Eur J Secur Res (2019) 4:33–49
https://doi.org/10.1007/s41125-017-0028-2

ORIGINAL ARTICLE

How to Improve the Security Awareness in Complex Organizations

Maria Carla De Maggio[1] · Marzia Mastrapasqua[2] · Marco Tesei[3] · Andrea Chittaro[2] · Roberto Setola[1]

Received: 18 September 2017 / Accepted: 22 December 2017 / Published online: 2 January 2018

Abstract The increasing interest arising around the field of security becomes a pragmatic issue when we consider the behavior of the employees of large organizations involved in critical infrastructures. As a matter of common knowledge, the human factor is the weakest link in the security chain. This introduces the topic of the security awareness of employees in large organizations. In this paper, we describe the results of a survey designed and delivered to large organizations in Europe, to understand how the topic of security is perceived and implemented and which are the security awareness initiatives held by organizations to instruct their employees. Moreover, we evaluate 23 methods to increase the security awareness, on the basis of several indicators describing their effectiveness, cost, implementation time, and other relevant aspects, to emphasize their pros and cons and their areas of applicability. Finally, we describe a tool developed to support the design of a security awareness campaign respecting the constraints imposed by the needs of each organization.

Keywords Security awareness · Critical infrastructure protection · Human factor · Physical security

✉ Roberto Setola
r.setola@unicampus.it

[1] Complex Systems and Security Laboratory, University Campus Bio-Medico of Rome, Rome, Italy

[2] SNAM, Corporate Security, Milan, Italy

[3] NITEL (Italian University Consortium for Transport and Logistics), Rome, Italy

1 Introduction

In a current scenario in which the society benefits of services provided by strictly interdependent infrastructures, daily operations, in small-to-large organizations, are becoming simpler, implying an increasing complexity in systems, processes, and communication links.

System complexity also introduces new technological challenges to protect infrastructures.

Developed countries are hit by a large number of incidents; in most of the cases, the "human factor", plays a crucial and decisive role in both positive and negative evolving events, like managing a crisis in a prompt and flexible way (solving it by minimizing damages) or lacking in communication and proper procedure implementation (causing further harms). Furthermore, the human factor is fundamental if we consider the insider threats (Hills and Anjali 2017); this issue emphasizes the importance of the "security culture" (Weinberg et al. 2014), particularly when we deal with prevention (Greitzer et al. 2013) and to facilitate the organization to promptly identify potential insider threats.

Taking care of the human factor is fundamental to increase the security level and to avoid big failures. Indeed, as emphasized by the high-reliability theory (Perrow 2011) concerning no-malicious accidents, i.e., safety, human factor can be the weakest and/or the strongest component of a system. In the security framework, this rule is emphasized due to the rational capabilities of the attackers that can operate to exploit any possible vulnerability, including human-related ones (e.g., via the so-called social engineering techniques (Workman 2007; Krombholz et al. 2015).

This is why we deal with the concept of "security awareness" with the aim to allow the organization personnel to be pro-active in the development and implementation of the security. In line with the all-hazard philosophy (Bullock et al. 2011) that has been recognized of utmost importance for the protection of critical infrastructures, in particular after big crisis involving critical infrastructures (Council 2004), (Liscouski and Elliot 2004), awareness should be addressed to all the safety and security issues in both physical and cyber domain. Now, while the relevance of the human factor in safety has been largely investigated in the literature [see, for example, (Cacciabue 2004; Dekker 2004)], less attention has been paid to the security issues related to physical security.

The concept of "awareness" has its roots in the behavioral theory, and it is strictly connected to the ideas of *motivation* and *attitude* (Siponen 2000). Generally speaking, the term "awareness" refers to the state resulting from the acquisition of a given knowledge. The sense of this definition is included in the term "acquisition": empirical evidences show that people commonly keep on adopting unsafe behaviors despite their knowledge of the risks. For example, it is well known that it is compulsory to drive with the seat belt fastened, but most people ignore this rule endangering their own safety. This example proves that knowing something is different from being conscious of something. Consciousness is connected to internal factors characterizing the individual, first of all his/her *attitude*, i.e., the expression of favor or disfavor toward a person, place, thing, or event (Allport 1935); in other

words, how the person considers that object of interest (Ryan and Deci 2000). Indeed, the attitude of a person is influenced by the consequences of the behaviors; it is the result of past and present experiences (Allport 1935; Siponen 2000).

Since people might represent the weakest link in the implementation of any security policy, it is paramount to strengthen that link before it gets broken (Pastor et al. 2010). Some studies explain how security initiatives should be arranged to influence the behavior of the employees (Swain and Guttmann 1983). However, while the safety awareness aspects are largely recognized, less attention is historically paid to security aspects, with the only recent exception of the cyber security. However, (Cobbina et al. 2013), (Manzo 2009) and (Kirschenbaum and Rapaport 2012) analyze the effectiveness of training applied to security officers, stressing that the recipient often considers the training not exhaustive. The first two papers are based on North American experiences, specifically on USA (Cobbina et al. 2013) and on Canada experience (Manzo 2009), where specific regulations exist for the definition of minimum requirements. Conversely, in Europe, there is a lack of standards in this topic (De Maggio et al. 2015). The third paper (Kirschenbaum and Rapaport 2012) conducts a sectorial study in airports, stressing how training can improve security decisions.

