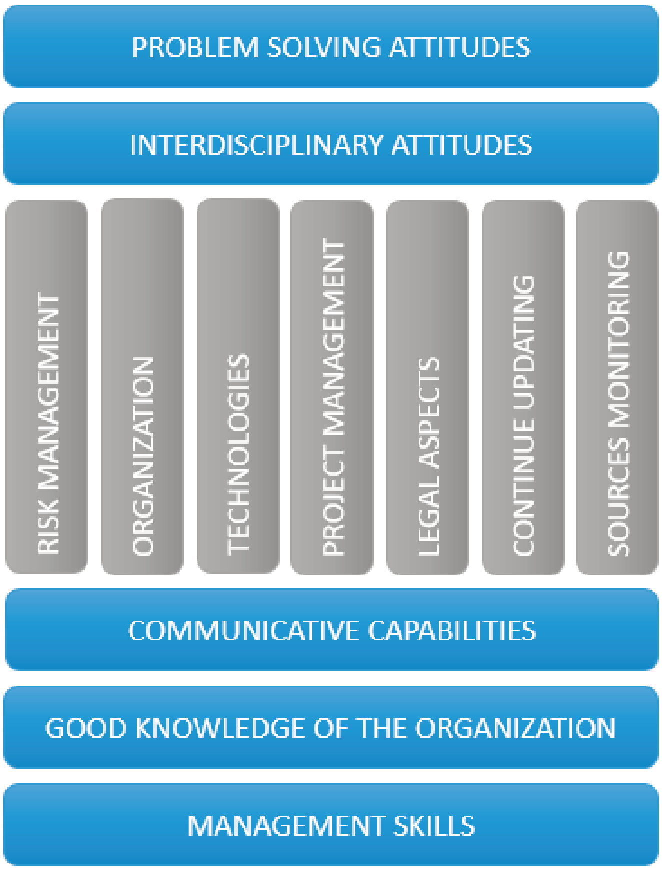
To achieve these tasks, the SLO must be a person with good communication skills, able to motivate people, and in particular must have a strong commitment from the top management. In this perspective, being primarily a coordinator/facilitator able to effectively communicate inside and outside the organization, the SLO needs to be at a top management level into the organization, referring preferably to the company board of directors. The SLO should in fact have experience in management, though not necessarily former experience in the law-enforcement or military field. However, the SLO should have a wide competence on his/her own organization and its sector, along with knowledge regarding other sectors, technologies and legislations in security matters, and a mandatory continuing training process should be aligned with context changes. SLO should have a strategic view to make sure that the company can face critical situations, prepare plans also taking advantage of external consultancy. However, the SLO should have strong autonomy with a bottom-up and top-down information sharing system. Social skills in addition to technical skills for the implementation of the security management plan are required. The SLO must have a security clearance and it is preferable the possession of some professional certificate or adequate academic degree. During the WSCs, also novel vulnerabilities stemming from the implementation of dramatically differing policies, particularly difficult for companies operating in many Member States, were analyzed.

**First Workshop Café,
11th October 2013
in Bucharest (Romania).**

**Second Workshop Café,
25th February 2014
in Rome (Italy).**

**Third Workshop Café,
21st May 2014
in The Hague (The Netherlands).**

Appropriate skills that should characterize the SLO gathered from the opinions shared during the three WSCs.



Though the WSCs activities resulted in very similar opinions among the attendees, they did not necessarily agree regarding the background and the position with respect to the organization of the SLO. In particular, these aspects were influenced by the current designation of the SLO in the origin country of the attendees. Whereas the SLO should be internal to the organization for most attendees, some participants did not exclude the possibility to designate an external officer with a broader range of experience and skills. Similarly, some of the attendees believe that the requirement of a SLO figure must be stated by the authorities, and in this framework selected by the organization, while other opinions deal with the complete autonomy of the organization to choose a SLO. However, all the participants regarding the need for an international standardization of the SLO professional profile.

INTERVIEWS

In addition to the questionnaires and the WSCs, the survey regarding the professional figure of the SLO has been conducted via interviews to different experts involved in CIP including Security Managers and Public Authorities. In particular, the interviews were aimed at identifying the elements which discriminate the Security Liaison Officer tasks from those of the Security Manager or Chief Security Officer, since the two positions are often assimilated in the field of Infrastructure Protection and the Council Directive does not clearly define potential differences between these roles.

The lack of regulatory references regarding the function and the characteristics of the SLO has led to the development of different dispositions in each Member State. It is common opinion that there exists a strong motivation to establish a standard profile of the SLO figure, and to introduce a more cogent and specific regulation on the subject to allow a more efficient cooperation of Security Liaison Officers of European Critical Infrastructures.

