Measuring the security culture in organizations: a systematic overview of existing tools

Marlies Sas, Wim Hardyns, Karolien van Nunen, Genserik Reniers & Koen Ponnet

Security Journal

ISSN 0955-1662

Secur J
DOI 10.1057/s41284-020-00228-4

palgrave
macmillan

Security Journal
https://doi.org/10.1057/s41284-020-00228-4

ORIGINAL ARTICLE

Measuring the security culture in organizations: a systematic overview of existing tools

Marlies Sas[1,2] · Wim Hardyns[1,3] · Karolien van Nunen[1,4,5] · Genserik Reniers[1,4] · Koen Ponnet[6]

Abstract

There has been an increase in research into the security culture in organizations in recent years. This growing interest has been accompanied by the development of tools to measure the level of security culture in order to identify potential threats and formulate solutions. This article provides a systematic overview of the existing tools. A total of 16 are identified, of which six are studied in detail. This exploration reveals that there is no validated and widely accepted tool that can be used in different sectors and organizations. The majority of the tools reviewed use only a quantitative method; however, security culture includes very different domains and therefore a mixed-method approach should be used. In contrast to security culture, instruments for measuring safety culture are widely available, and with many similarities between these two domains it is possible that well-established tools for measuring safety culture could be adapted to a security environment.

Keywords Security culture · Organizations · Measuring instruments · Systematic overview · Organizational culture

✉ Marlies Sas
marlies.sas@uantwerpen.be

[1] Antwerp Research Group on Safety and Security (ARGoSS), University of Antwerp, Venusstraat 23, 2000 Antwerp, Belgium

[2] Research Group on Law Enforcement, University of Antwerp, Antwerp, Belgium

[3] Institute for International Research on Criminal Policy (IRCP), Ghent University, Gent, Belgium

[4] Safety and Security Science Group, TU Delft, Delft, The Netherlands

[5] Research Chair Vandeputte, University of Antwerp, Antwerp, Belgium

[6] Department Communication Sciences, IMEC-MICT-Ghent University, Gent, Belgium

Published online: 07 February 2020

Introduction

Prior to 2001 organizations generally paid little or no attention to security threats. However, the terrorist attacks on 9/11 instigated a shift, and the issue of security was suddenly much more important (Baybut and Ready 2003). Many business leaders focused on implementing new security technology, and paid less attention to the broader 'security culture' of their organization (Chia et al. 2003). However, the increased interest in security within organizations encouraged researchers to study this topic more in depth. They realized that an organization's security culture might play an important role in maintaining an adequate level of security in an organization (Andress and Fonseca 2000; Beynon 2001; Breidenbach 2000; Schwarzwalder 1999; von Solms 2000). For instance, Connolly (2000) argues that a strong security culture is needed to convince employees that security is an important issue, as it impacts the likelihood of a malicious attack. Vierendeels et al. (2018) believe that the success of security measures is related to the security culture of organizations. According to Da Veiga and Martins (2015), a strong security culture enables members of an organization to behave in a more secure way in order to reduce security incidents.

Despite substantial interest in the subject, researchers struggle to agree on what factors or constructs constitute a security culture, and how it can be established (Alnatheer et al. 2012; Schlienger and Teufel 2003). A number of authors suggest that a security culture must be regularly modified to ensure that it constantly corresponds with the goals of an organization (Kruger and Kearney 2006; Martins and Eloff 2002; Schlienger and Teufel 2003). They emphasize the importance of repeated measurement in order to propose recommendations that establish, improve, and maintain a strong security culture (Chia et al. 2003). Unfortunately, very little research has been carried out into how organizational security culture should be evaluated (Chia et al. 2003), and only a few measuring tools have been created worldwide (Schlienger and Teufel 2005).

Effective tools for measuring organizational security culture enable businesses to uncover critical issues and risk areas, formulate recommendations, and implement improvements over time. Therefore, an overview of the tools that are currently available could provide useful insights for practitioners and highlight areas for further research (Chia et al. 2003). While van Nunen et al. (2018a) have explored the tools used and developed in Belgian organizations to measure safety culture, an overview of the existing instruments that measure security culture is lacking. Therefore, the aim of this paper is to provide a systematic overview of the science-based instruments that are used to assess security culture within organizations worldwide. Below, we first give an overview of the state-of-the-art insights into security culture. We then provide information about the methodological approach of our systematic review, followed by a comparison of the characteristics of the measuring tools that have been reviewed. Finally, we discuss the findings and provide recommendations for organizations and future research.

Security culture

Lundy and Cowling (1996) argue that security culture can be seen as a subculture of the organizational culture. The latter can, in simplest terms, be described as *"the way things are done in an organization"*. According to Schein (2009, p. 27), organizational culture is "a pattern of shared tacit assumptions that is learned by a group". When developed well, this can solve internal and external organizational problems. Nosworthy (2000) argues that organizational culture has a strong impact on security culture. A first definition of security culture was formulated within the domain of information security by Schlienger and Teufel (2003, p. 405), who stated that security culture is "all socio-cultural measures that support technical security measures". Malcolmson (2009, p. 361) presented a more extensive definition, arguing that "security culture is indicated in the assumptions, values, attitudes and beliefs, held by members of an organization, and behaviors they perform". Importantly, security culture should not be confused with the security climate, which refers to employees' shared perceptions about the organization's security policy. The security climate should therefore be seen as a part of the whole security culture of a company (Vierendeels et al. 2018).

