European Journal for Security Research (2020) 5:259–287
https://doi.org/10.1007/s41125-019-00052-x

ORIGINAL ARTICLE

A Review of Methods for Evaluating Security Awareness Initiatives

Giacomo Assenza[1] · Andrea Chittaro[2] · Maria Carla De Maggio[1] · Marzia Mastrapasqua[2] · Roberto Setola[1]

Received: 27 May 2019 / Accepted: 14 September 2019 / Published online: 26 September 2019

Abstract

The 'human factor' is commonly considered to be the weakest link in an organization's security chain, and a significant percentage of companies have implemented security awareness (SA) programs to address this vulnerability. However, an element whose usefulness is still underestimated is the importance to perform measurements of the different SA programs' effectiveness in order to assess their adequateness for achieving the intended goals. This gap has serious consequences as most of the security awareness campaigns have resulted to be largely unsuccessful. Awareness measurement tools might be determinant in providing feedback on the outcome of a program as well as in helping with the strategic planning for endorsing security. This article will introduce and critically compare a set of measurement methods. It will then discuss their attributes and suggested applications.

Keywords Security awareness · Security awareness measurement · Security management · Critical infrastructure security

1 Introduction

Today's critical infrastructures are becoming increasingly complex and vulnerable, and the 'human factor' is largely considered to be the weakest link in their security chain (Mitnick and Simon 2011; Patrick et al. 2003). In fact, humans perform a wide range of critical and complex activities (managing crisis, communication, and implementation of procedures) where even a single mistake can rapidly escalate creating mass havoc and big failures. Addressing the human factor with proper awareness training is a *condicio sine qua non* to pursue the well functioning of companies

✉ Roberto Setola
r.setola@unicampus.it

[1] Complex System and Security Lab, Università Campus Bio-Medico di Roma, Via Alvaro del Portillo, 21, 00128 Rome, Italy

[2] SNAM, Corporate Security, Milan, Italy

in general and critical infrastructure in particular. Hence, security compliance is not possible without addressing the human issues with proper awareness and training (Bresz 2004; Tsohou et al. 2008).

To date, although a significant percentage of companies have implemented or will implement security awareness (SA) programs, the number of those that have adopted procedures to measure the actual level of awareness is strikingly low. This discloses a deep discrepancy between the business sector and the academia that produced useful insights on the cruciality of performing SA evaluation, as well as suggesting measurement methodologies (Abawajy et al. 2008; Karjalainen and Siponen 2011; Rahim et al. 2015). Such a reluctance of organizations can have detrimental effects, as having implemented SA initiatives does not automatically ensure that employees comply with safety and security behaviors and respect the in-force standards and procedures (Kruger and Kearney 2006). Also, assessing the personnel level of awareness, before and after the implementation of security training and initiatives, could be the starting point for defining action plans to boost their impact and effectiveness. It would enable the security board to detect the intrinsic weaknesses of existing campaigns and adjust their contents to address the registered problems (Crossler et al. 2013; Choo 2011).

In other words, in order for security programs to strengthen the safety and security of an organization, it is of paramount importance to adopt a well-structured measurement approach enabling not only to assess the overall level of SA, but also to evaluate the effects of SA initiatives. This article will argue that the concept of awareness is composed of three components, namely knowledge, attitude, and behavior, and it will stress that an accurate evaluation should include the three of them. It will then introduce a set of measurement methods and approaches particularly suitable to measure these identified components. The pillar of this paper is that the most accurate and reliable measurement method is not necessarily the best one. On the contrary, organizations should elaborate their evaluation strategy according to their specification in terms of structure, field of operation, time, available budget, etc. To this end, the paper aims to provide useful and practical indications to all the companies willing to engage in SA assessment activities.

The argument proceeds as follows. Section 1 discusses the human factor's incidence in the increasing complexity of critical infrastructure panorama. Section 2 endorses the cruciality of adopting measurement plans in order to add value to SA campaigns. Section 3 analyses the concept of security awareness and identifies three elements (knowledge, attitude, and behavior) that should be taken into account when measuring. Sections 4 and 5 will introduce a series of measurement methods together with a set of indicators useful to evaluate and compare their strengths, weaknesses, and reliability.

2 The Human Factor

Critical national infrastructures (CNIs) are huge, complex, and global institutions whose systems, processes, communication links, offices, and personnel conduct a wide variety of operations and span across many countries. They operate in sectors

typically characterized by strong interdependence (Pescaroli and Alexander 2016; Zimmermann 2004) and high outsourcing, where some assets are necessary for the operation of others (Setola et al. 2016; Das et al. 2012; Brunner and Suter 2008). Such an infrastructural complexity is an indispensable attribute of today's organizations and brings both opportunities and risks. On the one hand, it makes daily operations simpler, faster, and more effective. On the other hand, it dramatically increases vulnerability and creates serious security issues and threats.

Technological systems are often seen as an effective way to curb threats and address vulnerabilities. All infrastructures are provided with abundant technologies aimed at improving security, for instance, firewall products, sensors, intrusion detection systems, and assets for strong authentication. Also, new instruments are constantly being developed and implemented, which might make one think that assuring critical infrastructure is relatively straightforward. However, data about incidents and breaches show that achieving satisfactory security standards is far from being a trivial task. This is because technology, no matter how independent or autonomous, needs to interface with people, which leaves an ample space to the incidence of "human errors" (Schultz 2005; Furnell et al. 2006).

For this reason, the "human factor" is largely considered to be one of the weakest links in the security chain (Mitnick and Simon 2011; Patrick et al. 2003; Solms 2000). Employees are somehow responsible for the majority of security breaches within organizations and pose a serious threat not only intentionally, such as in the case of 'disgruntled workers' engaging in actions of sabotage (Hills and Anjali 2017; Byres and Lowe 2004), but also unintentionally, as they play a crucial role in evolving events by performing activities such as crisis managing, communication, minimizing damages, and implementing recovery procedures (De Maggio et al. 2017). These tasks are particularly decisive in critical infrastructures where, due to the primary need for availability of offered services and the high degree of interdependence, even a single mistake can rapidly escalate creating mass havoc and big failures (Moteff and Parfomak 2004).

Many events showed how employees' inaccuracy and inadequate behaviors can cause accidents with serious or even disastrous ramifications. For example, a 2012 study on data protection indicates that at least 35% of breaches were caused by human factors and 78% of organizations experienced data loss as a result of employees' negligence or malicious actions (Ponemon Institute 2012).

The danger originated by the human factor is particularly stressed in the IT and cyber-security field, but it applies also to the physical, organizational, and all other aspects of security. The Chernobyl explosion, as an example, is probably the most known and dramatic episode of human active failure (Reason 2000). One of the factors causing the explosion of the nuclear reactor was that a team of technicians had disabled the emergency cooling system so as to prevent it from interfering with an ongoing test. The consequences of the Chernobyl incident were unprecedented: 56 direct deaths, 4000 cancer-related deaths, $1.2 billion in recovery costs, and 100,000 years of radioactivity of the area (BBC 2004).

Another emblematic episode is the 2003 blackout in North America. As appointed in the Final report of the US–Canada Power System Outage Task Force, the blackout was caused by a combination of human errors and technical failures

(US–Canada Power System Outage Task Force 2004). In particular, the Task Force identified specific weaknesses such as lack of adherence to industry practices, poor communication, and inadequate management and decision making. Despite not as catastrophic as Chernobyl, the outage had a significant impact in terms of damages and consisted in fifty million of users that lost power for up to 2 days, which indirectly contributed to the death of eleven people and caused six billion dollars of estimated cost (Muir and Lopatto 2004).

On the other side, the human resource represents the most effective element to manage any complex security-related situation. If well trained, humans could be the strongest link in the security chain. Indeed, only well-prepared and well-motivated personnel are able to adequately react to unexpected, noncompliant, and unpredictable events.

3 Security Awareness Initiatives and the Importance of their Measuring

It appears, therefore, clear that building a solid security system cannot disregard a robust intervention to address the human factor and for this reason many organizations have implemented security awareness programs (SA). SA is a concept that aims to turn humans from the weakest to the "strongest component of a system" (Perrow 2011) by enabling them to manage proactively and accurately the development and implementation of security. These programs are focused on building and disseminating a culture of incidents prevention, mitigation, and risk management and can entail a wide variety of activities such as training courses, role games, seminars, online self-education, and many other initiatives.

Today, engaging in SA activities is becoming increasingly common. A survey carried out by the authors between October 2014 and February 2015 and involving European companies operating in critical sectors shows that 84% of organizations have been implementing SA programs, 36% of which for more than 5 years (De Maggio et al. 2017). Half of the respondents declared that their organization has a specific staff somehow involved in the security awareness program and about one-third 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.

That survey, promoted by GIE—Gas Infrastructure Europe, shows that most of the awareness initiatives are addressed to all the employees (74% of the responders). Only a limited number of responders (14%) declared that security awareness initiatives involve only the employees working in the security departments and on critical process operations. Finally, very few responders (i.e., 7%) stated that security awareness programs were planned also for vendors, third parties, and business partners (De Maggio et al. 2017).