Although some discrepancies came up in the collected opinions while defining the personal point of view on the ideal SLO characteristics and position in the related Infrastructure or Institution, our work identified several analogies among the responses of the interviewees.

ROLE AND POSITION OF THE SECURITY LIAISON OFFICER

As stated in the Article 6 of the Council Directive 2008/114/EC, the Security Liaison Officer is the contact point between the organization owner of a Critical Infrastructure and the Public Authorities. As a consequence, the SLO must have a strategic view in order to guarantee the continuous protection of the Infrastructure; hence his/her main role is in the preparedness and prevention phase, and not during a critical situation. Therefore the SLO should not be involved in the Crisis Management activities, for which the company usually has a specific organization appointed, but he must only support them as a liaison officer.

> SLO must have a strategic view in order to guarantee the continuous protection of the infrastructure, hence his/her main role is in the preparedness and prevention phase, and not during an emergency.

Concurrently, the SLO should have a connection with all the departments of the organization, aimed at being in contact with the operational activities and with the senior management board as well. In particular, the SLO should be in a high-level position, for example a board representative or the CSO himself. A staff could support the SLO and he/she should report to a senior executive, with the authority to approve the security organization decisions and the potential suggestions regarding security policies.

For the designation of a Security Liaison Officer, most of the interviewees have expressed the opinion to appoint a person already in the organization context having a deep knowledge of the corporate processes and activities, vulnerabilities and potential threats which could impact the infrastructure. Another element of unanimous opinion was the access to classified information. The SLO should be a liable person, with a specific level of confidentiality, eligible for a security clearance according to the instruction of the MS. Therefore, though the organization should decide the person to designate as SLO, the Public Authorities participate in this process releasing guidelines for officers' eligibility and accrediting the subjects considered suitable. Though the appointment of the SLO should be achieved inside the organization, in case of specific or international complex situations (which could require a technical expertise), an external consultancy could be considered, or even the designation as SLO of a qualified professional not belonging to the organization is a possibility.

TASKS AND RESPONSIBILITIES OF THE SLO

Being involved in the preparedness phase, the main function of the Security Liaison Officer is to arrange prevention plans for the protection of the Infrastructure in case of critical situations, to be presented to the Public Authority, after the approval of the senior management board. The SLO position inside the organization allows to coordinate all the corporate departments, and he/she can also suggest solutions to the board. He should be able to motivate his/her staff in order to guarantee better cooperation in maintaining the best possible level of preparedness. Finally, if a critical situation occurs, the SLO should support the activity of the Crisis Management Unit.

Considering the SLO activities outside the organization, this figure is of utmost importance in the field of European Critical Infrastructure protection. “European Critical Infrastructures” are those who can affect two or more countries if subject to damage or disruption. The SLO of a ECI must be in contact with the SLOs of the other Infrastructures who could be involved in a potential critical situation. In order to allow this connection, it is necessary for all the involved SLOs to have similar roles, responsibilities and skills. This is one of the most important reasons why it is fundamental to define a common framework for the SLO profile.

SKILLS AND BACKGROUND OF THE SLO

So far, most of the SLOs come from the law enforcement field; thus they were former military, intelligence or law enforcement officers. However, because there is not a specific requirement for the background, the landscape is changing. For example, some SLOs have a law degree, and there is currently a much greater emphasis on a required academic background.

> Even if most of SLOs come from the law enforcement, currently an academic background is more and more required.

The deep knowledge of the organization structure and processes is an obvious requirement to perform the SLO activities. Since he/she is appointed to grant security preparedness, the SLO should possess expertise or studies in the field of security and risk management, with a multidisciplinary knowledge, in order to communicate in all directions within the organization and with PA. At the same time, the SLOT must be in contact with specialists who could provide specific support when required. For some interviewees, the SLO should be able to develop intelligence strategies and also be a Certified Protection Professional (CPP) holder, for the security clearance issue.

Regarding soft skills: in order to perform a liaison position it is necessary to possess excellent communication and organizational skills to manage and coordinate the connections inside and outside the organization for a correct implementation of the preparedness plans. In regards to this aspect, several years of experience in relationships with PA would be an advantage. In addition, the connection with the organization departments would require an excellent ability to motivate people, thus social skills are also appropriate to perform the activities of the SLO.