However, the security awareness is not merely dependent from "classical" training activities. A study (Fishbein and Ajzen 1975) asserts that human beliefs could be changed with active participation and persuasive communication. According to this statement, it is clear that these two elements should be the cornerstones of every organizational policy. "A culture exists when members of an organization share identity and mission" (Schein 2006). The principles of the organizational security culture should not be only embodied by a static document or classical training initiatives containing what people are allowed to do and what not to do, but should be a living and dynamic entity that reflects on their daily behaviors. The belief in the effectiveness of the security policy should start from the top senior executives who make decision regarding the measures to be adopted. The executives sometimes refuse to invest in security initiatives, since the advantage of such investment is not immediately visible. Nevertheless, the top figures of the organization should consider the benefits of improving the staff security awareness, because even a single error of an employee could seriously damage the organization business. The board endorsement is the first element that encourages the employees to follow the security practices.

To share the identity and the mission means that each member of the organization should follow the principles prescribed by the security culture. Thus, the policy should be addressed to all departments (security, human resources, regulatory compliance, legal, etc.), designing specific initiatives according to the functions of each sector. Of course, the bigger is the organization, the more difficult is to build a security culture, but if all the employees properly behave in terms of security, it is possible to avoid that they influence each other with incorrect and malicious actions.

Bad behaviors could be the result of an unclear language, or lack of knowledge, or negligence, if the policy is considered useless or too demanding to be performed (Al-Awadi 2009).

Some employees are aware of the rules, but they do not understand that leaving the worksite without locking their computer and leaving sensitive documents at

hand is like leaving the house in the morning without locking the door (Stackpole and Oksendahl 2010). Security is often underestimated until a serious breach happens (Huston 2001), and sometimes, it is a good reason not to repeat it again in the future. Last but not least, there are employees, as already said, who intentionally allow a security breach to damage the entire organization (Hills and Anjali 2017).

Active participation and persuasive communication generally are in the basic elements for an organizational policy to be recognized and to increase the employees' motivation, and this is also true for security. Regardless of the adopted solutions, the policy designers should introduce security as a part of the organization business, not as an appendage.

In this paper, security awareness is addressed with particular attention to physical security, even if a large part of the results described in the follows can be easily translated into all safety and security aspects. The objective of the study is to analyze and compare the most common methods adopted to increase the level of security awareness of employees inside complex organizations. This has been done by merging an extensive survey of open source documents with data elicited from interviews and an ad-hoc questionnaire whose most significant records are reported in Sects. 2 and 3.

Specifically, we analyzed 23 different methods to increase the security awareness within an organization (Setola et al. 2015). These methods, despite aiming at the same objective, largely differ from each other in terms of cost, time needed to design and deliver them, extension of the transmitted message, time horizon, etc. None of them can be considered as a silver bullet, since each organization interested in programming the security awareness initiative has different needs, goals, and starting points.

To better compare these methods, we introduced a set of metadata to capture their most relevant aspects allowing us to classify them with respect to a multitude of criteria. The software tool MEISA has been developed on the basis of such criteria; it is a decision support system tool able to support practitioners in identifying the instruments that have the better fitting with respect to a given context/goal.

In the following sections, we provide an analysis of data collected from the questionnaire on security issues delivered to European organizations (Sect. 2) and a comparison of methods to increase security awareness to build a customized security awareness campaign (Sect. 3). Section 4 illustrates how the MEISA tool can be used to support end-users to identify the most effective strategies to increase the security awareness. Finally, Sect. 5 collects some conclusive remarks.

2 Security Awareness Survey

To assess the actual concern about security issues of companies, in the period going from October 2014 to February 2015, a survey has been designed and delivered via an ad-hoc questionnaire.

The questionnaire has been conceived for organizations operating in critical sectors, which are supposed to have a particular attention for the security issues. Forty-nine questionnaires have been collected from different European Countries.

The study has been promoted by GIE—Gas Infrastructure Europe, an association representing the interest of the infrastructure industry in the natural gas business such as Transmission System Operators, Storage System Operators, and LNG Terminal Operators (www.gie.eu). Therefore, the questionnaire was first delivered to European gas infrastructure organizations belonging to GIE, who returned 24 questionnaires of the total number, and afterwards, other organizations, also operating in different sectors, were involved. Specifically, the 61% of the respondents works in the Oil & Gas industry, whereas the remaining 39% belongs to other sectors (mainly Telecommunications, Information Technology, Institutions). Regarding the dimensions of the respondent organizations, their budget were mostly under 100 M€ (22 respondents—45%) or between 101 and 500 M€ (13 respondents—27%); 20% of the respondents (10) work in organizations with income greater than 500 M. Concerning the organizations' dimension, 17 respondents (35%) worked in medium-size organizations with a number of employees between 201 and 1000. A smaller percentage of respondents belongs to small-size organizations; particularly, 21% (10 respondents) has less than 50 employees, and 18% (9 respondents) has between 51 and 200 employees. 24% of respondents (12) belongs to large organizations (10% with a number of employees between 1001 and 5000, and 14% with more than 5001 employees).

Most of the responders are security managers (51%), while the other were directors (19%), employees (12%), practitioners (6%), coordinators (8%), and researchers (4%). 38% of them works in the Security and Crisis Management department, 29% in the HSE (Health, Safety, Environment) department, and the remaining 33% in R&D and Human Resources departments.