A distinction can be made between information security, such as the protection of computer networks and the data therein, and physical security, such as the protection of infrastructure and employees. According to van Niekerk and von Solms (2005), who based their ideas on Schein's (2004) model of organizational culture, information security culture consists of four levels: (1) artifacts, (2) espoused values, (3) shared tacit assumptions, and (4) information security knowledge. The artifacts reflect the visible and measurable security aspects in an organization, such as the behavior of employees, security handbooks, or technology. Espoused values are a partially visible layer of security culture, such as the goals, strategies, or documents that describe the principles and values of the company. The shared tacit assumptions form the core of the organization's culture when the values and beliefs of the organization become shared. The fourth level, information security knowledge, supports the other three levels. According to the authors, in order to create a strong security culture, employees need to have enough security knowledge, they need to know the security needs of the organization, and they need to be aware of why security measures have been taken (van Niekerk and von Solms 2005). Other researchers (Schlienger and Teufel 2005; Vroom and von Solms 2004; Zakaria 2004) also link their model of security culture to Schein's (2004) organizational model and identify similar aspects of information security culture.

Focusing on physical security culture in chemical plants, Reniers and Dullaert (2007) identify three crucial domains: people, procedures, and technology. They argue that the *people* domain comprises individuals' ideas about the organization's security and the way they handle security. The *procedures* domain refers to the measures that are implemented to safeguard the security of the organization. Finally, the *technology* domain comprises the technical devices used to protect company from criminal acts. Starting from the same theoretical foundation

as Reniers and Dullaert (2007), a more elaborate description of physical security culture is proposed by van Nunen et al. (2018b), who focus on the similarity between aspects of a safety culture presented in The Egg Aggregated Model (TEAM) (Vierendeels et al. 2018). According to the authors, both safety and security culture can be separated into three domains: technological, organizational, and human (see Fig. 1). Focusing on security culture, the technological domain consists of aspects such as the security technology, equipment, and material of the organization. The organizational domain comprises the security policy, the resources available for security, and the security management. Finally, the human domain contains aspects such as security knowledge, attitudes, priorities, decisions, and the behavior of employees. Van Nunen et al. (2018b) argue that the organizational and human domains are manifested at two levels. At the first level are the observable security aspects that are noticeable when walking around the company. The second level consists of the non-observable, or not immediately apparent, aspects of security that can still be measured. In contrast to the organizational and human domain, the technological domain comprises only observable aspects of security.

In addition to the aspects related to the characteristics of the organization, the influence of external factors is emphasized. Factors such as the socio-economic status, level of technological development, or regulations and legislation of the country or region where the organization is based affect its security culture. Security culture is also determined by the security threats, such as theft, terrorism, or espionage, that an organization is exposed to. Organizations'

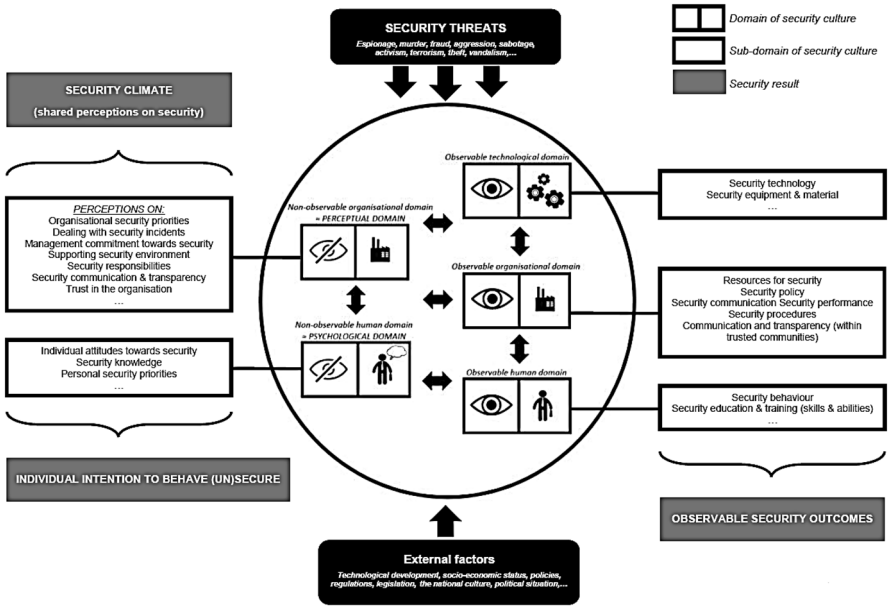

Fig. 1 An integrative conceptual framework for physical security culture in organizations (van Nunen et al. 2018b)

vulnerability to these threats differs depending on the company's characteristics. For instance, nuclear companies are more vulnerable to terrorism or activism, whereas in the financial sector security threats such as fraud or theft are more prominent.