CONCLUSIONS AND RECOMMENDATIONS

Six years after its release, Council Directive 2008/114/EC has only partially achieved its goals. It has certainly contributed to increase awareness about the intrinsic fragility of the complex system of systems and the need to identify innovative solutions and strategies capable of guaranteeing effective continuity for All-Hazard approaches embracing the huge number of actual threats. However, as emphasized also by the Working Document of the European Commission, the current perception among the majority of stakeholders is that concrete improvement in European CIP as a result of the Council Directive 2008/114/EC has been minimal, if at all, (even in the few cases where Member States felt that European CIP has improved, there was not sufficient evidence for making this case to their peers)[1]. Moreover, on the basis of our data, there is a limited familiarity for the security experts regarding the EPCIP programme and its instruments.

This can be explained by several reasons, starting from the complexity of the designation process, which is largely based on sector-oriented criteria. Additionally, there exists a poor understanding of the effective obligations (and of the possible benefits) for the CI operators which, consequently, have generally adopted a very conservative position.

This lack of clearness is particularly evident for the figure of the Security Liaison Officer whose designation is mandatory for any ECI. The Directive does not provide any element to characterize such a professional figure. The absence of any requirement has facilitated an insecure situation where each Member State, or even each CI, has adopted autonomous criteria; and this non-homogeneous situation represents a dangerous barrier for effective information sharing.

To overcome such a drawback the European Commission co-funded in the “Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risk Programme” of the Directorate-General Home Affairs the SLO project, which aims to better characterize roles, competences and background of this professional figure. To this end, the project team analyzed the literature to characterize the context and to acquire elements to compare the SLO with other professional figures active in the security, military and crisis management fields. Moreover, the project extensively elicited information from more than 350 public and private security field experts via questionnaires, workshop cafés and interviews.

The results of this study have been summarized in this report, while the full details will be included in the project deliverables.

The first evidence coming from our data is that the SLO figure is considered, from both CI operators and PA, an effective element to manage the complex relationships existing between CI and PA, where the SLO could allow them to use a common vocabulary, simplify the procedures and construct more cooperative strategies and solutions.

This is also due to considerable changes in the managing of Critical Infrastructures over the last ten years. The scope of the “security” was once limited to the protection of companies’ people and assets against malicious activities. Nowadays, the security mission embraces further aspects, including service continuity, company reputation, management of crisis situations, etc. This is because organizations today must operate in a global market characterized by the presence of a large number of interdependencies, fast dynamics, “new” types of threats and compelling requirements from the end-users. Our data shows that in response to such solicitations, the security budget for the next five years, even in the presence of generalized budgetary constraints, will be aligned with those experienced in the

[1] Study to support the preparation of the review of the council directive 2008/114/EC on the “identification and designation of European critical infrastructures (ECI) and the assessment of the need to improve their protection” contracting authority: European Commission; prepared by: Booz & Company GmbH - 05 March 2012

past and continue to increase. According to the data, more than 52% of the CSOs foresee an annual security budget greater than 5 M€ for the next five years, which will be allocated quite uniformly on all the different aspects of the security domain, i.e. physical, logical, ICT and personnel security. This imposes to have a multi-disciplinary security team whose numerical dimension has also continued to increase in the last years.

Consequently our data illustrates the existence of a strong motivation to establish a standard profile of the SLO figure, and to introduce a more cogent and specific regulation on the subject. This is especially applicable in the presence of ECIs and for all those situations where different countries are involved.

From the mass of data collected during the project, it emerged that the term which appeared least applicable for the figure of the Security Liaison Officer, is the word “OFFICER” in the title. During the project several experts expressed some reservations about the term because it could apply a “military-oriented” connotation that might induce a wrong bias with respect to his/her essential role. Indeed the SLO is primarily a “LIAISON”, to serve as an interface between the CI company and the PA or other operators. Therefore, his/her main role should be a link between the organization and both National/European PA and other CIs.

His/her activities should be focalized in the preparedness and prevention phase, and not during a critical situation, for which the organization usually has a specific structure appointed. To effectively perform his/her work, the SLO should be familiar with all the threats that are impacting the organization. Hence it is a largely shared opinion to appoint a person already within the organization having, then, a deep knowledge of the corporate processes and activities.

The SLO should have a strategic view in order to guarantee the continuous protection of the Infrastructure, with experience in management, but not necessarily former experience in law-enforcement or the military field. However, a mandatory continuing training process and an adequate academic background is more and more required.

It is interesting that there is a general sentiment which does not think it is necessary to have a dedicated CIP department inside a CI company. The majority of the answers identified a good collocation of the SLO inside the Security Department or as member of the Board of Directors: it is noteworthy that Academia prefers the SLO to fall under the more technical position of CSO.