The respondents were asked to provide their opinion on the concept of "security awareness" (Fig. 1). This stresses how security awareness is primarily a "cultural"

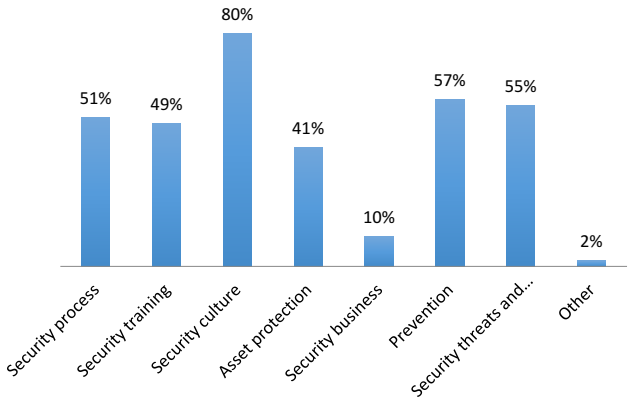

Fig. 1 Knowledge fields to which the term security awareness may refer to (46 answers; Multiple-choice questions)

issue for about three quarter of the respondents; however, it is more related to the "conscience" of a person rather than to the "knowledge", such as a habit that totally influence the people and their daily lifestyle inside and outside the work environment. All the other options collected largely less consensus: security process (51%), security training (49%), asset protection (41%), prevention (57%), security vulnerabilities, and threats (55%).

It should be stressed that only 10% of the respondents connect the concept of security awareness to the business. The poor level of security awareness seems depending on the senior management that rarely approaches this topic as a part of the business and as a consequence so do the employees. Hence, security awareness and more, in general, security activities are widely perceived as a pure cost rather than a cornerstone of the business. Organizations should highlight the relation between security and business to achieve a stronger commitment from both top management and employees to prevent incidents and negligent behaviors.

Respondents were asked if their organization had a program to increase security awareness and if yes, for how long it has been developing such procedures. 84% of the respondents states that their organization has been developing a security awareness program, 36% of which for more than 5 years. 30% affirms that their organization has been developing security programs for a period between 1 and 3 years, 17% between 3 and 5 years (Fig. 2). 16% of the respondents still do not have a security program in their organization.

33% of the respondents who confirmed the presence of a security awareness program within their organizations also declared that they have a specific budget invested in such procedures on a yearly basis.

The survey has shown that only half of the respondents declared that their organization has a specific staff somehow involved in the security awareness program. 84% of them have internal members employed in the security awareness issues, from a minimum of 1 person to a maximum of 10 people, whereas the remaining 16% of the respondents affirms that their organization outsourced this function from external entities/companies, investing an average budget of 10,000 € per year.

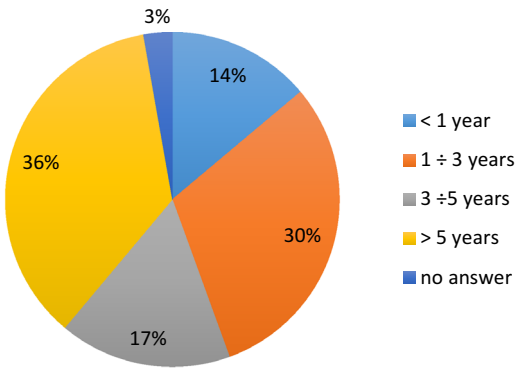

Fig. 2 If applicable, how recently organizations have developed security awareness programs (36 answers)

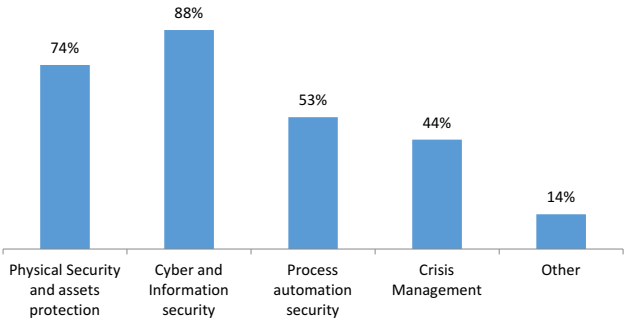

Fig. 3 Fields of application of the security awareness programs (42 answers)

Concerning the specific focus of the security awareness programs, the largest attention is paid on the cyber domain, a topic included in 88% of the security awareness programs, which is usually considered the most relevant and dangerous threat. The graph in Fig. 3 shows that almost 75% of the organizations that have a security awareness program also developed initiatives in the field of physical security. About half of the organizations performs security awareness programs for the industrial control systems (e.g., SCADA, PLC, etc.). Note that in the section "Other", the following fields have been indicated: business continuity, personal data, compliance, HSE, and disaster recovery program (1 respondent each). The attention for Crisis Management is unexpectedly quite limited (44%).

It is interesting to compare the above-mentioned results with the data collected on the topics managed by the security department (Fig. 4). This topic is well considered in the security awareness initiatives for almost all the organizations in which the physical security was managed by the security department.

According to 74% of the respondents, the security awareness program developed by their organization was addressed to all employees. 14% of the responders declared that only the employees working in the security departments and on critical process operations were involved in the security awareness initiatives. Finally, only 7% of the responders stated that the security awareness programs were planned for vendors and business partners. This limited attention to third parties can represent a serious weak point.

A large number of respondents (80%) report that in their organizations, there is a specific process for revising and updating security governance, security policies, and procedures. In particular, most of them affirmed that this process is performed by the management system, within the security function itself, or within the ISO 27001 certification process.