Concerning the focus of the security awareness programs, the largest attention is paid to the cyber domain, a topic included in 88% of the security awareness programs, which is usually considered as the most relevant and dangerous threat. The graph in Fig. 1 shows that almost 75% of the organizations that have a security

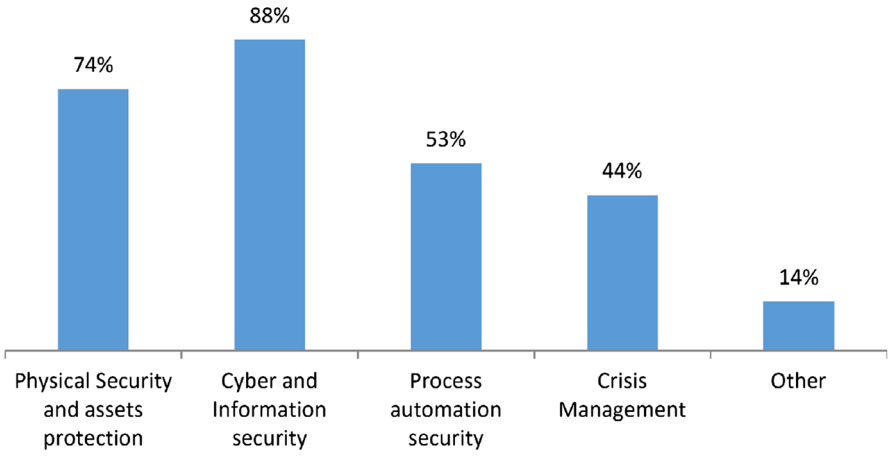

Fig. 1 Fields of application of the security awareness programs (42 answers) (De Maggio et al. 2017)

awareness program also developed initiatives in the field of physical security. About half of the organizations perform security awareness programs for the industrial control systems (e.g., SCADA, PLC, etc.) being these a critical element in the GIE company business. The attention to crisis management is unexpectedly quite limited (44%).

However, the most surprising figures concern the activities developed by such companies to "measure" the effectiveness of their awareness programs. Although a significant percentage of companies are implementing (or will implement) security awareness (SA) initiatives, the number of those that have adopted procedures to measure the impact of these efforts and the improvement of the actual level of awareness is strikingly low. In the same survey, the respondents were asked to declare if their organizations had specific programs or indexes to monitor the SA level of their employees, or at least whether they were planning to elaborate one. Only 29% asserted to have implemented measurement methods and, while 40% of organizations were planning to launch programs of this fashion, 31% of respondents did not consider them useful or advantageous (Fig. 2).

This means that investments and initiatives are largely based on a priori qualitative assumptions rather than on quantitative ex-post empirical evidences. A possible explanation is that, in several companies, security managers adopt an experience-based approach rather than a structured methodology.

However, even if experience can be extremely valuable, it appears inadequate to manage the actual security scenario, due to the increasing complexity and fast dynamics of threats and contexts. In particular, such an approach risks to be ill-suited for monitoring the awareness level as SA programs are essentially prevention oriented, and by focusing only on occurred episodes of security breaches, the assessment risks being limited and inaccurate. On the contrary, an efficient SA evaluation should be based on how daily operations are performed, together with the perception and understanding of the personnel.

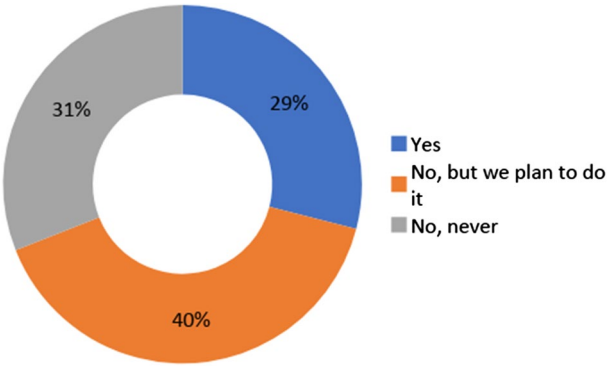

Fig. 2 Organizations with programs for measuring SA

In fact, having implemented SA initiatives does not automatically guarantee that employees understand their role in preserving safety and security and respect the in-force standards and procedures (Kruger and Kearney 2006). Measuring the stage of security awareness is of paramount importance as the few data available show these programs to be far from effective. As acknowledged by a study of the Information Security Forum (ISF), 85% of organizations reported their personnel to be unaware or aware but not willing to adopt the correct behaviors for minimizing the security risks. Similarly, the same report notes that only 15% of the ISF members that have engaged in awareness action plans declared to have reached the desired awareness level (ISF 2014).

Also, this lack of commitment of organizations toward performing evaluation activities discloses a deep discrepancy between the business sector and the academia. In fact, assessing SA is not a new concept, and many scholars have engaged with the study of these topics. These focus on different groups of people ranging from home users (Furnell et al. 2007; Talib et al. 2010) to youngsters (Rahim et al. 2015) to college and universities, but the most studied environment are organizations (Mani et al. 2014; Parsons et al. 2014; Caputo et al. 2014). The current literature, by proposing a wide set of measurement tools such as survey, questionnaire, e-learning, role games, etc., has also stressed the importance of adopting assessment strategies that are based on multiple methods and that combine quantitative and qualitative tools. This should ensure the validity and reliability of the feedback as weaknesses and strengths of each method would complement each other (Rahim et al. 2015). For example, several authors propose systematic program evaluation techniques (Tsohou et al. 2008), such as the Kirkpatrick's four-level learning model (Abawajy et al. 2008; Karjalainen and Siponen 2011), whose output is the result of a multi-layered and all-encompassing process.

Certainly, the existing literature impeccably acknowledges that adopting methods to study and assess awareness is crucial for SA initiatives to contribute in raising the general level of security of an organization as it would provide useful feedbacks and indications to the people in charge about the status of the SA campaign, and would assist them in their strategic planning and corrective interventions (Crossler

et al. 2013; Choo 2011). On the other hand, it is of little help in providing concrete directions to those aiming to design and implement evaluation campaigns. By overfocusing on identifying the most accurate, reliable, and descriptive measurement approaches, it scarcely takes into account typical business-like issues, such as tight deadlines, limited resources, and heavy workload, that mark the working pace of all organizations. In other words, individuating the best evaluation methodology is of little utility if its implementation results overly expensive, long, and complex. Such a theory-oriented approach partially explains the existing disparity between the academia, which has so far produced valuable insights on the topic of SA assessment, and the business, whose practical engagement in evaluating its personnel is far below the advisable level, with significant consequences for security.

In order to try to reduce this gap, this paper will introduce a taxonomy of measurement methods stressing their practical advantages, disadvantages, and applicability. With the idea that the "best method" is not necessarily the most suitable, the paper will attempt to provide meaningful guidelines for implementing effective SA evaluation campaigns in organizations, and with the aim of helping companies in their trade-off between security and feasibility.

In any case, in order to elaborate a structured and consistent methodology to measure awareness, one must first answer two essential questions: what to measure? And how to measure it? The following sections, starting with an analysis of the different components of the concept of awareness, will attempt to address these questions.

4 Security Awareness, What to Measure?

Before analyzing the methods to evaluate the level of SA, it is necessary to define the concept of awareness, thus understanding what are the variables and components worth taking into account when measuring it. Awareness is a concept that has its roots in the behavioral theory and refers to the state resulting from the acquisition of knowledge, norms, or practices (NIST 1998; Mishra and Dhillon 2006). In this definition, "acquisition" is an emblematic word in need of further specification. Acquiring something is the result of a personal process connected to intimate factors that characterize not only the single employee as an individual, but also the personnel as a whole.

Three elements of this process can be identified: *knowledge*, *attitude*, and *behavior* (Kruger and Kearney 2006). *Knowledge* indicates the process by which employees learn the existing standards, norms, and procedures that are desirable to ensure both the environment and operations. The learning process can be realized through various activities (i.e., trainings, information campaigns, and brochures) but despite relevant, if taken alone it represents an improper objective to raise SA as it 'does not reflect the idea of prescriptiveness' (Siponen 2000). In other words, people might know the security guidelines and nevertheless adopt non-compelling and unsafe behaviors (Siponen 2001; Workman et al. 2008; Herath and Rao 2009; Siponen et al. 2010). For instance, although it is common knowledge that driving with the

seat belt fastened is both prudent and mandatory, most people deliberately ignore the risk and behave unsafely.

The idea of prescriptiveness does not stem from an external input, but it is rather the consequence of one's *attitude*. The attitude is strictly connected to the consciousness of an individual (Murchison 1935) and refers to the perception that the latter has about the object of interest (Ryan and Deci 2000). In this case, the attitude arises from the belief of usefulness that the personnel has about security norms (Davis 1989) as well as their present and past experience. There is a positive attitude inside an organization when all employees feel actively involved in the security process, they understand its importance and share the same values. The attitude is deeply influenced by the organizational culture, defined as the pattern of assumptions that a given group has developed (Schein 2009) including a system of shared security values and practices (Szilagyi and Wallace 1983).

