Cybersecurity Education for Awareness and Compliance

Noted as an IGI Global Core Reference Title in Security & Forensics for 2019.

Ismini Vasileiou (University of Plymouth, UK) and Steven Furnell (University of Plymouth, UK)

Release Date: February, 2019
Copyright: © 2019
Pages: 306
ISBN13: 9781522578475
ISBN10: 1522578471
EISBN13: 9781522578482
DOI: 10.4018/978-1-5225-7847-5

Achieving a Security Culture

By Adele da Veiga, Unisa, dveiga@unisa.ac.za

ABSTRACT

A security culture can be a competitive advantage when employees uphold strong values for the protection of information and exhibit behavior that is in compliance with policies, thereby introducing minimal incidents and breaches. The security culture in an organization might, though, not be similar among departments, job levels or even generation groups. It can pose a risk when it is not conducive to the protection of information and when security incidents and breaches occur due to employee error or negligence. This chapter aims to give organizations an overview of the concept of security culture, the factors that could influence it, an approach to assess the security culture, and to prioritize and tailor interventions for high-risk areas. The outcome of the security culture assessment can be used as input to define security awareness, training and education programs aiding employees to exhibit behavior that is in compliance with security policies.

Keywords: Cybersecurity culture, information security culture, changing security culture, assessing security culture, human, behavior, factors, influence, measure, information security culture assessment, ISCA

INTRODUCTION

The protection of information in an organization is a combined effort of technological, procedural as well as human-related controls (ENISA, 2017). Management that understands the behavioral and cultural aspects of their organization can use it to reduce the risk end-users could pose to information protection (Whittman & Mattord, 2012). One of the human or behavioral controls that organizations can focus on is to inculcate a strong security culture (AlHogail, 2015; ENISA, 2017; Geeling, Brown, & Weimann, 2016). A strong security culture is a culture where information is protected throughout its lifecycle when employees process and interact with it, introducing minimal risk from accidental or ignorant behavior as part of everyday practice in the organization (Da Veiga & Martins, 2015a).

A strong or positive security culture in an organization is essential to mitigate risk from a human perspective in order to secure information (AlHogail, 2015; ENISA, 2017). This will contribute to reducing the risk of employee misbehavior, increase the overall security policy and regulatory compliance, improve the organization's security stance and aim to minimize financial loss due to security incidents or breaches related to employee behavior (Mahfuth, Yussof, Baker & Ali, 2017; Van Niekerk & Von Solms, 2010; Verizon, 2017). It is critical to evaluate the security culture continuously and to address identified gaps to improve employees' compliance with security policies and requirements. Organizations can achieve this by regularly conducting an assessment of the security culture, monitoring the change and implementing corrective actions to influence the culture positively (Da Veiga & Martins, 2015a).

This chapter defines the concept of a security culture in the context of an information security and cybersecurity culture. An overview of the development of it in an organization is discussed, focusing on

the internal factors that could potentially influence the security culture. A security culture assessment approach is discussed with practical advice to roll out such an assessment in an organization. The emphasis is on understanding what the as-is security culture is in order to implement corrective actions to influence it positively. Examples are given of how to analyze the data, which management can use to define change management plans using methods such as awareness, training and education.

DEFINING A SECURITY CULTURE

A security culture can be seen as the unconscious manner in which things are done in an organization to secure information

Every organization has a security culture, which is a subculture of the wider organizational culture (Da Veiga & Martins, 2017; Hayden, 2016; Schlienger & Teufel, 2003; Van Niekerk & Von Solms, 2005). The security culture can be explained as the "way things are done" in the organization to secure information. The way things are done by employees are underpinned by their assumptions, values, beliefs and attitudes (Schein, 1985, Van Niekerk & Von Solms, 2005), which is described as, "the way an organization functions as a sort of collective unconscious for the organization" (Hayden, 2016, pp. 44).

The manner in which employees undertake to protect information when they process it, is based on their shared tacit assumptions, as formed by their beliefs and values, and relates to the motivation for their decisions (Da Veiga & Eloff, 2010; Van Niekerk & Von Solms, 2006). The espoused values such as honesty and fairness form over time and relate to what employees believe should be done to protect information (Da Veiga & Martins, 2015b; Van Niekerk & Von Solms, 2006). The security culture of an organization is visible in tangible aspects of the organization, which are referred to as artifacts, underlined by the values of the organization. These tangible aspects could relate to the security policies and related training sessions, an incident-reporting or helpline, monthly awareness e-mails, the use of technology such as digital certificates for e-mail and so on (Okere, Van Niekerk, & Carroll, 2012; Schein, 1985; Schlienger & Teufel, 2003).