The respondents were asked to provide some suggestions for the development of a security awareness program. Although it was an open question, it has been noted that many respondents answered in a quite similar way (Fig. 5). 36% of the answers suggest to adopt a systematic approach by defining specific rules and strategies and by establishing the priorities. 13% of the respondents emphasize the importance of creating the security culture and a similar percentage of answers underlines the importance of the senior management support in building the security awareness

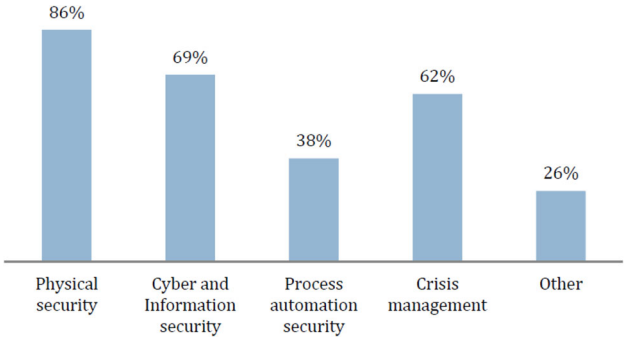

Fig. 4 Topics managed by the security department of the organizations, expressed in percentage (42 answers; multiple-choice questions)

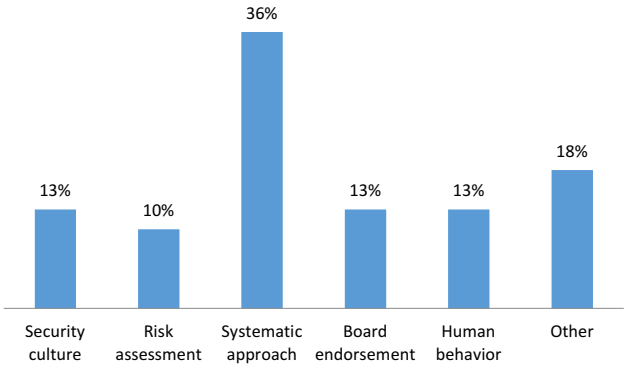

Fig. 5 Suggestions to start a security awareness program (39 answers)

program. 13% of the respondents suggest to explain the importance of the human factor, which is often the target of malicious actions aimed to cause security breaches (e.g., social engineering attacks). 10% of respondents affirm that the risk assessment is an element that should be included in a strong security awareness program.

3 Proposal for the Assessment of a Proper Security Analysis Campaign

The questionnaire was also devoted to collect data regarding methods and best practices actually used or experienced by recipients to increase the level of security awareness of their organizations. The data collected from questionnaires have been merged with data coming from literature analyses and specific interviews.

This survey has considered 23 different methods to increase security awareness. Each one of these methods has been outlined and summarized in a "datasheet" containing short descriptions, advantages and disadvantages, best practices, references, and examples (see Setola et al. 2015).

Table 1 Assessment indicators for methods to increase the security awareness

Indicator	Definition
Effectiveness	How much the initiative reaches the goal of increasing the security awareness
Design cheapness	The extent to which the method requires low-cost design processes, including all the activities from the definition of the idea until the delivery of the method (not included). The higher the value of the design cheapness, the less expensive the design of the method
Design time	The overall time needed for the design process, including all the activities from the definition of the idea until the delivery of the method (not included). The higher the value of the design time, the faster the process to design the method
Delivery cheapness	The extent to which the method requires low-cost processes to deliver the method to the target employees of the initiative. The higher the value of the delivery cheapness, the less expensive the delivery of the method
Delivery time	The overall time required for the delivery of the method to the target recipients
Completion time	The overall time needed for the single person to complete the actions required by the method to increase the security awareness. The higher the value of the completion time, the shorter the time to complete the task
Time Horizon	This indicator measures for how long the enhancing action of the considered method shows significant effects on the security awareness
Basic awareness	The basic level of security knowledge and awareness required for the recipient to be able to fully understand the content of the method
Message extension	The amount of information conveyed, i.e., transmitted through the considered method
Recipient dimension	The number of people that could be involved using the method
Type of recipient (qualitative)	The people to whom the security awareness initiative is addressed according to their position within or belonging to the organization. Some techniques are suitable for members of specific departments of the organization and they cannot be delivered to all employees, since they are focused on specific tasks or require a basic level of awareness
Field of application (qualitative)	Security sectors involved in the security awareness initiatives. Some of the initiatives could be suitable only for selected fields of the organization, among the ones listed
Popularity (qualitative)	How often the method is/has been adopted

Moreover, a quantitative assessment method has been used to assign synthetic "assessment indicators" used to compare the different methods. Specifically, 10 numerical indicators and 3 qualitative descriptors have been identified and listed in Table 1. For numerical indicators, we assume a scale from 1 to 5,[1] where 5 means that the method completely fulfills the criterion, while for qualitative indicators, the responder has to select among a set of five descriptive and ordered items.

For each method and with reference to each single indicator, the numerical values have been extracted from experts' answers using the AHP procedure described in (Saaty 1988).

[1] Responders are allowed to provide fractional points.

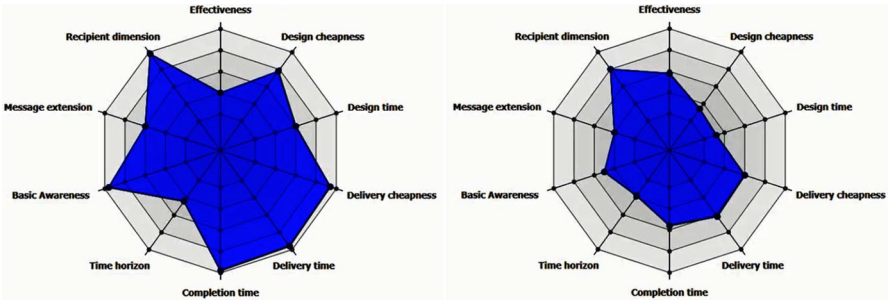

Fig. 6 Examples of radar plot of the methods (Brochure on the left, PC game on the right)