There is an important debate regarding the opportunity for the existing CSOs to also serve as the SLO. This is because there are overlapping knowledge/skillsets between these two professional profiles. However, our data emphasized that it should be preferable to have two separate professional figures.

It is important to stress that to operate effectively, also the Public Authorities should also introduce a figure similar to the SLO in order to facilitate the exchange of information.

A final consideration is on the word “SECURITY” in the name of the SLO label. From the project, the need emerges to mandatorily consider All-Hazard approaches to guarantee the capability of the different infrastructures to supply their essential services to the citizens. With this vision in mind, it appears more suitable to use the meaning of the Italian term “SICUREZZA”, which embraces a holistic vision of both the accidental and malicious threats, hence stressing the opportunity to adopt Safety & Security approaches.

Analyzing the current EU legislative framework, it seems mandatory to supplement Council Directive 114/08 with voluntary measures to inter alia address the shortcomings of the current legal framework. All stakeholders, due to their flexibility and adaptability to special circumstances and sectorial specificities, see these enhanced voluntary measures in a positive light. However, it is highly desirable for the SLO figure to have a unified framework facilitating the definition of his/her role inside the organization, for that which concerns his/her relationships with PA and other CIs, and to facilitate information sharing. In this way, the PA can participate in the process of designating a SLO inside CIs releasing guidelines and criteria for eligibility.

PROJECT PARTNERS

University Campus Bio-Medico of Rome
Complex Systems and Security Lab (Coordinator)

The University Campus Bio-Medico of Rome (UCBM) is the first thematic Italian University centered on the Person. It includes two faculties (Medicine and Engineering), a University Hospital and one macro-department (the CIR - Center of Integrated Research). The Complex Systems & Security Lab (COSERITY LAB) operates within the CIR and is one of the leading Italian research institutions in the field of Critical Infrastructure Protection.

The research activities of COSERITY LAB are focused on the development of innovative and strongly multi-disciplinary methodologies, tools and technologies to support the study of large infrastructures in terms of their behaviors, threats, vulnerabilities and management aspects. Based on the experience acquired over more than ten years, the University Campus Bio-Medico of Rome activated in 2009 a Master in Homeland Security, which aims at crafting cutting-edge experts in the field of Critical Infrastructure Protection. This master program is arranged in strong cooperation with several Italian law enforcement agencies and with the support of the major Italian players in the field of security.

http://www.unicampus.it/

http://www.coseritylab.it/

Romanian Association for Critical Infrastructure Protection – ARPIC

The aim of the Romanian Association for the Protection of Critical Infrastructures and Related Services – ARPIC, is to bring together specialists from different fields, so as to contribute to the understanding and harmonization of specific norms and operating procedures for the protection of Critical Infrastructures and related services, in Romania, as well as at the regional, European and international levels.

The Association acts to promote national and international synergies among scientists, experts and practitioners in the field of Critical Infrastructure Protection.

Through the competence of its founding members (active, honorary and associate), the Association aims to work with educational institutions, state designated authorities, NGOs, professional associations, critical infrastructure operators in the country or abroad, to carry out joint projects, including participation in scientific activities and international cooperation programs.

http://www.arpic.org/

ASSOCIATE PARTNERS

Italian Association of Critical Infrastructure Experts – AIIC

AIIC is a non-for-profit association founded in 2006 to exchange expertise and knowledge in order to the develop awareness, strategies, methodologies and technologies able to adequately manage Critical Infrastructures, especially in crisis scenarios resulting from both natural catastrophes or intentional malicious behaviors.

AIIC involves academics, professionals, researchers, and experts from different Critical Infrastructures, governmental and independent organizations, universities, public and private companies. Such a multitude of perspectives allows a deep, global vision of the problem and enables the Association to support public institutions and private enterprises to deal with this complex “system of systems”. One of the main objectives of AIIC is the dissemination of knowledge among their members by means of specific events (i.e., Workshops, conferences, etc.) covering different aspects of CI(I)P.

http://www.infrastrutturecritiche.it

ASIS International – Italy Chapter

ASIS International is the preeminent organization for security professionals, with more than 38,000 members worldwide.

Founded in 1955, ASIS International is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests, such as the ASIS Annual Seminar and Exhibits, as well as specific security topics. ASIS International also advocates the role and value of the security management profession to business, the media, government entities, and the public.