SECURITY CULTURE IN AN ORGANIZATIONAL CONTEXT

The Difference Between A Security Culture And A Cybersecurity Culture

The concepts of cybersecurity culture and information security culture both refer to the concept of a culture related to security, but from a different context. Cybersecurity can be seen as a subset or a component of information security (ISACA, 2017; B. von Solms & R. von Solms, 2018). In the same manner a cybersecurity culture is a subset of an information security culture. The distinguishing factors are the format of the information, the technology and the human element involved, as explained below.

Cybersecurity is concerned with the safeguards that must be implemented to protect information in a digital format from threats that emanate from a global network, like the internet (ISACA, 2017). Information security, on the other hand, includes threats to information across the architecture and in various formats, including hardcopy documents as well as verbal or visual communications (ISACA, 2017, C. P. Pfleeger, S. L. Pfleeger, & Margulies 2015). The cybersecurity culture is therefore described as the way things are done by users to protect information in cyberspace, whereas the information security culture is the way users do things to protect information throughout its lifecycle and in various formats, typically in the context of an organization or entity. From an organizational perspective the cybersecurity culture forms part of the wider information security culture in an organization. For example, the risk that employees introduce by downloading malicious files from the internet will pertain to the cybersecurity culture as well as the information security culture, whereas leaving confidential client documents in open office areas relates only to the context of information security culture.

A cybersecurity culture has been defined formally as, "the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest in people's behaviour with information technologies" (ENISA, 2017, pp. 5). This definition is in line with the aim of cybersecurity culture being, "to instill a certain way to 'naturally behave' in daily life, a way that subscribes to certain [cybersecurity] assumptions" (Gcaza et al., 2015, pp. 3). The definition of cybersecurity includes three distinct concepts, namely the protection of digital information and information system resources in cyberspace as well as the protection of the end user using cyberspace (Da Veiga, 2016b; Von Solms & Van Niekerk, 2013). A cybersecurity culture can therefore not be confined to people in organizations, but extends to the individual in his/her work and home environment, the national and international context which includes organizations and even governments (Da Veiga, 2016b) who should define action plans and strategies on all levels to mitigate risks from cyberspace (Luiijf, Besseling & De Graaf, 2013). In contrast, an information security culture focuses on the organizational environment and what the organization, as the accountable party, should do to protect organizational information, which includes a focus on the behavior of employees who process the information.

The information security culture includes what employees do on a routinely basis that is accepted as the norm when processing information across the security architecture of an organization. The information security culture also extends to the behavior of employees relating to physical security, disaster recovery and business continuity (Da Veiga & Eloff, 2010). The scope of information security culture therefore focuses specifically on the culture of employees of an organization, which could include permanent staff, contractors, temporarily staff, consultants and third parties. In the context of this chapter the term "security culture" will be used when referring to an "information security culture", which is inclusive of a cybersecurity culture in the context of an organization.

Dominant And Sub Security Cultures In Organizations

The security culture in an organization often manifests in a dominant security culture with related sub security cultures (Da Veiga & Martins, 2017). The dominant security culture reflects the common perceptions of the majority of the employees of how information should be secured in line with the fundamental information security requirements. The subcultures are reflected in groups of employees that have common perceptions as a result of residing in a certain region, being in different departments or having different demographical traits related to age, gender, race or educational backgrounds (Da Veiga & Martins, 2017; E. C. Martins & N. Martins, 2016). A subculture might transpire in a department where employees believe the protection of the confidentiality of information is less important and where the emphasis is on meeting deadlines and sharing information quickly. The dominant security culture can be leveraged to influence the sub security cultures and to aid in directing beliefs and behavior of a sub security culture with the aim of aligning it with the dominant culture (E. C. Martins & N. Martins, 2016). Having a dominant security culture and various sub security cultures in one organizations has the result that the same approach cannot be followed to change or influence the security culture, as the perceptions and non-compliance behavior across the subcultures might vary. A tailored and focused approach for the dominant and sub security cultures is therefore required to institute effective change in each. A security culture assessment can aid management to understand the security culture across the organization and to match the interventions to the needs.