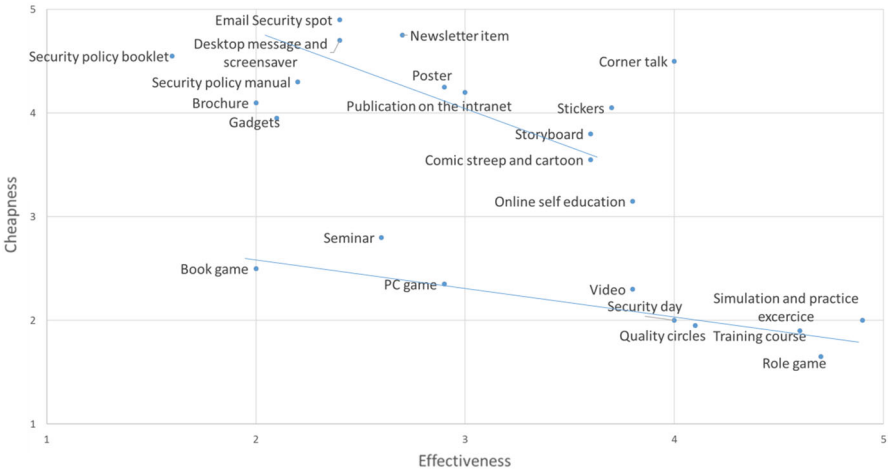

Fig. 7 Methods to increase the security awareness represented in their effectiveness and total cheapness

The values of the different indicators of each method have been represented in a radar plot that allows to understand which are the weaknesses and the strong points of each of them, in the perspective of being implemented. Two examples of radar plots are showed in Fig. 6. This type of representation facilitates the comparison between methods.

In Fig. 7, the collected methods are represented comparing their cheapness (including both design and delivery phases) with respect to their effectiveness. There are several methods which are quite no effective even if they are very cheap (top left corner), while the most effective methods (right side) are very expensive. It is clear that in this graph, the methods are positioned along two straight lines with a negative slope. This means that any increment in efficiency is paid by an augmentation in terms of cost of the method. In the graph, we can identify two classes of methods. The first class, along the top line, is composed of generally cheap methods, but their effectiveness is limited. The second group (arranged along the bottom line) is characterized by a more active involvement of the employees. These methods have a cost about one order of magnitude greater than those of the

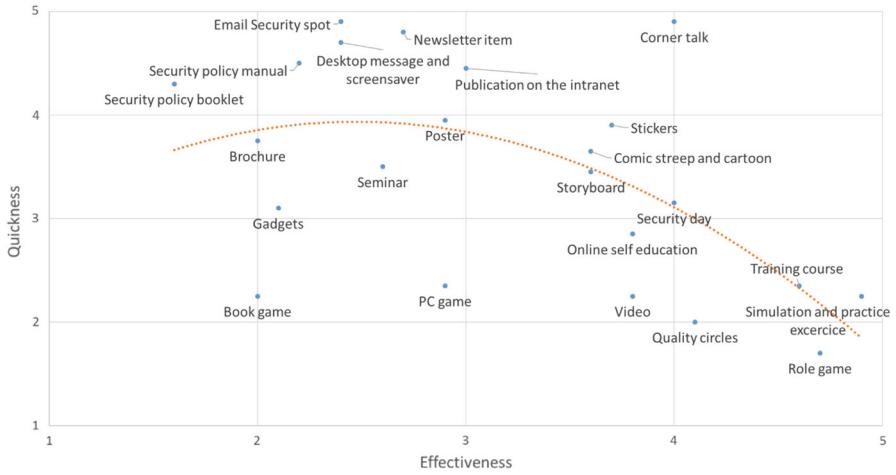

Fig. 8 Methods to increase the security awareness represented in their effectiveness and total time (i.e., design time and completion time)

first group and they are also able to reach a degree of awareness definitely greater than those of the first group; moreover, they have a comparable level of effectiveness. However, there are some interesting exceptions, such as *Newsletter items* (with regards to the first group) but especially *On-line self-education* and *Corner talk* (second group) that show significantly better performances than the corresponding group.

In Fig. 8, the same analysis has been accomplished by comparing the effectiveness and the total time spent from the design to the completion of the method. In this case too, the quickest methods do not require an active involvement of the employees. In the most effective methods, the employees have an active role; their setup requires more time for completion (from 1 to 3), in particular *Simulation and practice exercises*, *Role games*, *Training courses,* and *Quality circles*, whose results are very similar to those case in which the costs were considered. It is noticeable the presence of outlier methods (e.g., *Book game* and *PC game*) that take a very long time to be completed, with a low effectiveness. On the contrary, *Corner talk* shows a very good trade-off between quickness and effectiveness.

Figure 9 shows a representation of the effectiveness of methods with respect to the time horizon, i.e., how long the "message" remains clear in the mind of the recipients. In this case, two main clusters are observed. The first cluster is composed of methods with a limited time horizon that is independent from the effectiveness of the method. This represents a group of methods useful to solicit the attention of employees on a specific issue but not fully recommended for reaching a persistent enhancement in the level of security awareness. The second cluster is composed of methods with considerably higher effectiveness and time horizon, grouped along a straight line with a positive slope. In the top right corner of the graph, we found *Simulation and practice exercise*, *Role game,* and *Training course*, that better fulfill

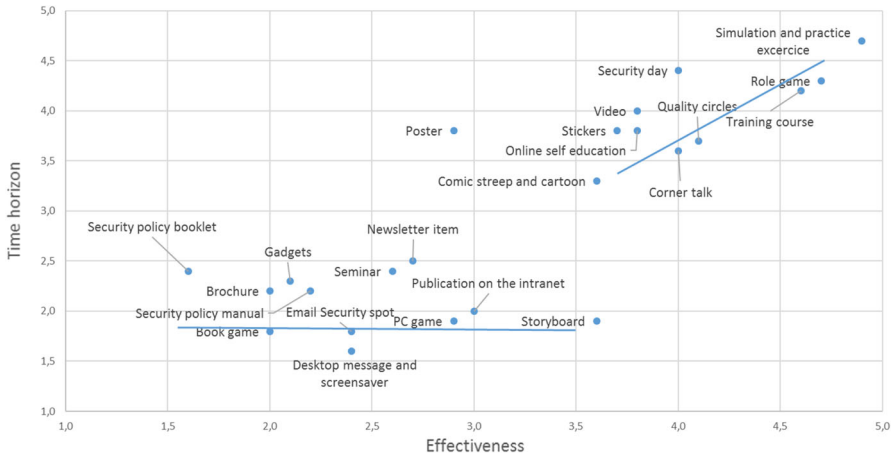

Fig. 9 Methods to increase the security awareness represented in their effectiveness and time horizon

the goal of improving the security awareness. It is interesting to point out that *Poster* represents a good solution that provides a good time horizon.