Attitude and organizational culture form together the motivation of leading the employees to assume a positive *behavior*. As asserted by Émile Durkheim, 'Man cannot become attached to higher aims and submit to a rule if he sees nothing above him to which he belongs' (Durkheim 1897). In the SA case, the prescriptive character of security policies, regardless whether these are enforced or not, is the consequence of shared values and a sense of belonging that in turn affect the consciousness of employees and thus their behavior. The utopic outcome of SA campaigns is not endorsing a one-time behavioral change, probably after an incident occurred, but rather establishing a long-term, repetitive change (Pfleeger et al. 2014) with a preemptive approach. The staff of a company can be considered aware when it is the carrier of positive habits that completely mold the way in which the operations are carried out in the everyday routine.

In other words, security awareness is a complex and multifaced concept that includes at least three main elements, namely knowledge, attitude, and behavior, and an accurate evaluation should not miss any of them. This intrinsic complexity implies that evidence of awareness cannot be found through an all-encompassing instrument. On the contrary, it would be more recommended to adopt an approach structured on variety of different indicators. The following section will introduce a series of assessment tools, each of which is suitable for measuring specific aspects of the wider SA concept.

5 How to Measure It?

This section will introduce different methods for measuring the level of security awareness. As mentioned before, SA is composed of three main elements, knowledge, attitude, and behavior, which are inherently different from each other and thus require specific tools and indicators to be monitored. For each component, a set of measurement methods will be introduced together with their descriptions, advantages, and disadvantages. Also, a series of parameters evaluating these methods' performance will be presented with the corresponding radar plots.

Specifically, 8 numerical indicators and 4 qualitative descriptors have been considered. Table 1 shows these indicators and identifies the relative indexes to measure

Table 1 Parameters for evaluating SA measurement method's performance

Indicator	Definition	Options
Reliability	The extent to which the method yields unbiased results from the measurements.	1. Poor 2. Fair 3. Good 4. Very good 5. Excellent
Design cheapness	The extent to which the method requires low-cost design processes, including all the activities from the definition of the idea till the delivery of the method (not included). The higher the value of the design cheapness, the less expensive the design of the method for the organization.	1. More than 100 k€ 2. 50 to 100 k€ 3. 10 to 50 k€ 4. 1 to 10 k€ 5. Less than 1 k€
Design time	The overall time necessary for the design process, including all the activities from the definition of the idea till the delivery of the method (not included). The higher the value of the design time, the faster the process to design the method.	1. More than 1 year 2. 6 to 12 months 3. 3 to 6 months 4. 1 to 3 months 5. Less than 1 month
Delivery cheapness	The extent to which the method requires a low-cost process to deliver the method to the target audience. The higher the value of the delivery cheapness, the less expensive the delivery of the method.	1. More than 100 k€ 2. 50 to 100 k€ 3. 10 to 50 k€ 4. 1 to 10 k€ 5. Less than 1 k€
Delivery time	The overall time necessary for the implementation of the method, namely the duration of the activities involved in the measurement process till the elaboration and processing of the results. The higher the value of the delivery time, the faster the process to deliver the method to the recipients.	1. More than 1 year 2. 6 to 12 months 3. 3 to 6 months 4. 1 to 3 months 5. Less than 1 month

Table 1 (continued)

Indicator	Definition	Options
Completion time	The overall time necessary to provide the method to a single person.	1. More than 8 h 2. 1 to 8 h 3. 10 to 60 min 4. 1 to 10 min 5. Less than 1 min
Results extension	The amount of information collected investigating via the considered method.	1. Poor 2. Sufficient 3. Good 4. Very good 5. Excellent
Recipient dimension	The number of people that could be involved using the method.	1. Less than 10 2. From 11 to 30 3. From 31 to 100 4. From 101 to 500 5. More than 501
Type of recipient	This indicator identifies the people to whom the class of methods is addressed according to their position within the organization. Some techniques are suitable for members of specific departments of the organization and cannot be delivered to all employees, since they are focused on specific tasks.	1. All employees 2. Employees operating in security functions 3. Only management 4. Only executives 5. Employees working on (critical) process operations 6. Front-end employees 7. Employees working in other countries' assets/offices 8. Vendors and business partners 9. Other

Table 1 (continued)

Indicator	Definition	Options
Scheduling	How often the method is delivered to the organization's employees. Depending on the measurement technique, the collection of information regarding the staff security awareness could occur periodically or at specific moments of the security awareness enhancement path.	1. Periodically, in order to have an update of the organization's situation 2. After every initiative for security awareness 3. Before the planning of a new initiative for security awareness, to identify proper objectives and methods 4. Before and after every security awareness initiative, in order to verify the initiative's efficiency 5. After a relevant security incident 6. After a relevant change in the organization 7. Continuous 8. Other
Field of application	This indicator contains the information regarding the security sectors where the method could be applied. Some of the initiatives could be suitable only for selected fields of the organization, among the ones listed.	1. Physical security and assets protection 2. Cyber and information security 3. Process automation security (e.g., SCADA, ICS, PCS, etc.) 4. Crisis management 5. Other
Popularity	This indicator provides a measure of how often the method is/has been adopted.	1. Very uncommon 2. Uncommon 3. Known 4. Popular 5. Very popular

them. To some of them, it is attributed an integer number on a scale from 1 to 5, where 1 indicates the worst condition and 5 the most advantageous level. Other indicators can assume a unique value, numerical or qualitative, which adds further information to describe the method. The indicators and descriptors assigned to each method have been selected merging the answers of experts surveyed in De Maggio et al. (2017). Specifically, 24 experts have been engaged to asses the relevance, for each method, of the different indicators using the analytic hierarchy procedure described in Saaty (1988).

5.1 Assessing Knowledge: Questionnaire, Interview, and Post-training Tests

Among the three, *knowledge* is probably the most directly "measurable" component. Evaluating the knowledge of employees entails gathering information regarding the level of preparation, learning, and know-how within the internal department (Wilson and Hash 2003). *Questionnaires*, *tests*, and *interviews* are common methods to survey security awareness in general but result to be particularly practical for assessing knowledge. In fact, these can be structured so as to include a set of questions testing the level of expertise of respondents. The questions can be all encompassing, thus aimed at verifying whether employees have developed a thorough comprehension of the security topic in general, for example, by investigating if the personnel are aware of the main threats to the organization or of the most common errors that might cause serious security breaches. Or else, they can be focused on determined security aspects that are relevant according to the position or tasks of the respondents, such as specific policies and procedures or particular standards and best practices in being.

Questionnaires, tests, and interviews have different characteristics and can be used depending on the needs of a company. A *questionnaire* is an online or written survey and can be structured following an ad hoc design in order to suit the specific unit to which it is addressed or to investigate a particular aspect of the security issue. The radar plot in Fig. 3 reports the assessment indicators discussed in Table 1 applied to the questionnaire as a measurement tool. The chart emphasizes

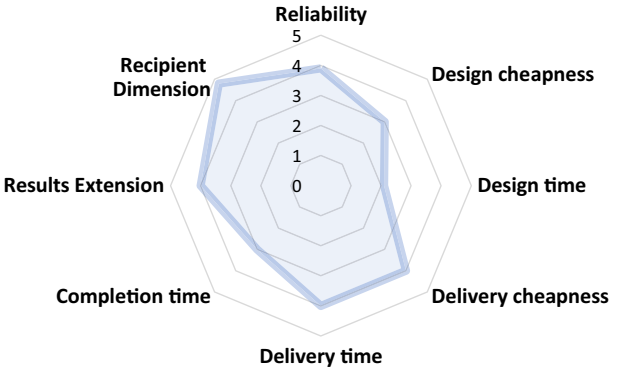

Fig. 3 Radar plot for questionnaire method (Setola et al. 2015)

the capability of questionnaires to be adopted for large audience but, at the same time, they require significant investments in terms of cost, design, and completion time. Depending on the type of questions, questionnaires can have a uniform or mixed structure. For example, a uniform questionnaire contains only a type of question, i.e., open, yes/no, or multiple-choice questions, whereas mixed questionnaires present a combination of the three kinds (Agresti 2018; Stone 1993). A key factor influencing the reliability of questionnaires is both the number and type of questions. Long and complex surveys can provoke a loss of attention in the respondents leading to a rushed and negligent completion, which in turn affects the measurement accuracy (Bradburn et al. 2004). For this reason, it is good practice to choose a structure that allows to collect the largest amount of information with the minimum number of questions. Also reducing the open questions in favor of multiple-choice and yes/no questions could be a strategy (Groves et al. 2011). Certainly, open questions have a deeper investigative potential as respondents are required to develop personal considerations, opinions, and understanding. On the other hand, multiple-choice and yes/no questions are straightforward, and the data collected are in a convenient format for statistic processing.