When measuring security culture, van Nunen et al. (2018a) recommend a multi-method approach in order to take into account the technological, organizational, and human aspects. The authors argue that quantitative methods such as questionnaires are needed to measure the non-observable domains of security culture, for instance the security knowledge of employees. Qualitative tools such as observations, interviews, or focus groups are required to measure the observable security domains, for instance the written security procedures. Qualitative methods can also provide a broader view of the non-observable aspects, such as the management's security priorities. Alvesson and Berg (1992) point out that qualitative and quantitative methods have both weaknesses and strengths, and therefore a mixed-method approach should be used to measure the security culture in depth. The International Atomic Energy Agency (IAEA) (2017) agrees, and states that a triangulated approach is needed to gather data from multiple points of reference. For instance, surveys could be followed by interviews to clarify ambiguities and fill in possible gaps.

Despite researchers' increased interest in security culture, there is no widely accepted or validated tool available for measuring security culture within different kinds of organization. However, a few researchers have developed tools that measure culture within a specific security domain. As part of this study, in order to get a clear view of the different approaches, a systematic overview was conducted. It was hoped that identifying the characteristics of current measuring tools would enable researchers and organizations to gain more insight in order to develop a standardized and validated instrument. The methodological approach used for the systematic overview is presented below.

Methodology

Search strategy

Two online databases, Google Scholar and Web of Science, were searched for measuring tools. The following keywords were used: [instrument OR survey OR measuring tool OR assessment OR questionnaire] AND [security OR security culture OR security behavior OR security climate]. In addition, other relevant studies were retrieved by manually screening the references of all the full-text articles that were included in the study. When necessary details about a measuring tool were missing in the article or related studies, the developer of the tool was contacted via email in order to gather more information. No limits were put on where or when studies were conducted. However, as research on security culture is still at an early stage, only studies between 2000 and 2019 were found and selected.

Inclusion criteria

Studies were selected for inclusion by reviewing each article for its relevance and content. The inclusion process was based on five criteria:

(1) A focus on security culture: Because numerous researchers argue that security awareness should be seen as only a part of the security culture (Alnatheer et al. 2012; van Niekerk and von Solms 2005), studies from authors who indicate that they only focus on security awareness among employees of an organization were excluded from the review.
(2) Original tool: Only articles that contain a description of a tool by its original developers are included in the review. Studies containing information about a tool developed by someone other than the article authors were excluded. In such cases, the original tools were checked for their relevance to this study.
(3) Sufficient information about the content of the instrument: The article must contain sufficient, and detailed, information about the content and application of the measuring tool, to enable this study to provide a comprehensive overview of the different options. Articles that contain only limited details, even after contacting the author, were excluded.
(4) Possible applications of the tool: Because this article aims to give an overview of the existing tools within very different security domains, it is important that a specific comparison is possible. For instance, Maidabino and Zainab (2011) developed a tool that can only be used to measure the security culture in libraries, so its application possibilities are limited to one specific sector. Only studies that provide a tool with more or less generalizable content were included.
(5) Practical approach: In order to understand how the tool can be used in practice, only articles that contain a clear description of the application process are included. Solely theoretical approaches were excluded.

Results of the search

In total, 12 tools were retrieved during the search using the keywords, while four other relevant studies were retrieved by manually screening the references of all the full-text articles included in the overview (see Fig. 2). Application of the inclusion

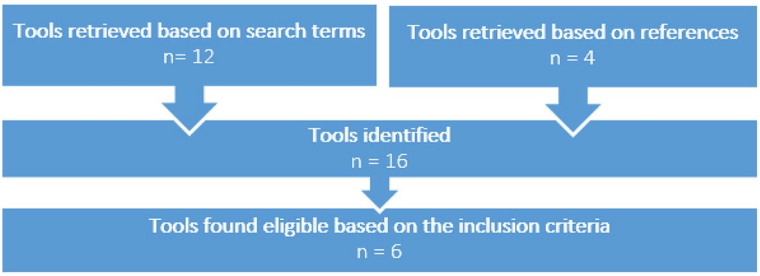

Fig. 2 Results of the search for security culture measuring tools

criteria resulted in a number of exclusions. Four tools were excluded because of their narrow focus on security awareness instead of security culture (criterion 1). One tool was excluded because the tool had been created by someone other than the article authors (criterion 2). Two tools were excluded because of a lack of sufficient information about the content of the instrument (criterion 3). One tool was excluded because the tool could not be generalized to other situations (criterion 4). Two tools were excluded because they were solely theoretical (criterion 5). In the end, six tools were eligible for inclusion in the systematic overview.

Information collected per tool

Table 1 provides an overview of the general characteristics of the reviewed tools. Firstly, the domain the instrument was developed for is specified. Next, the key indicators of each tool are listed; this shows which aspects of a security culture the developers of the tool have prioritized. Details about the theoretical foundation of the tool are included, followed by the main objectives of the instrument.