In Fig. 10, the popularity of each used method is compared with the penetration depth. It is calculated as the average among the recipient dimension (the more the rate is high, the more the number of employees involved in the security awareness initiative is large), the message extension (the amount of information provided), and the time horizon (how long the message can be remembered by recipients). In the top right corner of the graph, we found the *Training course*, meaning that it is a widely used method with a high penetration depth. Moreover, it should be noted that quite all the methods are polarized in the top right corner of the graph. This means that the popularity of each method is well justified by the penetration depth that characterizes each method, which is a valid indicator of efficiency.

Finally, in Fig. 11, the popularity of each method is linked with its effectiveness. The graph does not show a clear pattern, meaning that the popularity of the method is not even related to the effectiveness of the method. Specifically, the method *Quality circle* shows a high popularity not justified by its perceived effectiveness, whilst *Training course* and *Role game* show a popularity in line with their high level of effectiveness.

4 Methodology to Increase the Level of Security Awareness Software Tool

From the data collected during the survey, it arises that not always the most popular methods are the most effective. Moreover, as highlighted by the above-mentioned analysis, it does not exist a single method that can be considered as the silver bullet, but there are a set of effective methods suited to quickly deliver specific messages and some other more suitable to increase the general awareness of the employees. Some methods require a very long time to be designed and delivered. Some easily

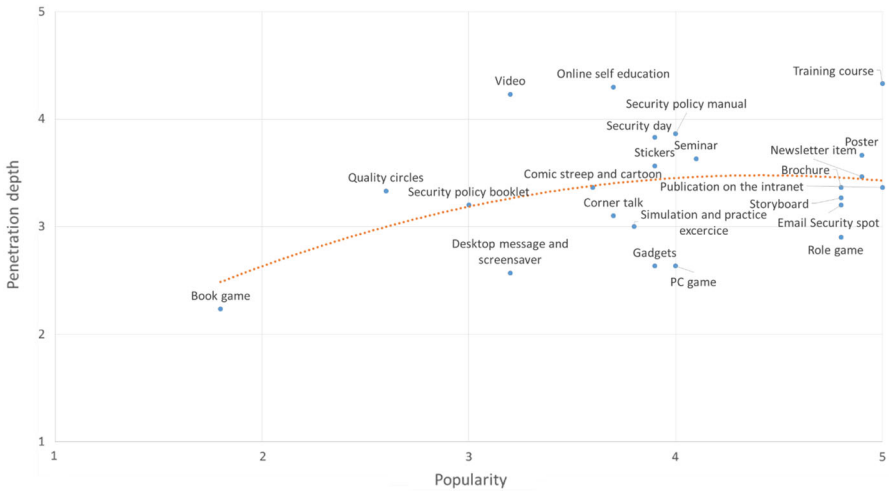

Fig. 10 Methods to increase the security awareness represented in their popularity and penetration depth

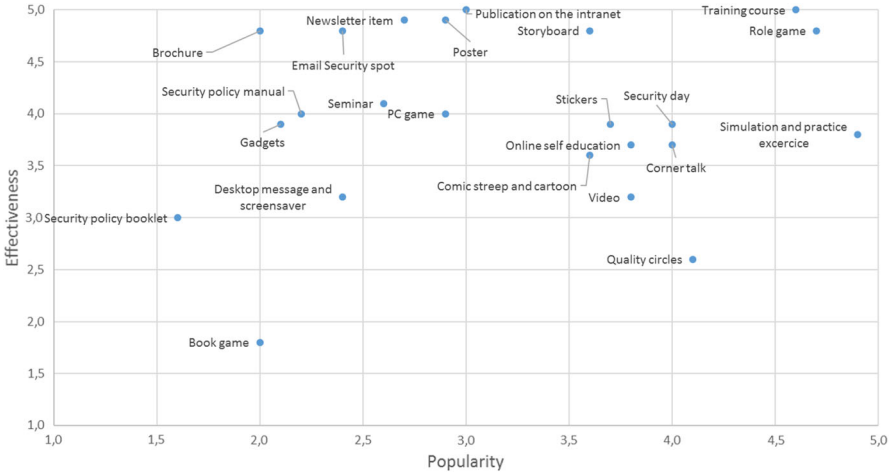

Fig. 11 Methods to increase the security awareness represented in their popularity and effectiveness

scale with the dimension of the audience and some are feasible only for small groups of people, possibly with a specific background. Finally, in any organizations, the cost of the "best" method cannot overcome the allocated budget. Hence, the "best" method strongly depends on the problem at hand.