As well as for the questionnaire, all the polling methods are subject to a trade-off between the depth of the gathered information and their statistical generalization potential (Corbetta 1999; Larsson 1993). In this sense, *interviewing* is a methodology characterized by a flexible framework that allows to investigate specific aspects of security awareness, including knowledge, with the preferred degree of detail. Figure 4 illustrates the corresponding radar plot. In a typical interview, the respondent is asked a set of questions in front of a single person, in an isolated and informal environment. In such a context, the interviewer plays an active role in orienting the focus of the questions on aspects or elements that emerges as more relevant or controversial (Gubrium and Holstein 2001). This kind of survey is not limited by a pre-arranged set of standard questions and allows to collect more information and gain precise insight on the actual expertise and knowledge of the respondent. On the other hand, as emphasized in the radar plot, interviewing has drawbacks in terms of timeline and practicality. Employees are interviewed one by one, which dilates

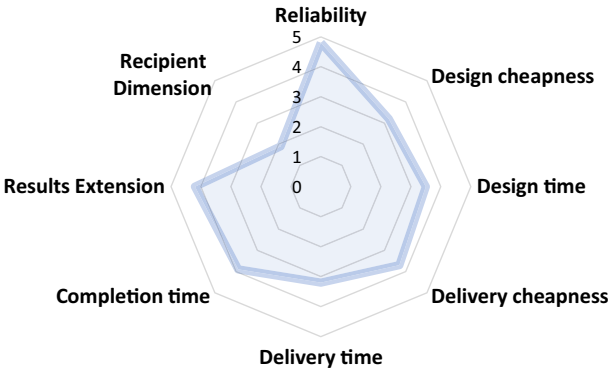

Fig. 4 Radar plot for interview method (Setola et al. 2015)

the time of execution and makes it problematic to include the whole staff within the recipient dimension which then results restricted.

Surveying the knowledge of employees is also a valuable tool for assessing the effectiveness of some campaigns to raise the SA level. For example, many organizations engage in activities such as training courses or other educational initiatives specifically aimed at increasing the staff knowledge and understanding of the security aspects (De Maggio et al. 2017).

However, implementing an informational program does not imply that the actual knowledge has increased (Peltier 2005). Establishing a *post-training test* can result to be advantageous not only because it indicates the acquired competencies and to some extent the security level reached after the attendance of the course, but it also provides a useful feedback to the senior management about the quality of the training course, its effectiveness and the toughest topics for the participants. The radar plot in Fig. 5 shows post-training tests to be an advantageous tool in terms of time consumption. Also, according to the recent experience of some companies, implementing tests right after training has a favorable cost and is time effective (Setola et al. 2015). However, post-training tests are not suitable for assessing the employees' general knowledge, but they rather focus on the specific objectives of the course. Investigating the level of preparation immediately after an educational campaign provides an overview of its short-term effectiveness but it does not take into account that notions learned might not have a long-term durability (Bulgurcu et al. 2010). Therefore, this kind of measurement might not be a reliable tool for assessing the actual level of knowledge in the long term.

5.2 Assessing Attitude: Using "Metadata" and Indirect Indicators

Assessing the attitude of employees toward SA, thus how they feel about security and security campaigns, is of utmost importance, but it results particularly difficult, as it is a non-tangible aspect that lies mostly in the psychological sphere. Little evidence of positive or negative attitudes can be found through the more classical measurement methodologies. For example, questionnaires, interviews, and tests are

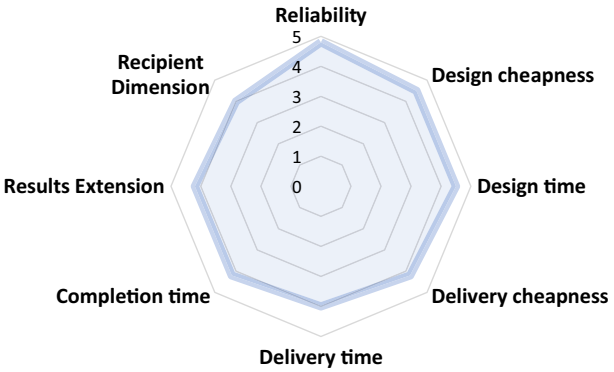

Fig. 5 Radar plot for post-training test method (Setola et al. 2015)

often employed as a principal and all-encompassing instrument for measuring the level of security awareness not only in relation to the component knowledge, but also for attitude (Velki et al. 2014), and surveys typically include questions such as "how your attitude to information security has changed over the past years?" or "do you consider your computer to be a valuable target to hackers?" (AFPPU 2009; SANS 2012). However, answers to these questions are not reliable enough to constitute a stand-alone indicator of positive attitude toward security awareness. In fact, employees showed the tendency to provide "expected" answers rather than "actual" answers. This is probably induced by the fear of potential repercussions and anonymity, which is strongly suggested in any survey, has the potential to decrease this phenomenon, but it is not incisive enough to overcome it. For example, in a study comparing the SA level in different organizations, Manke and Winkler found a considerable difference between the results of face-to-face interviews and those of questionnaires completed by the same responders: while 74% of employees gave positive feedbacks about their company's security policy in a written test, just the minority of them confirmed this positive judgment in front of the interviewer (Manke and Winkler 2012).

This shows that the answers collected through questionnaires, interviews, and tests, despite useful for a preliminary approach, are a superficial measurement when it comes to attitude and needs to be integrated. An interesting methodology for assessing the attitude of employees is through the analysis of "metadata". These are indirect indicators that can be extracted from other SA related activities. For example, the way in which the personnel engages in interviews, questionnaires, and tests discloses valuable insights on their consideration and commitment to security. Surveys can be analyzed by paying attention to data such as filling time, average time of submission, number of finalized tests, number and length of open questions answered, and number of hints and suggestions provided. In an average organization, the workload and tight timelines might make finalizing surveys an overburdening and demanding activity. For this reason, when initiatives of this fashion, despite not mandatory, are widely participated, and surveys are filled with meticulousness, it is an important signal of involvement and commitment of the staff, thus a proof of their positive attitude.

Similarly, useful indirect indicators for measuring the attitude can be collected during the execution of common programs to raise the company's level of SA.

For example, it is common to use the internal network to disseminate security policies or to publish short articles promoting upcoming security events or providing practical tips for endorsing a stronger level of security. This information is accessible to all the personnel and could, therefore, be exploited to indirectly monitoring the number of subjects that show interest in security-related material. The internal network can generate intranet push notices every time someone visits an article or click on a link about a specific topic. Figure 6 illustrates the corresponding radar plot. This method, in addition to being simple and cheap, has the advantage of being delivered to all the employees of an organization. Hence, the senior management can obtain a further element to judge the staff attitude. If SA contents receive great attention, it indicates the staff to feel involved in the security process and shows their willingness to contribute proactively.

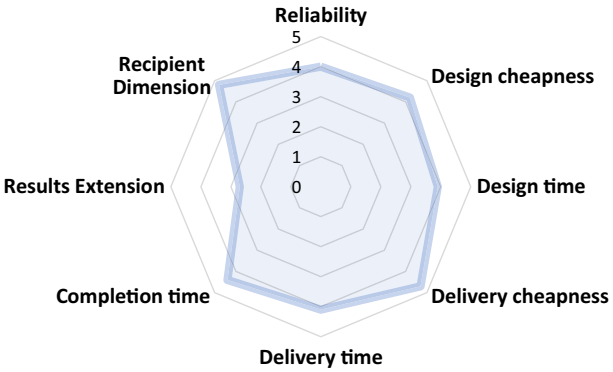

Fig. 6 Radar plot for intranet push notice method (Setola et al. 2015)

Online self-education programs are other initiatives that produce relevant indirect indicators. Self-education consists of a platform that employees access via the web and where they can autonomously manage the "study" of the security topic. This entails completing online courses, downloading materials watching videos, etc. From the online activity of the personnel, it is possible to extract insights of their attitude toward security awareness programs. Key questions could be how many people perform online courses? How often do they connect to the platform? How much time do they spend on it? Also, this monitoring system collects simultaneously data from several employees and the information has a digital format that can be easily processed for statistical purposes. On the other hand, organizations can engage in this kind of measurement only if they have already implemented online trainings. Collecting metadata is subordinate to the existence of e-learning platforms whose development is long and expensive. This in turn, as shown in the radar plot reported in Fig. 7, affects the economic impact and velocity of the method.

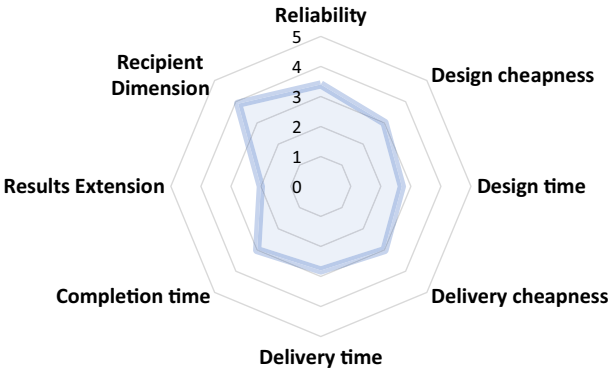

Fig. 7 Radar plot for online self-education method (Setola et al. 2015)

5.3 Assessing Behavior: Looking for a Practical Dimension

According to the National Institute of Standards and Technology (NIST 800-50), the final goal of SA programs is "to change behavior or reinforce good security practices" (Wilson and Hash 2003; Hansche 2001). Therefore, an accurate measurement must include methods specifically focused on the practical dimension of the security awareness. This entails monitoring and assessing how the personnel behaves and if they comply with the corporate policies and practices not only when managing critical operations but also in the everyday working routine.