In order to understand the practical application of the tool, the methodological strengths and limitations of its reliability and validity are presented. The table specifies whether a multi-method approach was applied and, when a questionnaire was used, the type of survey, number of items, type of answers and target population. For tools that required a qualitative approach, the target population of the interviews or observations is included. These methodological characteristics are presented in Table 2.

Results

General characteristics of the tools

Based on the systematic overview, it is clear that the tools only focus on two security domains. Four of the six included instruments were specifically developed to measure information security culture within organizations, while the other two measure physical security culture. The information security domain has a predominant position within research on security culture; as organizations rely ever more heavily on technology to run their businesses, so interest in information security has rapidly increased (Kruger and Kearney 2006).

A more detailed analysis of the measuring tools shows that the authors emphasize similar aspects of the security culture within organizations. Based on the TEAM model of Vierendeels et al. (2018), security culture consists of both observable and non-observable security domains. A comparison of the tools' key indicators shows that they all aim to measure the non-observable security domain, which includes the security climate or shared security perceptions and individuals' views on security. For instance, Alnatheer et al. (2012) focus on the security climate by measuring top management involvement in information security and who is responsible for security. Schlienger and Teufel (2003) include the company's perceptions of security as

Table 1 General characteristics of the measuring tools

	Analyzing Information Security Culture (Schlienger and Teufel 2003)	Self-assessment of nuclear security culture in facilities and activities (International Atomic Energy Agency 2017)	A WINS international best practice guide for nuclear security culture (World Institute for Nuclear Security 2011)	Information Security Culture (Martins and Eloff 2002)	Understanding and measuring information security culture (Alnatheer et al. 2012)	Organizational Information Security Culture Assessment (AlHogail and Mirza 2015)
Domain	Information security	Physical security	Physical security	Information security	Information security	Information security
Key indicators	– Artifacts (e.g., behavior, technology, security handbooks) – Official values (i.e., the perception of the company on security) – True values (i.e., the individual attitude towards security)	– Beliefs and attitudes – Principles for guiding decisions and behavior – Leadership behavior – Management systems (e.g., processes, procedures, programs) – Personnel behavior	– Beliefs, principles and values – Characteristics (e.g., leadership, accountability, competency) – Documented expectations (e.g., security policy, responsibilities) and behaviors	– Organizational level: policy, benchmarking, risk analysis and budget – Group level: management and trust – Individual level: awareness and ethical – Change	– Top management involvement in information security – Information security policy enforcements – Information security training – Information security awareness – Information security ownerships	– Strategy (S) (e.g., policies, guidelines, best practices) – Technology (T) (e.g., hardware, software, services) – Organization (O) (e.g., beliefs, values, norms) – People (P) (e.g., behavior of employees) – Environment (E) (e.g., national culture, ethical conduct, legal systems)

Table 1 (continued)

	Analyzing Information Security Culture (Schlienger and Teufel 2003)	Self-assessment of nuclear security culture in facilities and activities (International Atomic Energy Agency 2017)	A WINS international best practice guide for nuclear security culture (World Institute for Nuclear Security 2011)	Information Security Culture (Martins and Eloff 2002)	Understanding and measuring information security culture (Alnatheer et al. 2012)	Organizational Information Security Culture Assessment (AlHogail and Mirza 2015)
Theoretical foundation	Schein's model of organizational culture (2004)	Schein's model of organizational culture (2004) (questionnaire)	No details are given	Information Security Culture Framework from Da Veiga and Eloff (2010)	Model developed by Alnatheer et al. (2012)	Framework developed by AlHogail (2015) and based on STOPE development profile (Bakry 2003), Human Factor Diamond Framework (AlHogail and Mirza 2015) and Information security culture change framework (AlHogail and Mirza 2014)
Main objectives	Measurement and improvement of security culture	Measurement of security culture	Measurement and improvement of security culture	Measurement and improvement of security culture	Measurement of security culture	Measurement and improvement of security culture

Table 2 Methodological characteristics of the measuring instruments

	Analyzing Information Security Culture (Schlienger and Teufel 2003)	Self-assessment of nuclear security culture in facilities and activities (International Atomic Energy Agency 2017)	A WINS international best practice guide for nuclear security culture (World Institute for Nuclear Security 2011)	Information Security Culture (Martins and Eloff 2002)	Understanding and measuring information security culture (Alnatheer et al. 2012)	Organizational Information Security Culture Assessment (AlHogail and Mirza 2015)
Reliability and validity	– Tool consists of a multi-method approach. – No formal guidelines or established framework was used when conducting the interviews, document analysis and observations (difficult to repeat the exact same assessment in other organizations or by other researchers)	– Tool consists of a multi-method approach – No scientific results available about the validation of the instrument	– Tool can be used by different nuclear companies. The WINS practice guide contains supporting guidelines for organizations – No use of multi-method approach – Not clear on what theoretical or practical basis the tool has been developed – No scientific results available about the validation of the instrument	Good scores on reliability and validity (verified by authors)	– The development of the tool is well substantiated by using a mixed-method research design – Process for deriving the questionnaire items was relatively subjective – Tool is developed for Saudi Arabia. It is not known whether the tool can be used in other settings	– Tool shows good scores on reliability and validity (verified by authors) – Tool is developed for a developing country. It is not known whether this tool can be used in other settings
Measurement approach	Questionnaire + interviews + document analyses + observations	Questionnaire + interviews + document analyses + observations	Questionnaire	Questionnaire	Questionnaire	Questionnaire
Type of questionnaire	Self-assessment	Self-assessment	Self-assessment	Self-assessment	Self-assessment	Self-assessment
Number of items	42	25–35	52	45	19	79