To support organizations in identifying the most valuable initiatives, we developed a decision support system called MEISA (MEthodology to Increase the level of Security Awareness tool). It is a software designed to support practitioners in identifying methods to increase the Security Awareness of their organizations on the basis of a set of parameters. Specifically, the aim of the tool is to provide a set of

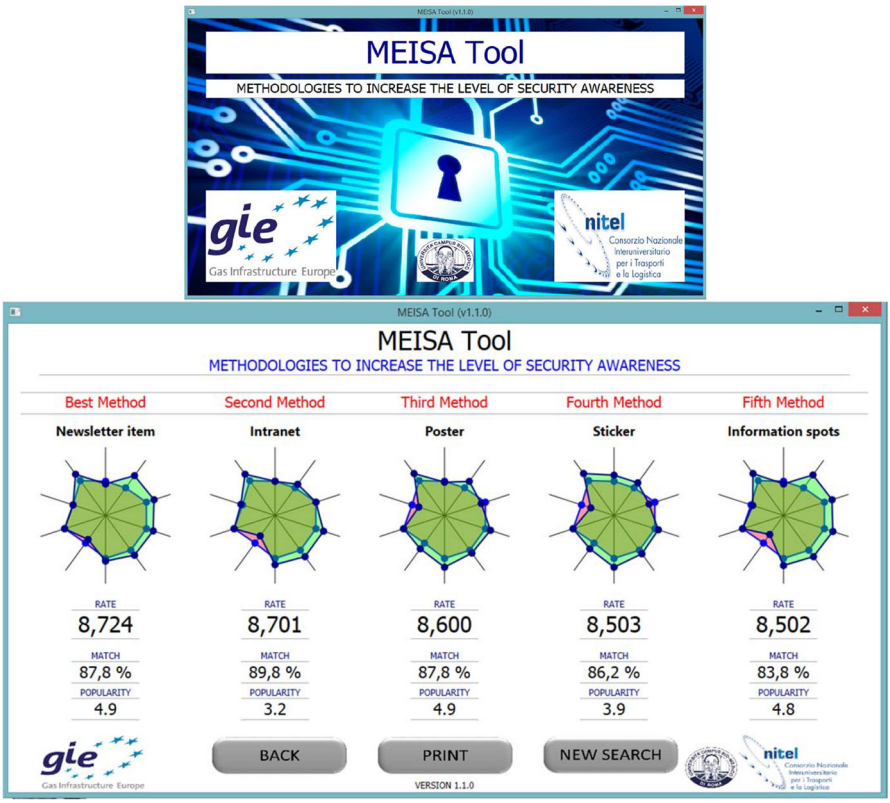

Fig. 12 MEISA Tool home query results screen

five methods that better fit users' requirements to guide them in selecting the most appropriate method.

Once requirements have been chosen through a set of parameters (up to 12, Fig. 12), the tool finds the best-fitting methods among those illustrated in the paper and better described in (Setola et al. 2015). To this end, the tool compares the numerical indicators specified in the user's requirements with those associated with the different methods in the MEISA database to identify the methods that better fit the requirements avoiding both under- and over-performances and also considering the limited importance of each parameter. To manage the uncertainties and the vagueness of the collected information, the software uses a fuzzy logic engine (Dubois and Prade 1982) managing all the inputs quantities through triangular fuzzy numbers.

Specifically, due to the ambiguities resulting from the data, the software displays the best five methods to help the end-user in identifying, via a deep analysis of the proposed methods, the ones that better fit his/her requirements. To this end, the software shows the corresponding radar plots with the obtained ratings, the matching values, and the popularity of each method (Fig. 13). In particular, the radar plot of the method is showed in green and the one of the user's query in red.

Fig. 13 MEISA Tool home screen and requirements setting screen

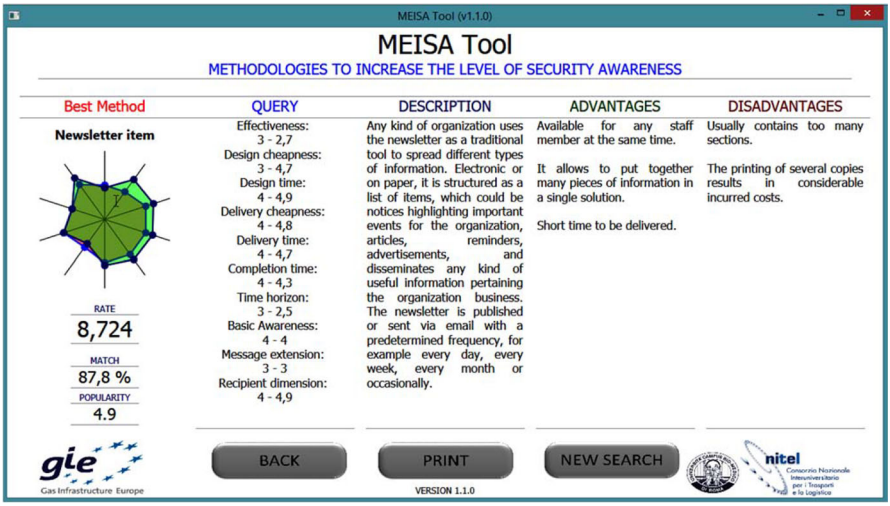

Fig. 14 MEISA Tool method details screen

The system calculates:

- the rating, to give a measure of the relevance/convenience of the method. The value of the rating is from 1 to 10 and correlates each parameter introduced in the query with the related parameter inside the database;
- the matching value indicates how much the characteristics of the methods correspond to the desired ones, expressed in percentage;
- the popularity, taken from the method datasheet and not requiring any calculation, ranges from 1 to 5.

Furthermore, for each method, the tool shows its short description, advantages, disadvantages, and the comparison between the numerical values corresponding to the query and the method's assessment indicators (Fig. 14).

5 Conclusions

Security awareness is a basic concept in the current societal scenario, due to the huge interconnections of technological systems and to the increased importance of the human factor for the security and resilience in large and complex organizations. Indeed, a large percentage of security incidents originates or escalates from human errors, because of a lack of knowledge, negligence, etc. Moreover, enemies can take advantage of the human weaknesses and exploit acquired information and/or privileges to perform attacks.