To date, the most common way for the monitoring of the human factor is accomplished through forms of auditing, which consists of *investigating the occurred security breaches* in order to check to what extent the behaviors of employees resulted compliant with the existing security policies and procedures. Noncompliant behaviors can be indexed to form indicators of the current level of security awareness. Relevant information can be drawn from episodes like security incidents, reported incorrect behaviors, number and value of thefts, perimeter violations, virus infections, attempts to visit unauthorized websites, and attempts to access from unauthorized IP addresses (Peltier 2005; Kruger and Kearney 2006; Al-Awadi 2009). This approach is largely common because of its cheapness and low time consumption. In fact, the necessary information is automatically collected by the auditing department; hence, organizations do not need to engage in further activities that would increase both the budget and the workload.

However, basing the measurement on the monitoring of the past security breaches can create false confidence. In fact, the absence of incidents does not automatically depend on the organization's impeccable security standards, but it might instead mean that currently there are no real threats (Setola et al. 2015). For example, Edward Smith, Captain of Titanic, proudly declared his boat to be unsinkable as he had never experienced any serious incident in more than 50 years of navigations (Davie 1986). Also, this method does not take into account a wide spectrum of extremely rare events whose non-occurrence is not a direct consequence of high levels of security awareness, but it is rather connected to the low probability that a concatenation of adverse events takes place at the same time. Nevertheless, rare events pose a dormant but concrete threat and the incidents experienced by a single organization does not represent a solid body of analysis to assess whether the level of SA is suitable for mitigating the risks. This is reflected in Fig. 8. In fact, the radar plot for security incidents monitoring reveals positive performance in terms of costs and velocity but a poor reliability and result extension.

In other words, monitoring the security incidents is a useful differential indicator to evaluate the effectiveness of a security awareness initiative, but it does not provide an exhaustive measure of the real SA level. By comparing the trend of security breaches before and after having implemented a SA campaign, one can evaluate its success in relative terms, but in order to have a more consistent measurement, other tools need to be integrated. An accurate evaluation should take into account not only how the personnel behaved in the past incidents, but also how they would react and manage emergencies that have never occurred. To this purpose, organizations can take advantage of exercises such as *PC games*, *role games*, and *practice simulations*,

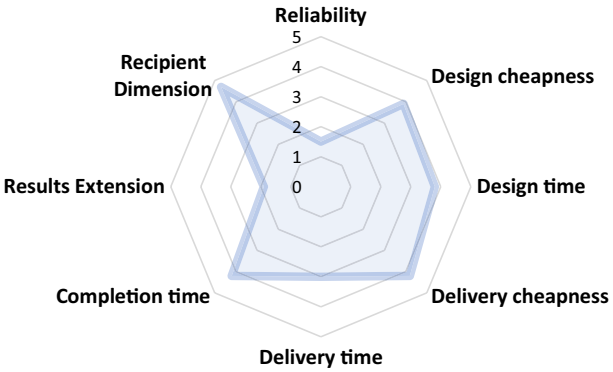

Fig. 8 Radar plot for security incidents monitoring method (Setola et al. 2015)

that recreate hypothetical (i.e., synthetical) scenarios in order to allow the staff to have a direct experience of a security breach.

The three exercises are different from each other but respond to the same ratio. *Practice simulations* (Fig. 9) reproduce with high realism specific events, *PC games* (Fig. 10) involve users in a virtual quest, while in *role games* (Fig. 11), participants are assigned a role to play in a defined problematic situation. The three exercises are aimed at questioning the ability of the participants to react to dangers and threats by translating into practice their knowledge of the security issue. In particular, these scenarios are specifically designed to test the staff capable of managing the risk appropriately and taking the correct actions to minimize damages and resume a quick recovery. As shown in the charts, role games and practice simulations present similar performances. They have the advantage to be highly reliable but require more time and investments. Also, they can be delivered to a small number of employees which determines a limited recipient dimension. On the contrary, PC games, despite less reliable, result to be of easier implementation, and thanks to their replicability, can be delivered to the totality of the staff with little marginal efforts.

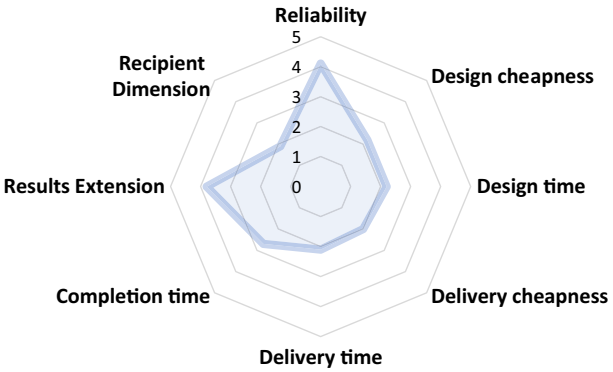

Fig. 9 Radar plot for practice simulation method (Setola et al. 2015)

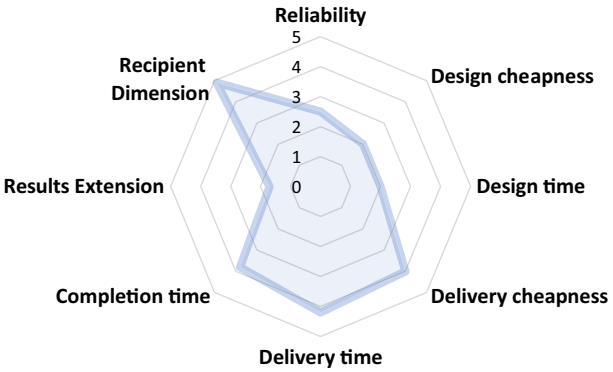

Fig. 10 Radar plot for PC games method (Setola et al. 2016)

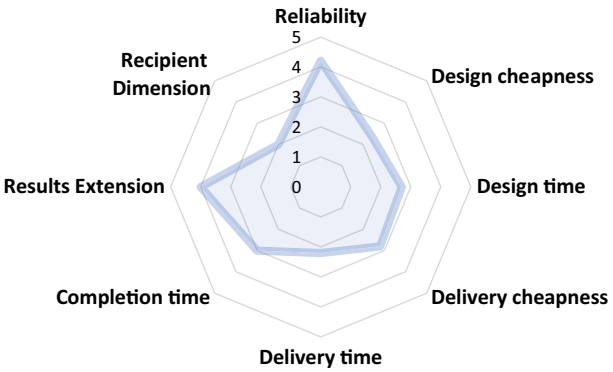

Fig. 11 Radar plot for role game method (Setola et al. 2015)

Practical exercises can be arranged to create a quantitative indicator. By assigning to the different steps of the simulation a symbolic numerical score, to each action and decision of participants can be given a bonus or a malus. Therefore, at the end of the exercise, it would be possible to evaluate their performance with an overall score. Afterward, the senior management appointed for the assessment of the security awareness could use this score to define a quantitative evaluation for each employee and process these data for further analyses, such as the trend of the security awareness in the last years, the variation of the security awareness level before and after the initiative, etc. (Setola et al. 2015; Pastor et al. 2010).

For better verifying the readiness of employees and maximizing the truthfulness of these exercises, it is of paramount importance that the simulation environment is designed to be as realistic as possible. This entails introducing elements of time and resource constraints as well as factors of unpredictability and hazard (Cone et al. 2007). Nonetheless, when designing a game or an emergency situation, it is difficult to consider all the possible threats, consequences and failures, thus testing will never simulate reality with perfect accuracy. Furthermore, as participants know they are

taking part in a game, their approach can be biased, which consequently might partially reduce the reliability of these measurement methods.

A way to overcome this problem consists of simulating *social engineering attacks*. Figure 12 presents the corresponding radar plot showing a solid threshold of reliability together with demanding levels of time and cost, and an optimal recipient dimension which comprehends between 11 and 30 individuals. This instrument allows companies to try their personnel's behavior without them knowing. Social engineering is "the art and science of getting people to comply with your wishes" and consists of gathering confidential information about the victim in order to influence their behavior and making them to perform specific actions that allow the attacker to proceed (Mitnick and Simon 2011; Granger 2001). In order to verify how employees deal with this threat the company can target them with a set of social engineering attacks. Simulated phishing tests is so far one of the most employed methods to assess how the personnel responds to an attack. This entails the company sending to its employees simulated malicious emails containing untrustworthy links, attachments, websites, or requesting sensitive information and then monitoring the consequent "click rate" (Williams et al. 2018). Despite the increasing emphasis on awareness and security trainings, employees' susceptibility to phishing remains a critical vulnerability. The 2016 data breach incident report (Verizon 2016) shows that 30% of employees involved in phishing test opened simulated suspicious message and 12% actually clicked on the malicious link. Similarly, a 2016 report based on 8 million simulated emails sent to 3, 5 million companies highlighted a "click rate" of approximately 20%, with 67% of the victim being recidivist thus likely to open malicious emails in the future (Computer Fraud and Security 2016). Interestingly, both studies highlight very tight timelines for the attacks to reach their goal. In fact, the median time for the first victim of a phishing test to open the malicious email is less than 2 min, and the median time to the first click on the corrupted link or attachment is below 4 min (Verizon 2016). Overall, 87% of the employees that failed the test opened the email on the day it was sent (Computer Fraud and Security 2016). On the one hand, this data shows that organizations have little time to proficiently individuate and respond to phishing campaigns. On the other hand, the

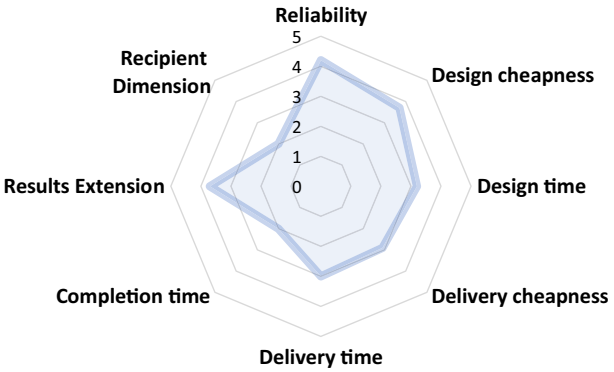

Fig. 12 Radar plot for social engineering attacks method (Setola et al. 2015)

human factor, despite its innate tendency to fail, seems once again the most efficient element of the security chain.