By providing members and the security community with access to a full range of programs and services, and by publishing the industry's No. 1 magazine – Security Management – ASIS International leads the way for advanced and improved security performance.

http://www.asisitaly.org/

BC Manager – The Italian Association of Continuity Managers

The association BCManager is aimed at promoting the knowledge of the discipline of Business Continuity Management and related disciplines (e.g. Crisis Management, Risk Management, etc.) through initiatives, activities and services aimed at the growth and cultural development of associates.

BCManager aims at becoming a privileged interlocutor of the economic world by establishing relations with its most representative realities, such as trade associations, chambers of commerce, public authorities, and supervisory bodies. It is aimed at increasing the knowledge of the characteristics and purpose of the Business Continuity Management within institutions, media, companies and academia through cultural exchanges, visits, joint events, in-depth meetings, conferences, round tables, and trainings intended to update members and affiliates.

Eventually, BCManager collects and prepares a mish-mash of principles, rules, standards, national and international literature as well as the establishment of a center of documentation relating to the discipline of Business Continuity Management.

http://www.bcmanager.it/

Transelectrica

Transelectrica is the Romanian Transmission and System Operator (TSO), which plays a key role in the Romanian electricity market. The company manages and operates the electricity transmission system and provides the electricity exchanges between the central and eastern European countries as an ENTSO-E member (European Network of Transmission and System Operators for Electricity).

Transelectrica ensures the Romanian Power System (RPS) maintains reliable and stable operation at quality standards, while providing the national electricity transmission network under transparent, non-discriminatory and fair conditions to all market participants.

The vision of the Company is to become the technical and operational authority of the RPS and the key transmission and system operator in South-East Europe, while operating interconnected to ENTSO-E and providing electricity wheeling to the regional electricity market.

https://www.transelectrica.ro

KEY PEOPLE

SLO PROJECT TEAM

Prof. Roberto Setola, project coordinator
Università Campus Bio-Medico di Roma - Complex Systems and Security Lab

Dr. Alessandro Lega
Corporate Security Advisor

Eng. Maria Carla De Maggio
Università Campus Bio-Medico di Roma - Complex Systems and Security Lab

Dr. Gregory N. Fink
Università Campus Bio-Medico di Roma - Complex Systems and Security Lab

Eng. Marzia Mastrapasqua
Università Campus Bio-Medico di Roma - Complex Systems and Security Lab

Eng. Stelian Arion
Romanian Association for Critical Infrastructures and Services Protection

Eng. Septimiu Caceu
Romanian Association for Critical Infrastructures and Services Protection

SLO ADVISORY BOARD

Dr. Laura Barettini, *Heidrick & Struggles (Italy)*

Dr. Sandro Bologna, *AIIC (Italy)*

Dr. Genséric Cantournet, *ASIS Italy Chapter*

Dr. Andrea Chittaro, *SNAM (Italy)*

Dr. Francesco Di Maio, *ENAV (Italy)*

Dr. Maria Giovannone, *ANMIL (Italy)*

Dr. Francesco Lambiase, *BCManager (Italy)*

Dr. Umberto Saccone, *Eni (Italy)*

Eng. Fabrizio Sechi, *Fastweb (Italy)*

Dr. Marko Sukilovic, *ASIS International*

Eng. Adrian Vâlciu, *Transelectrica (Romania)*

ACKNOWLEDGEMENTS AND SPECIAL THANKS

The SLO project team would like to thank all the people contributing in different ways to the success of the project.

Special thanks to Adrian Alexandru Badea for his support in the arrangement of the first Workshop Café in Bucharest, and to Erik de Vries, Jan Verkaar and Coen van Gulijk for their support to the arrangement of the third Workshop Café in The Hague. Moreover, the useful inputs and suggestions from Genséric Cantournet, Francesco Di Maio, Laurent Ducamin, Antonino Franza, Jean-François Morel, Paolo Puri and Umberto Saccone, have been crucial towards the success of the project.

Contacts
Prof. Roberto Setola
Complex Systems and Security Lab
Università Campus Bio-Medico di Roma
Website: http://www.coseritylab.it/
Email: contacts@coseritylab.it

SECURITY LIAISON OFFICER PROJECT

Project Coordinator: Prof. Roberto Setola
Complex Systems and Security Lab
Università Campus Bio-Medico di Roma

Agreement Number: HOME/2012/CIPS/AG/4000003747

COSERITY
LAB
COMPLEX SYSTEMS & SECURITY LABORATORY

http://www.coseritylab.it/

With the support of the “Prevention, Preparedness and Consequence
Management of Terrorism and other Security-related Risks Programme”
European Commission - Directorate-General Home Affairs