Notice that while the relevance of the human factor has been recognized as a cornerstone of any safety strategy, less attention is paid in the security awareness of the employees, even in critical infrastructures' companies.

The study described in this paper shows that organizations are always more interested in campaigns and initiatives promoting the security awareness among their employees. When asked to define what the security awareness refers to, the majority of responders deal with "security culture".

The present study aimed at investigating how the security awareness is perceived and at acquiring details regarding the most common initiatives and tools used by large organizations to increase the level of security awareness of the employees, to provide an effective support to the design of security awareness campaigns. In particular, 23 methods to increase the security awareness have been collected and organized in datasheets containing a detailed analysis of each method. Furthermore, a set of assessment indicators provides a quantitative evaluation of the performance of the method with respect to a set of assessment parameters.

The assessment indicators allowed to elaborate analysis for the comparison of each method as presented in Sect. 3. This assessment has been the basis for the design of the MEISA software tool described in Sect. 5; it aims at helping organizations to design a security assessment campaign for their employees that fit their need and constraints in terms of costs, time, number of recipients, etc.

Since the critical infrastructure protection environment evolves quite fast, security awareness initiatives are increasing, involving not only the security but also all the organization departments to provide the basis for an efficient and collaborative protection of the business. To this end, it is important to properly select the right approach to use on the basis of the actual goal, context, time, and cost constraints.

Acknowledgements The authors would like to thank the Security Study Group of GIE—Gas Infrastructure Europe—for the commitment and the support.

References

Al-Awadi M (2009) A study of employees' attitudes towards organisational information security policies in the UK and Oman (Doctoral dissertation, University of Glasgow)

Allport GW (1935) Attitudes. In: Murchison C (ed) Handbook of social psychology. Clark University Press, Worcester, pp 789–844

Bullock J, Haddow G, Coppola DP (2011) Introduction to homeland security: principles of all-hazards risk management. Butterworth-Heinemann, Oxford

Cacciabue PC (2004) Human error risk management for engineering systems: a methodology for design, safety assessment, accident investigation and training. Reliab Eng Syst Saf 83(2):229–240
Cobbina JE, Nalla MK, Bender KA (2013) Security officers' attitudes towards training and their work environment. Secur J 29:385–399
Council ECR (2004) The economic impacts of the August 2003 blackout. Washington, DC
De Maggio MC, Mastrapasqua M, Setola R (2015) The Professional Figure of the Security Liaison Officer in the Council Directive 2008/114/EC. In: International Conference on Critical Information Infrastructures Security (pp. 211-222). Springer International Publishing
Dekker S (2004) Ten questions about human error: A new view of human factors and system safety. CRC Press, Boca Roton
Dubois D, Prade H (1982) A class of fuzzy measures based on triangular norms: a general framework for the combination of uncertain information. Int J Gen Syst 8(1):43–61
Fishbein M, Ajzen I (1975) Belief, attitude, intention, and behavior: an introduction to theory and research. Mass: Addison-Wesley, Boston
Greitzer FL, Kangas LJ, Noonan CF, Brown CR, Ferryman T (2013) Psychosocial modeling of insider threat risk based on behavioral and word use analysis. e-Serv J 9(1):106–138
Hills M, Anjali A (2017) A human factors contribution to countering insider threats: practical prospects from a novel approach to warning and avoiding. Secur J 30(1):142–152
Huston T (2001) Security issues for implementation of e-medical records. Commun ACM 44(9):89–94
Kirschenbaum AA, Rapaport C (2012) Does training improve security decisions? A case study of airports. Secur J 30:184–198
Krombholz K et al (2015) Advanced social engineering attacks. J Inform Secur Appl 22:113–122
Liscouski B, Elliot W (2004) Final report on the august 14, 2003 blackout in the United States and Canada: Causes and recommendations. A report to US Department of Energy, 40(4)
Manzo J (2009) Security officers' perspectives on training 1. Can J Criminol Criml Justice 51(3):381–410
Pastor V, Díaz G, Castro M (2010) State-of-the-art simulation systems for information security education, training and awareness. In: Education Engineering (EDUCON), 2010 IEEE. IEEE, pp 1907–1916
Perrow C (2011) Normal accidents: Living with high risk technologies. Princeton University Press, Princeton
Ryan RM, Deci EL (2000) Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. Am Psychol 55(1):68
Saaty TL (1988) What is the analytic hierarchy process? In: Mitra G, Greenberg HJ, Lootsma FA, Rijkaert MJ, Zimmermann HJ (eds) Mathematical models for decision support. Springer, Berlin, Heidelberg, pp 109–121
Schein EH (2006) Organizational culture and leadership, vol 356. Wiley, Hoboken
Setola R, Mastrapasqua M, Tesei M, De Maggio MC, Corradini I, Pantaleo C, Capitello ME, De Simio F (2015) Study on security awareness in gas infrastructure. Final report
Siponen MT (2000) A conceptual foundation for organizational information security awareness. Inform Manag Comput Secur 8(1):31–41
Stackpole B, Oksendahl E (2010) Security strategy: from requirements to reality. CRC Press, Boca Roton
Swain AD and Guttmann HE (1983) Handbook of human-reliability analysis with emphasis on nuclear power plant applications. Final report (No. NUREG/CR-1278; SAND-80-0200). Sandia National Labs., Albuquerque, NM (USA)
Weinberg A, Kaplan J, Bailey T (2014) The $3,000 bn threat from cyber attacks. Financial, Times, p 28
Workman M (2007) Gaining access with social engineering: an empirical study of the threat. Inform Syst Secur 16(6):315–331