Simulated phishing campaigns are not the only method for a company to test its employees. This procedure can also be enlarged considering making phone calls or setting "critical" situations to check how employees react. For example, leaving some USB stick in the parking floor and checking if they introduce them in their PC (Setola et al. 2015). The organizations willing to engage in SA measurement of this fashion should consider the delicacy of these operations. It goes without saying that in order to gather genuine and unbiased data the personnel should not be aware of the ongoing test. On the other hand, operating in secret clashes with the necessity of building an open and trusted relationship within the company. In fact, such procedures might negatively affect the moral of employees who might feel tricked and kept under surveillance. Moreover, in some countries, such activities are considered illegal because they violate the employment protection legislation. In any case, it is strongly recommended to arrange this kind of monitoring activities with the cooperation of the unions and in compliance with regional regulations.

These methods focus on how employees act in response to security incidents, failures, and emergencies, but it does not take into account their conduct during the execution of standard operations. Security awareness behaviors do not include only best practices and procedures illustrating how to react to rare and critical situations, but they also refer to the everyday routine that characterizes everyone's professional life.

In other words, a fair measurement of an organization's SA level must also consider to what extent its staff respects the basic security rules and activities for maintaining a secure working environment during the ordinary course of daily operations. This aspect of security awareness can be deepened by conducting *walkabouts* (see Fig. 13 for the associated radar plot).

Walkabout is an activity that entails the patrolling of offices after the normal working hours, in order to verify whether the staff complies with the basic rules of the security behaviors. Key indicators could be, for example, offices locked and work stations secured, desks and cabinets locked, logout executed from IT devices, sensible information secured and recording media (CDs, USB drives, hard drives,

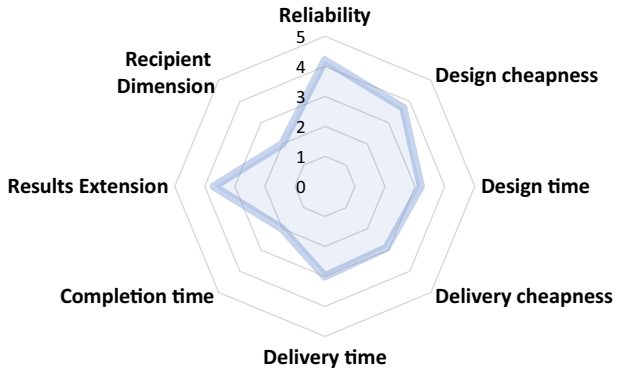

Fig. 13 Radar plot for walkabout method (Setola et al. 2015)

etc.) removed and correctly stored (Peltier 2005). The walkabout is a cheap method which requires low economic and organizational resources. It is sufficient to appoint a small number of people (depending on the size of the working spaces and of the organization) to perform the patrolling of the different offices with little impact on the working activities.

5.4 Measuring Security Awareness: Merging the Three Components

From our analysis, it has emerged that it does not exist an all-encompassing measuring instrument able to synthesize the concept of awareness in all its aspects, but rather each method allows to focus on specific and circumscribed areas (and subareas), namely knowledge, attitude, and behavior. Therefore, an organization willing to build a reliable and consistent assessment should adopt a combination of tools ensuring that the three components of the concept of awareness are represented. As discussed in the next section, the decision concerning which methods to adopt depends on the organizational characteristics of the subject engaging in the measurement.

6 Comparison of Security Awareness Measurements Methods

Due to the intrinsic complexity of the concept of security awareness, it does not exist a single method of measurement that can be considered as a silver bullet. The effectiveness of a measurement is not an innate characteristic of the employed tool, but rather depends on the specifications of the situation that one wishes to evaluate. As discussed in the previous section, each tool is suited to focus on specific aspects or components that together form the SA level. Organizations willing to evaluate the SA level of their staff need, before engaging in the measurement, to settle their objectives and prioritize the aspects they consider most relevant for their environment. For example, a plant operating in the energetic sector, in light of the recent cyber-attacks that caused outages in Ukraine in 2015 and 2016 (Lee 2017), might be more interested in settling a role game with a red team impersonating cyber attackers and a blue team the defenders, while a pharmaceutical plant would rather submit a quiz to its employees in order to verify their knowledge of physical security standards and procedures.

Also, the choice of the methods should be adequate to the structural characteristics of the company, such as its budget, audience, geographic dispersion, and urgency of the measurement. In fact, some methods require a very long time to be planned and accomplished, some easily scale with the dimension of the audience and some are doable only for small groups of people, preferably with a homogenous background and performing similar tasks. Finally, in any organization, the cost is a paramount factor to consider.

In other words, the "best" measurement strongly depends on both the company and the problem at hand. The set of indicators and description of each method introduced in the previous section can prove to be useful for identifying the most

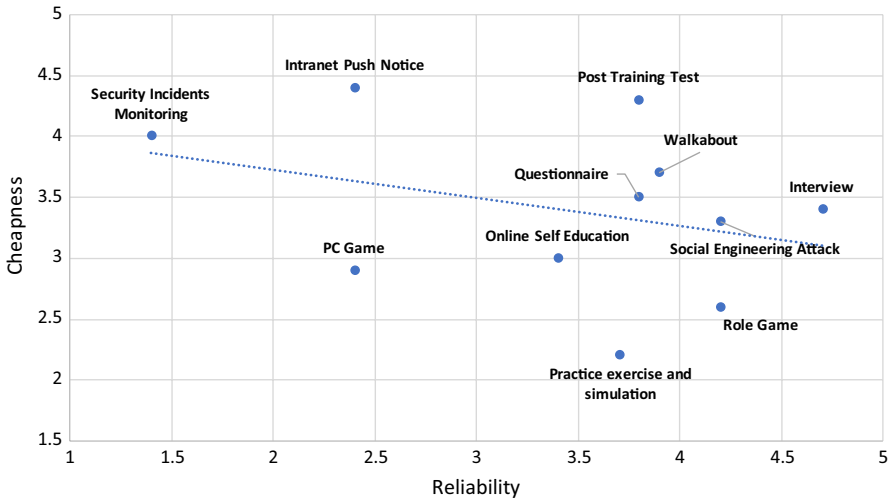

Fig. 14 Methods to measure the security awareness represented in their reliability and total cheapness

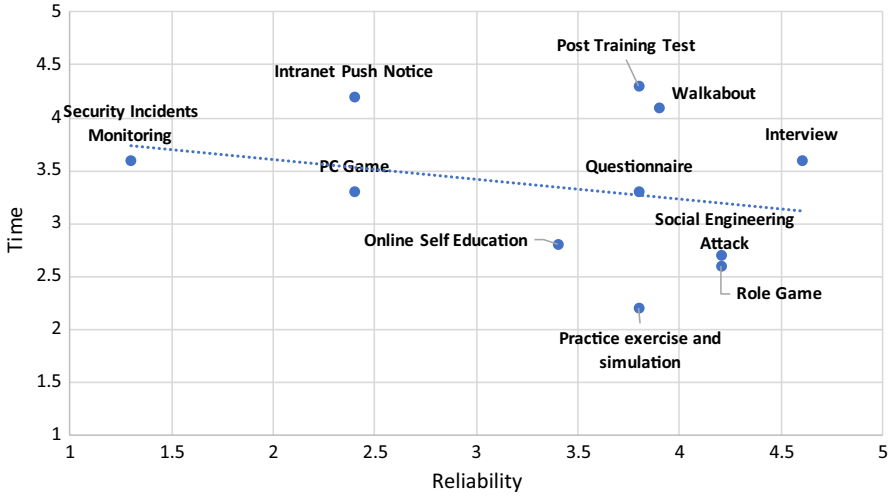

Fig. 15 Methods to measure the security awareness represented in their reliability and total time

convenient and suitable tool. These indicators allow us to compare the most relevant features of the different methods and thus provide a useful guide for companies that aim to implement a security awareness measurement campaign.