Table 2 (continued)

	Analyzing Information Security Culture (Schlienger and Teufel 2003)	Self-assessment of nuclear security culture in facilities and activities (International Atomic Energy Agency 2017)	A WINS international best practice guide for nuclear security culture (World Institute for Nuclear Security 2011)	Information Security Culture (Martins and Eloff 2002)	Understanding and measuring information security culture (Alnatheer et al. 2012)	Organizational Information Security Culture Assessment (AlHogail and Mirza 2015)
Type of answers	Three answer options (true-false-I don't know)	Seven point and eleven point Likert scale (strongly disagree–strongly agree)	Five point Likert scale (strongly disagree–strongly agree)	Five point Likert scale (strongly disagree–strongly agree)	Five point Likert scale (strongly disagree–strongly agree)	Two point and five point Likert scale (strongly disagree–strongly agree)
Target population	– Questionnaire: employees from different job levels. – Interviews: Chief Security Officer – Observations: employees from different job levels	– Questionnaire: employees from different job levels – Interviews: employees from different job levels – Observations: employees from different job levels	Questionnaire: employees from different job levels	Questionnaire: executive and senior managers, department managers and supervisors, operational job staff and technology staff	Questionnaire: employees of private, public, non-profit and semi-public Saudi Arabian organizations from different job levels	Questionnaire: employees from different job levels of Saudi Arabian organizations

a key indicator in order to assess shared security perceptions. To measure individuals' mindsets on security issues, IAEA (2017) focuses on employees' beliefs and attitudes, while WINS (2011) included employees' beliefs, principles, and values as a key indicator.

The security culture also consists of an observable domain, which includes organizational, human, and technological security aspects (Vierendeels et al. 2018). The overview revealed that all instruments aim to measure organizational security aspects. Martins and Eloff (2002) include the organizational security policy and budget as key indicators, while AlHogail and Mirza (2015) focus on the security policies, guidelines, and best practices with their key indicator strategy. Subsequently, each tool focuses on human aspects or the security behavior of employees. For instance, IAEA (2017) measures personnel behavior and Schlienger and Teufel (2003) include the indicator artifacts which also include the behavior of employees. In contrast to the organizational and human domains, only half of the tools included key indicators to measure technological security measures. While Martins and Eloff (2002), AlHogail and Mirza (2015), and Schlienger and Teufel (2003) explicitly mention that they measure the technological security aspects of the organization, Alnatheer et al. (2012), IAEA (2017) and WINS (2011) do not focus on any technological aspects. Although IAEA (2017) indicates that the human and organization aspects are inextricably linked to the technological measures, the tool does not assess the technological aspects. Finally, only AlHogail and Mirza (2015) focus on the impact of external security aspects, such as national culture, laws, and regulations on the security culture of the organization, while other tools only focus on internal security aspects.

The majority of the instruments are based on a theoretical concept. For instance, both Schlienger and Teufel (2003) and the IAEA (2017) created their tool based on the model of organizational culture developed by Schein (2004). Martins and Eloff (2002) use the framework of Da Veiga and Eloff (2007) as a foundation for their instrument. Only Alnatheer et al. (2012) and WINS (2011) combine theoretical insights with experiences and expertise from practitioners in the development of their tool.

Finally, when analyzing the main objectives of the measuring instruments, it becomes clear that only half focus explicitly on improving the security culture by formulating specific recommendations. For instance, WINS (2011) and Martins and Eloff (2002) state that goal of their measuring process is the formulation of well-founded recommendations. In contrast, IAEA (2017) and Alnatheer et al. (2012) emphasize the measuring process without making specific recommendations based on the results.

Methodological characteristics of the tools

Only Schlienger and Teufel (2003) and IAEA (2017) make use of a multi-method approach to assess security culture, with the other tools only including a questionnaire. When analyzing the methodological strengths and limitations of the reliability and validity of the tools, the use of a multi-method approach can be seen as a strength.