Figure 14 correlates the reliability of each method, defined as its capacity to generate unbiased and veracious results, with their total cheapness which includes both design and delivery costs. Similarly, Fig. 15 compares the reliability of the methods with the total time (design, delivery, and completion time).

If time and cheapness seem to be correlated, from the graphs, we can see that there is a weak degree of correlation between them and the level of reliability, which means that the most expensive and time-consuming methods are not necessarily the most accurate and unbiased. For example, it emerges that interviewing is a good compromise with a high rate of reliability and a level of costs and lengths, which does not seem to be prohibitive. Interviewing is a method that provides a general idea of the level of awareness, if instead a company has the need to measure the specific knowledge acquired during an initiative, the best method, in terms of resources and accuracy, appears to be the post-training test. Another interesting aspect refers to the relation between the parameters considered in the charts and the object that the different methods aim to evaluate. In fact, the tools to monitor knowledge and attitude are scattered in the upper half of Figs. 14 and 15 (except for online self-education, whose implementation depends on the previous development and delivery of e-learning platforms), indicating that they are, in general, more immediate to be implemented and with a more bearable economic impact. Also, in relation to knowledge and attitude, it does not seem that there is a correlation between the object of evaluation and the time and cheapness of methods. However, the instruments for monitoring attitude, such as intranet push notice, show a limited reliability. In fact, measuring what employees feel about a subject and to which level they feel involved in the security process is certainly more difficult and less precise. Nonetheless, it remains extremely important for the success of the whole SA campaign. For example, in an organization where the staff results sensible to the security topic an awareness campaign based on online self-education, characterized by great freedom and flexibility for the personnel to engage with, would produce better results than in an organization where the attention is low and the staff detached. On the contrary, the measurement tools for investigating the behavior of employees are concentrated in the lower-right of the charts (with the exception of incidents monitoring whose cost, time, and reliability is discussed in Fig. 8), which suggest that their implementation provide more accurate measurements but are also more time and resource consuming.

Figure 16 compares the popularity of each method with its completeness, calculated as the average between results extension and recipient dimension. Completeness refers to the capability of a method to collect a large amount of information and to include a large population in the measurement, while popularity provides a measure of how often the method has been adopted (De Maggio et al. 2017). The analysis shows that some of the most popular methods, i.e., post-training tests and interviews, are also among the most complete. However, the most interesting element is the correlation between the time and cheapness of the methods and their popularity. The three charts show the most employed evaluation instruments (questionnaire, post-training test, and interviews) are also among the less expensive and time consuming. This suggests that elaborating feedbacks on the effectiveness of a SA effort as well as evaluating the general awareness level is a practice strictly linked with the resources at hand. It shows that measurement activities are seen as a cost which burdens on the corporate budget rather than an investment for maximizing the effectiveness and efficiency of the management. It goes without saying that the first step for fostering awareness with well-tailored programs is the sensibilization of the

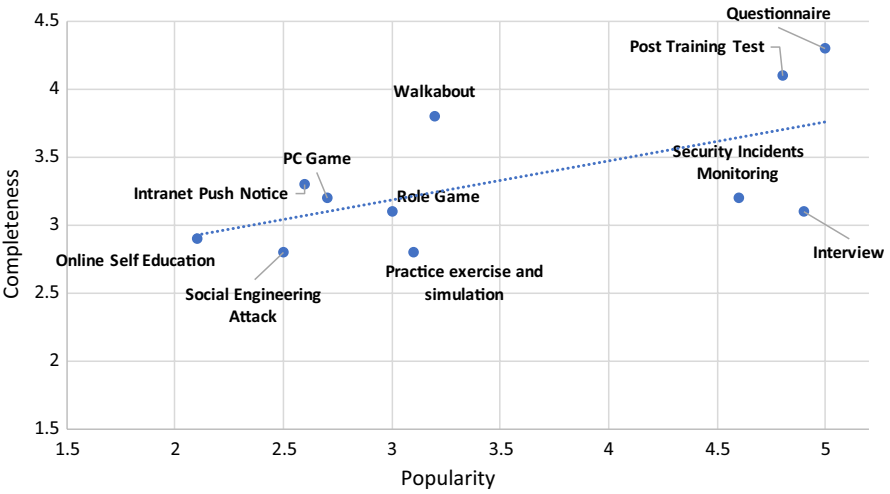

Fig. 16 Methods to measure the security awareness represented in their popularity and completeness

management in charge, which should allocate adequate resources. However, security investments result particularly hard to be justified as they aim to reduce loss rather than generate value. This implies a lack of tangible return on investment which has so far led companies to adopt compliance-oriented approaches. This is a detrimental trend for security as compliance does not equal good security. As emerged from interviews with 40 CISO, building a compliant profile is often reduced to put in place the strictly necessary security measures "to get a checkmark" and respect, with minimum spending, the existent regulations and best practice (Moore et al. 2015). Way more effective for enhancing and measuring awareness would be to set SA programs in the broader context of risk assessment. This entails analyzing how SA campaigns indirectly influence the overall risk considered as a combination of threat probabilities, vulnerabilities, and expected consequences. As reported in Soomro et al. (2016), the literature on this subject is still ongoing with the research mostly orientated toward quantitative security models for risk assessment (Ruan 2017). From this perspective, an interesting tool is the return of security investments (RoSI) which would help organizations to determine the cost-effectiveness of their SA programs as well as to justify the budget usage in front of the executive boarder (ENISA 2012). For example, in 2017, the Aberdeen Group elaborated a Montecarlo model, based on publicly available data, for calculating the RoSI of an awareness campaign specifically focused on phishing and spear-phishing attacks. According to their study, the investment in phishing SA programs would result in a median reduction in the annualized risk of such attacks of about 50% with a median annual return on investment of about 5 times. Also, the study estimates that the likelihood that the cost of the training will be inferior to the impact of phishing attacks is about 72% (Brink 2017).

Finally, from this graph, it emerges that the methods to assess knowledge are more popular than those to evaluate attitude and behavior. Questionnaire,

post-training tests, and interviews are concentrated on the right side of the chart. This discloses that the concept of security awareness is still strongly believed to be based on learning procedures. It also means that the majority of companies engaging in measurement activities underestimate the importance of including in their analysis how their employees feel about the SA campaign, and how it influences their behavior. In addition, the monitoring of security incidents is way more popular than the other methods to assess behavior. This shows that companies are less interested in monitoring how their personnel conduct operations in the everyday routine. This approach might result detrimental as the management of emergency situations is just an aspect of SA and relates to the capability of employees to react. However, it does not take into account their commitment in preventing major accident to occur, which is a crucial factor for securing organizations.

7 Conclusion

In conclusion, an element whose usefulness is only partly understood and certainly underestimated is the importance to perform measurements not only of the actual level of the security awareness inside an organization, but also of the effectiveness of the different SA programs. This gap has serious implications. In fact, the implementation of programs to increase the SA in most of the critical sectors turns out to be ineffective, and accidents caused by human errors, resulting from lack of knowledge, negligence or noncompliant behavior, still represent a large percentage. This article has argued that, for better measuring it, awareness has to be decomposed into three elements, namely knowledge, attitude, and behavior, each of which should be object of a separate evaluation with an ad hoc method. Also, the article has introduced a set of different measurement tools and has analyzed their strengths, weaknesses and to what particular aspects of awareness they can be applied in order to maximize the reliability of the overall measurement. The data collected and evaluated with these methods could be then exploited to design or revise the security awareness program and strengthen the weakest topics, which in turn would boost the security chain of any organization.

References

Abawajy J, Thatcher K, Kim TH (2008) Investigation of stakeholders commitment to information security awareness programs. In: 2008 international conference on information security and assurance (ISA 2008) IEEE, pp 472–476

Academic Frontier Project for Private Universities (2009) Survey on the internet security awareness. March. https://www.kansai-u.ac.jp/riss/en/shareduse/data/17_E_questionnaire.pdf. Accessed 4 Sept 2019

Agresti A (2018) An introduction to categorical data analysis. Wiley, New York

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

BBC News (2004) The Chernobyl disaster. BBC special reports. http://news.bbc.co.uk/1/shared/spl/hi/guides/456900/456957/html/nn1page1.stm. Accessed 4 Sept 2019