Although questionnaires can be used to measure the security climate of an organization, qualitative methods are vital to obtain a clear picture of the whole security culture. For instance, our comparison of the tools' key indicators showed that they all emphasize employee behavior. However, depending on the methodological approach used, different forms of behavior will be measured. When the instrument only includes a quantitative approach, such as a survey, the focus is on self-reported behavior. When qualitative methods such as observations are used, the actual behavior of individuals can be observed and measured. While it can be very time-consuming and difficult to observe behavior in various situations, a combination of two methods would provide a more global view of individuals' security behavior. For instance, Schlienger and Teufel (2003) conduct unstructured interviews with the chief security officer of an organization, and IAEA (2017) proposes a semi-structured approach that includes staff members from the entire organization. Both use document analysis to obtain an overview of the organization's security policy and carry out audits to verify the answers provided by respondents, and to get a deeper insight into their actual behavior. Although IAEA (2017) emphasizes the importance of formal guidelines when carrying out the interviews, document analysis, and observations, Schlienger and Teufel (2003) did not use any formal guidelines when conducting these qualitative methods. Unfortunately, this makes it very difficult to repeat the exact same approach in other settings or by other researchers.

According to the articles' authors, most of the tools show good results on reliability and validity. Although the tools already contain numerous strengths, the developers themselves indicate that some adjustments still have to be made in order to fully develop them. For instance, Alnatheer et al. (2012) developed a tool for measuring the information security culture in Saudi Arabian companies, and it is not clear whether the tool could be used in other countries. The authors indicate that the business environment of Saudi Arabia is different from that of Western countries. While Saudi Arabian information technology companies are still developing, most international information security standards are written from the perspective of more technologically advanced Western countries. The different technological levels combined with the cultural differences between Western countries and Saudi Arabia cause challenges when implementing the same measuring tool in both contexts.

When a questionnaire is included in these measuring tools, it is always as a self-assessment. The number of items varies between 19 and 79. Alnatheer et al. (2012) have developed the shortest questionnaire (19 items), while AlHogail and Mirza (2015) have expanded their survey to 79 items. Five of the six questionnaires utilize a Likert scale. Only Schlienger and Teufel (2003) use a categorical answering scale with the options 'True,' 'False,' or 'I don't know.' Employees from different job levels are included in the research samples. For instance, WINS (2011) gathers data from staff at all levels, including the board of directors.

Conclusion and discussion

This article identified and analyzed tools that measure organizational security culture. Six tools were eligible for inclusion in the systematic overview. It was found that the tools focus on two security domains, namely information security and physical security. The tools were compared based on their general characteristics and methodological approach. While they all included similar key indicators, notable differences were found in their methodology.

As has already been mentioned, a common view on or widely accepted theoretical approach to security is lacking. While some researchers and practitioners do get involved in the debate about security culture, their attention is focused on certain security domains (e.g., information security) and sectors (e.g., nuclear companies). Indisputably, in scientific research, information security culture holds a dominant position. Despite the actual threats related to information security, the vulnerability of organizations to other threats, such as terrorism, cannot be underestimated. For companies to prevent and be prepared for threats related to security, more research about physical security culture is needed.

Additionally, there is no widely accepted and consolidated approach or unique toolset available that can be used in different sectors or by different organizations (Schlienger and Teufel 2003). Therefore, a standardized measuring tool needs to be developed. Collaboration between researchers and practitioners is required in order to create a strong, practical-based instrument that can be validated in scientific research. By adjusting the tool to the characteristics of the company in the preparation phase of the measuring process, a standardized instrument could be used by different organizations and sectors. As the overview showed that tools that only measure information security or physical security contain similar key indicators, an instrument that combines these two security domains could readily be developed. Most importantly, a tool must be adaptable to an organization's specific characteristics. For instance, different organizations are more or less exposed to security threats, so this should be taken into account in the developing process. This means that a one-size-fits-all approach must be avoided. Additionally, there are some benefits for benchmarking when different organizations use the same instrument and the results can be compared. The insights obtained by a company comparing its results to those of a similar one can enable it to improve its security culture.

In creating a standardized instrument, much can be learned from adapting the knowledge about safety culture to the measurement of security culture. In contrast to the limited number of tools that are currently available to measure security culture, several tools already exist to measure safety culture. While safety and security were long seen as independent of each other, more recent research shows that there are a lot of similarities between these domains (Kria et al. 2015; van Nunen et al. 2018b). Both domains focus on the prevention of undesirable events, such as injuries to people, and material or environmental damage. The main difference is in the origin of these events—damage is unintentional in the field of safety and intentional in the case of a security incident. Additionally, there is a

difference between risks related to the domain of safety and threats in the field of security. As safety risks are mostly rooted inside the organization and therefore are well known, security threats are predominantly rooted outside of the organization and are more difficult to uncover. The greatest similarity is that both safety and security are part of the overall culture of the organization. This implies that a focus on the technological, organizational, and human aspects in both fields is needed to ensure an integrated and strong organizational culture (van Nunen et al. 2018b). Therefore, it can be useful to consider to what extent the existing tools for measuring safety culture can be applied to the security context. Adjustments or additions could be made to preexisting tools by altering the aspects included in the tool to the different aspects of a security culture. This process would result in the creation of a measuring tool for security culture based on an already existing framework developed for measuring safety culture.

Recommendations

Based on the systematic review, some recommendations can be made about creating an effective tool for assessing the security culture within an organization.

Firstly, a multi-method approach should be used, as it provides a more detailed picture of the security culture of an organization. All tools in the systematic review used a quantitative approach, while only two add qualitative methods. Due to their statistical robustness, questionnaires can be included without major costs (Da Veiga 2008). Additionally, completing the survey could create more security awareness among employees. On the other hand, as there is no certainty as to how respondents interpret the specific questions, the reliability of this method remains uncertain. In contrast, qualitative methods have the benefit of revealing more detailed insights in the results (Kaplan and Duchon 1988), but also have their limits, especially in terms of generalizability and time (Alvesson and Berg 1992). Considering both the weaknesses and strengths of qualitative and quantitative methods, it is believed that a multi-method approach is needed to measure security culture (Alvesson and Berg 1992). As the results of one method can be verified with those of other approaches, there are greater opportunities for data analysis (Schlienger and Teufel 2005). Additionally, the researcher is able to explore different points of view when interpreting the results (Fleeger 1993). Considering the very different domains of a security culture, it is recommended that both quantitative and qualitative methods be used. For instance, while data about the observable security aspects can be gathered through qualitative methods such as interviews, focus groups, document analyses, or observations, a quantitative approach is needed to explore employees' perceptions of security issues (van Nunen et al. 2018b). The multi-method approach makes the measuring process more time-intensive, but ensures a more detailed and realistic result that can be translated into substantiated recommendations for the organization. As culture has a very comprehensive structure, it is impossible to measure it well in a short period of time.

Secondly, it is recommended that the entire organization should be involved in the measuring process. Numerous authors argue that the involvement of both staff

and top management is necessary to measure and improve a security culture (Chia et al. 2003; Da Veiga and Eloff 2007; Kraemer et al. 2009; Schlienger and Teufel 2003). As cultural change in an organization should always start with the support of top management, a strong security culture can only be created and maintained with the consistent involvement and support of those at the top of the organization (Alnatheer et al. 2012; O'Donovan 2006). Ownership of and commitment to security by both management and employees is necessary for them to understand their role in the security policy and to be convinced that security is important (Connolly 2000).

Thirdly, external security threats should be included in the measuring process, in addition to internal security aspects. Organizations are always more or less exposed to certain external security threats, such as theft or fraud, depending on the company's characteristics. It is important that these 'standard' threats are considered when developing a measuring instrument. In addition, the external aspects or the general characteristics of the country or region where the company is based also have an influence on the security culture of an organization. For instance, national culture, socio-economic or technological development, and legislation could all have a substantial impact (van Nunen et al. 2018b). Therefore, as organizations are always exposed to these security threats and external factors, it is important to take them into account when measuring security culture.

Finally, the formulation and implementation of well-founded recommendations and systematic follow-ups are required to achieve a strong security culture. This review found that only two tools explicitly mention possible improvements to the security culture of the organization. Other tools were still being developed and therefore only their methodology could be reviewed. However, all authors focus on identifying weaknesses and strengths in the field of security, so it is highly recommended that those results are used when formulating recommendations. Assessing the security culture helps an organization to discover its strengths and weaknesses in order to make the right strategic choices (Ross 2011; Schein 2009). Also, the results of regular assessments can show whether recommendations from previous measurements were actually implemented, and the extent to which these measures effectively improved the security culture of an organization (Martins and Eloff 2002). If newly implemented measures are found to be inefficient, there may be some shortcomings with the measuring tool. Therefore, it is important that tools contain easily applicable criteria to translate measurement results into well-founded recommendations for an organization. Only in this way can security culture be improved and maintained.

References

AlHogail, A. 2015. Design and validation of information security culture framework. *Computers in Human Behavior* 49: 567–575.

AlHogail, A., and A. Mirza. 2014. A framework of information security culture change. *Journal of Theoretical and Applied Information Technology* 64 (2): 540–549.

AlHogail, A., and A. Mirza. 2015. Organizational information security culture assessment. In: *The 2015 World Congress in Computer Science, Computer Engineering and Applied Computing (SAM'15) Proceedings*, pp. 287–292.

Alnatheer, M., T. Chan, and K. Nelson. 2012. Understanding and measuring information security culture, Pacific Asia Conference on Information Systems (PACIS).

Alvesson, M., and P.O. Berg. 1992. *Corporate Culture and Organizational Symbolism*. Berlin: Walter de Gruyter.

Andress, M., and B. Fonseca. 2000. Manage people to protect data. *InfoWorld* 22 (46): 48.

Bakry, S. 2003. Development of security policies for private networks. *International Journal of Network Management* 13 (3): 203–210.

Baybutt, P., and V. Ready. 2003. Strategies for protecting process plants against terrorism, sabotage and other criminal acts. *Homeland Defense Journal* 2: 1–4.

Beynon, D. 2001. Talking heads. *Computerworld* 24 (33): 19–21.

Breidenbach, S. 2000. How security are you? *Information Week* 800: 71–78.

Chia, P., S. Maynard, and A.B. Ruighaver. (Eds.) 2003. Understanding organisational security culture. In: *Information Systems: The challenges of theory and practice*. Las Vegas: Information Institute.

Connolly, P. 2000. Security starts from within. *InfoWorld* 22 (28): 39–40.