Bradburn NM, Sudman S, Wansink B (2004) Asking questions: the definitive guide to questionnaire design–for market research, political polls, and social and health questionnaires. Wiley
Bresz FP (2004) People—often the weakest link in security, but one of the best places to start. J Health Care Compliance 6(4):57–60
Brink DE (2017) Security awareness training: small investment, large reduction risk. Aberdeen Group. https://www.proofpoint.com/us/resources/analyst-reports/aberdeen-security-awareness-training. Accessed 4 Sept 2019
Brunner EM, Suter M (2008) International CIIP handbook 2008/2009. Center for Security Studies, ETH Zurich, Zurich
Bulgurcu B, Cavusoglu H, Benbasat I (2010) Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q 34(3):523–548
Byres E, Lowe J (2004) The myths and facts behind cyber security risks for industrial control systems. In: Proceedings of the VDE kongress, vol 116, pp 213–218
Caputo DD, Pfleeger SL, Freeman JD, Johnson ME (2014) Going spear phishing: exploring embedded training and awareness. IEEE Secur Priv 12(1):28–38
Choo KKR (2011) The cyber threat landscape: challenges and future research directions. Comput Secur 30(8):719–731
Computer Fraud & Security (2016) News—employees prone to phishing. Comput Fraud Secur 2016(1):3. https://doi.org/10.1016/S1361-3723(16)30004-5
Cone BD, Irvine CE, Thompson MF, Nguyen TD (2007) A video game for cyber security training and awareness. Comput Secur 26(1):63–72
Corbetta P (1999) Metodologia e tecniche della ricerca sociale. http://www.uniroma2.it/didattica/statistica_sociale_B/deposito/corbettametodologia_e_tecniche_della_ricerca_socialeriassunto.pdf. Accessed 4 Sept 2019
Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M, Baskerville R (2013) Future directions for behavioral information security research. Comput Secur 32:90–101
Das SK, Kant K, Zhang N (2012) Handbook on securing cyber-physical critical infrastructure. Elsevier, Amsterdam
Davie M (1986) The Titanic: the full story of a tragedy. Random House, London
Davis FD (1989) Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Q 13:319–340
De Maggio MC, Mastrapasqua M, Tesei M, Chittaro A, Setola R (2017) How to improve the security awareness in complex organizations. Eur J Secur Res 4:1–17
Durkheim É (1897) Le suicide: étude de sociologie. Alcan, Paris
ENISA (2012) Introduction to return on security investment. https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment. Accessed 4 Sept 2019
Furnell SM, Jusoh A, Katsabas D (2006) The challenges of understanding and using security: a survey of end-users. Comput Secur 25(1):27–35
Furnell SM, Bryant P, Phippen AD (2007) Assessing the security perceptions of personal Internet users. Comput Secur 26(5):410–417
Granger S (2001) Social engineering fundamentals, part I: hacker tactics. Secur Focus
Groves RM, Fowler FJ Jr, Couper MP, Lepkowski JM, Singer E, Tourangeau R (2011) Survey methodology, vol 561. Wiley, New York
Gubrium JF, Holstein JA (2001) Handbook of interview research: context and method. Sage Publications, Thousand Oaks
Hansche S (2001) Designing a security awareness program: part I. Inf Syst Secur 9(6):14–23
Herath T, Rao HR (2009) Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. Decis Support Syst 47(2):154–165
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
Information Security Forum (2014) From promoting awareness to embedding behaviours. https://www.securityforum.org/uploads/2015/03/From-Promoting-Awareness-ES-2014_Marketing.pdf. Accessed 4 Sept 2019
Karjalainen M, Siponen M (2011) Toward a new meta-theory for designing information systems (IS) security training approaches. Jo Assoc Inf Syst 12(8):518–555
Kruger HA, Kearney WD (2006) A prototype for assessing information security awareness. Comput Secur 25(4):289–296

Larsson R (1993) Case survey methodology: quantitative analysis of patterns across case studies. Acad Manag J 36(6):1515–1546
Lee R (2017) Crashoverride: analysis of the threat to electric grid operations. Dragos Inc., Rome
Mani D, Raymond Choo KK, Mubarak S (2014) Information security in the South Australian real estate industry: a study of 40 real estate organisations. Inf Manag Comput Secur 22(1):24–41
Manke S, Winkler I (2012) The habits of highly successful security awareness programs: a cross-company comparison. Technical report, secure mentem, 2012. http://www.securementem.com/wp-content/uploads/2013/07/Habits_white_paper.pdf. Accessed 4 Sept 2019
Mishra S, Dhillon G (2006) Information systems security governance research: a behavioral perspective. In: 1st annual symposium on information assurance, academic track of 9th annual NYS cyber security conference, pp 27–35
Mitnick KD, Simon WL (2011) The art of deception: controlling the human element of security. Wiley, New York
Moore T, Dynes S, Chang FR (2015) Identifying how firms manage cybersecurity investment. Southern Methodist University. http://blog.smu.edu/research/files/2015/10/SMU-IBM.pdf. Accessed 4 Sept 2019
Moteff J, Parfomak P (2004) Critical infrastructure and key assets: definition and identification. Library of Congress Washington DC Congressional Research Service
Muir A, Lopatto J (2004) Final report on the August 14, 2003 blackout in the United States and Canada: causes and recommendations
Murchison C (1935) A handbook of social psychology. Clark University Press, Worcester, pp 789–844
NIST (1998) Information technology security training requirements: a role-and performance-based model (supersedes NIST Spec. Pub.500-172), SP 800-16, March
Parsons K, McCormac A, Pattinson M, Butavicius M, Jerram C (2014) A study of information security awareness in Australian government organisations. Inf Manag Comput Secur 22(4):334–345
Pastor V, Díaz G, Castro M (2010). State-of-the-art simulation systems for information security education, training and awareness. In: 2010 IEEE education engineering (EDUCON). IEEE, pp 1907–1916
Patrick AS, Long AC, Flinn S (2003). HCI and security systems. In: CHI'03 extended abstracts on human factors in computing systems. ACM, pp 1056–1057
Peltier TR (2005) Implementing an information security awareness program. Inf Syst Secur 14(2):37–49
Perrow C (2011) Normal accidents: living with high risk technologies-updated edition. Princeton University Press, Princeton
Pescaroli G, Alexander D (2016) Critical infrastructure, panarchies and the vulnerability paths of cascading disasters. Nat Hazards 82(1):175–192
Pfleeger SL, Sasse MA, Furnham A (2014) From weakest link to security hero: transforming staff security behavior. J Homel Secur Emerg Manag 11(4):489–510
Ponemon Institute LLC (2012) The human factor in data protection. https://www.ponemon.org/blog/the-human-factor-in-data-protection. Accessed 4 Sept 2019
Rahim NHA, Hamid S, Mat Kiah ML, Shamshirband S, Furnell S (2015) A systematic review of approaches to assessing cybersecurity awareness. Kybernetes 44(4):606–622
Reason J (2000) Human error: models and management. BMJ 320(7237):768–770
Ruan K (2017) Introducing cybernomics: a unifying economic framework for measuring cyber risk. Comput Secur 65:77–89
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 (ed) Mathematical models for decision support. Springer, Berlin, pp 109–121
SANS (2012) Security awareness survey. Sans Institute, April. https://www.sans.org/sites/default/files/2018-01/security-awareness-survey.pdf. Accessed 4 Sept 2019
Schein EH (2009) The corporate culture survival guide, vol 158. Wiley, New York
Schultz E (2005) From the Editor-in-Chief: the human factor in security. Comput Secur 24(6):425–426
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. NITEL, March
Setola R, Rosato V, Kyriakides E, Rome E (2016) Managing the complexity of critical infrastructures. In: Janusz K (ed) Studies in systems, decision and control book series, vol 90. Springer, Berlin
Siponen MT (2000) A conceptual foundation for organizational information security awareness. Inf Manag Comput Secur 8(1):31–41

Siponen MT (2001) Five dimensions of information security awareness. SIGCAS Comput Soc 31(2):24–29
Siponen M, Pahnila S, Mahmood MA (2010) Compliance with information security policies: an empirical investigation. Computer 43(2):64–71
Solms BV (2000) Information security—the third wave? Comput Secur 19(7):615–615
Soomro ZA, Shah MH, Ahmed J (2016) Information security management needs more holistic approach: a literature review. Int J Inf Manag 36(2):215–225
Stone DH (1993) Design a questionnaire. BMJ 307(6914):1264–1266
Szilagyi AD, Wallace MJ (1983) Organizational behavior and performance. Good Year Books, Culver
Talib S, Clarke NL, Furnell SM (2010) An analysis of information security awareness within home and work environments. In: 2010 international conference on availability, reliability and security. IEEE, pp 196–203
Tsohou A, Kokolakis S, Karyda M, Kiountouzis E (2008) Investigating information security awareness: research and practice gaps. Inf Secur J Glob Perspect 17(5–6):207–227
US-Canada Power System Outage Task Force (2004) Final report on the August 14, 2003 blackout in the United States and Canada: causes and recommendations. US-Canada Power System Outage Task Force
Velki T, Solic K, Ocevcic H (2014) Development of users' information security awareness questionnaire (UISAQ)—ongoing work. In: 2014 37th international convention on information and communication technology, electronics and microelectronics (MIPRO). IEEE, pp 1417–1421
Verizon (2016) 2016 data breach investigations report. http://www.verizonenterprise.com/verizon-insights-lab/dbir/. Accessed 4 Sept 2019
Williams EJ, Hinds J, Joinson AN (2018) Exploring susceptibility to phishing in the workplace. Int J Hum Comput Stud 120:1–13
Wilson M, Hash J (2003) Building an information technology security awareness and training program. NIST Spec Publ 800(50):1–39
Workman M, Bommer WH, Straub D (2008) Security lapses and the omission of information security measures: a threat control model and empirical test. Comput Hum Behav 24(6):2799–2816
Zimmerman R (2004). Decision-making and the vulnerability of interdependent critical infrastructure. In: 2004 IEEE international conference on systems, man and cybernetics, vol 5. IEEE, pp 4059–4063