Da Veiga, A. 2008. Cultivating and assessing information security culture (unpublished PhD thesis), University of Pretoria.

Da Veiga, A., and J.H.P. Eloff. 2007. Information security culture—Validation of an assessment instrument. *Information Systems Management* 24: 361–372.

Da Veiga, A., and J.H.P. Eloff. 2010. A framework and assessment instrument for information security culture. *Computers & Security* 29: 196–207.

Da Veiga, A., and N. Martins. 2015. Improving information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security* 49: 162–176.

Fleeger, M.E. 1993. Assessing organizational culture: A planning strategy. *Nursing Management* 24 (2): 39–42.

International Atomic Energy Agency (IAEA). 2017. Self-assessment of nuclear security culture in facilities and activities. *IAEA Nuclear Security Series* 28: 1–124.

Kaplan, B., and D. Duchon. 1988. Combining qualitative and quantitative methods in information systems research: A case study. *MIS Quarterly* 12 (4): 571–587.

Kraemer, S., P. Carayon, and J. Clem. 2009. Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security* 28: 509–520.

Kria, S., L. Pietre-Cambacedes, M. Bouissou, and Y.A. Halgan. 2015. A survey of approaches combining safety and security for industrial control systems. *Reliability Engineering & System Safety* 139: 156–178.

Kruger, H.A., and W.D. Kearney. 2006. A prototype for assessing information security awareness. *Computers & Security* 25 (4): 289–296.

Lundy, O., and A. Cowling. 1996. *Strategic Human Resource Management*. London: Routledge.

Maidabino, A.A., and A.N. Zainab. 2011. Collection security management at university libraries: Assessment of its implementation status. *Malaysian Journal of Library & Information Science* 16 (1): 15–33.

Malcolmson, J. 2009. What is security culture? Does it differ in content from general organisational culture? *43rd Annual 2009 International Carnahan Conference on Security Technology*, Zurich, Switzerland: IEEE.

Martins, A., and J. Eloff. 2002. Information security culture. In *Security in the Information Society, IFIP Advances in Information and Communication Technology, 86*, ed. M.A. Ghonaimy, M.T. El-Hadidi, and H.K. Aslan. Boston: Springer.

Nosworthy, J. 2000. Implementing information security in the 21st century—Do you have the balancing factors? *Computers & Security* 19 (4): 337–347.

O'Donovan, G. 2006. *The Corporate Culture Handbook: How to plan, implement and measure a successful culture change*. California: Lifey Press.

Reniers, G., and W. Dullaert. 2007. *Gaining and Sustaining Site-Integrated Safety and Security in Chemical Clusters*. Zelzate: Nautilus Academic Books.

Ross, S.J. 2011. *Creating a Culture of Security*. Illinois: Information Systems Audit & Control Association.

Schein, E.H. 2004. *Organizational Culture and Leadership*. San Francisco: Jossey-Bass.

Schein, E.H. 2009. *The Corporate Culture Survival Guide*. San Francisco: Jossey-Bass.

Schlienger, T. and S. Teufel. 2003. Analyzing information security culture: Increased trust by an appropriate information security culture. In: *14th International Workshop on Database and Expert Systems Applications*.

Schlienger, T., and S. Teufel. 2005. Tool supported management of information security culture: Application in a private bank. In *Security and Privacy in the Age of Ubiquitous Computing, SEC 2005, IFIP Advances in Information and Communication Technology, 181*, ed. R. Sasaki, S. Qing, E. Okamoto, and H. Yoshiura. Boston: Springer.

Schwarzwalder, R. 1999. Intranet security. *Database and Network Journal* 22 (2): 58–62.

van Niekerk, J. and R. von Solms. 2005. A holistic framework for the fostering of an information security sub-culture in organizations. Paper presented at the 4th Annual ISSA Conference South Africa.

van Nunen, K., G. Reniers, and K. Ponnet. 2018a. Measuring and improving safety culture in organizations: An exploration of tools developed and used in Belgium. *Journal of Risk Research* 21 (5): 622–644.

van Nunen, K., M. Sas, G. Reniers, K. Ponnet, and W. Hardyns. 2018b. An integrative conceptual framework for physical security culture in organizations. *Journal of Integrated Security Science* 2 (1): 25–32.

Vierendeels, G., G. Reniers, K. van Nunen, and K. Ponnet. 2018. An integrative conceptual framework for safety culture: The Egg Aggregated Model (TEAM) of safety culture. *Safety Science* 103: 323–339.

Von Solms, B. 2000. Information security—The third wave? *Computers & Security* 19 (7): 615–620.

Vroom, C., and R. von Solms. 2004. Towards information security behavioural compliance. *Computers & Security* 23 (3): 191–198.

World Institute for Nuclear Security (WINS). 2011. *A WINS international best practice guide for your organization: Nuclear security culture*, 1–22. Vienna: WINS.

Zakaria, O. 2004. Understanding challenges in information security culture: A methodological approach issue. In: *Proceedings of the 2nd Australian Information Security Management Conference*, Australia: Perth.