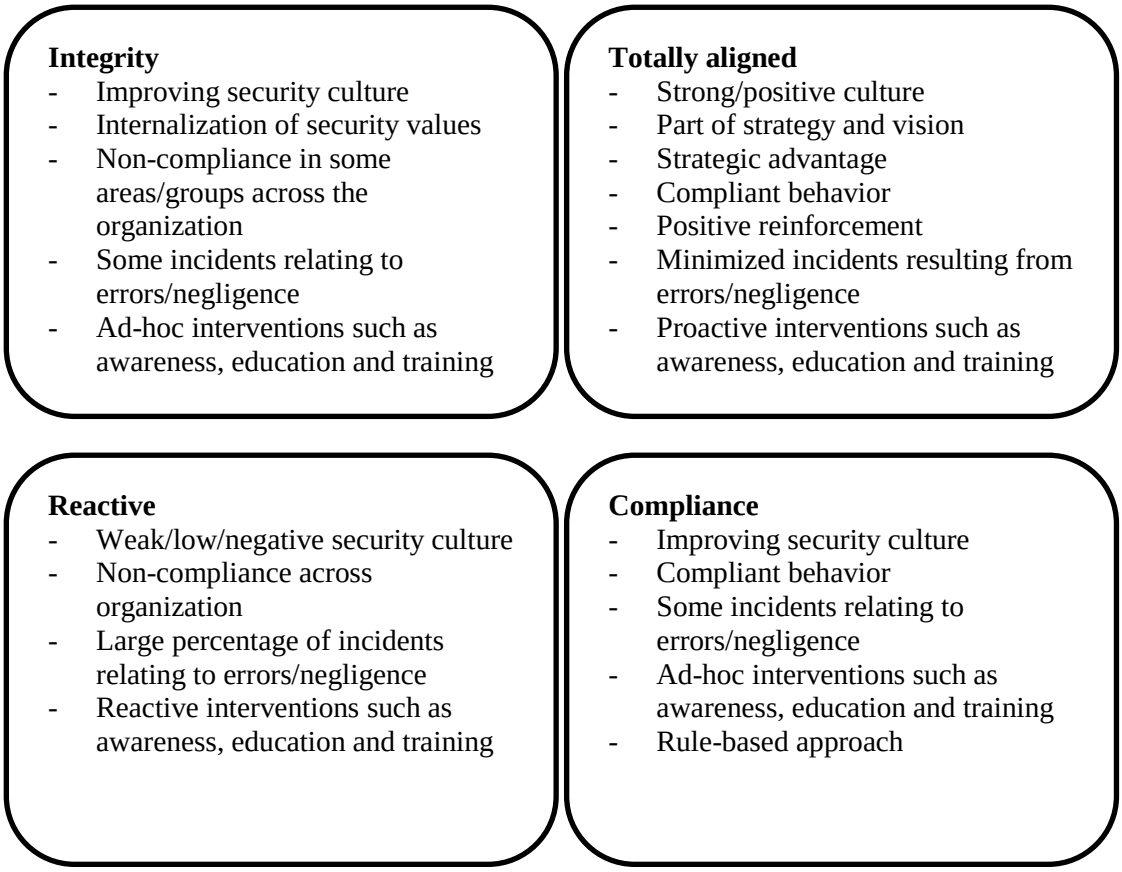
The Desired Security Culture

The information security culture in an organization can be compared with an ethics culture as defined by Rossouw and Van Vuuren (2013). They name four categories of strategies for an ethical culture, namely reactive, compliance, integrity and totally aligned, which can also be applied to a security culture, figure 1. Management should aim for a totally aligned strategy for a security culture. In such a security culture management proactively engages with employees and deploys resources to direct the security culture. The

organization's strategy and vision accommodate security, and positive reinforcement is used to reward compliance behavior. The totally aligned security culture can be seen as a strong or positive culture where employees value information and process it securely throughout its lifecycle. The incidents related to employee errors and negligence are minimized in the totally aligned security culture and employees have a thorough understanding of what is expected of them when processing information.

A reactive strategy towards security culture is the opposite of the aligned strategy. Organizations that are reactive focus on equipping employees on an ad-hoc basis, often after data breaches or security incidents occurred. An organization has an integrity strategy towards the security culture when it proactively implements strategies to minimize incidents, such as employee training and awareness, and data-loss prevention strategies; however, the approach is neither proactive nor integrated with the overall strategy of the organization. A compliance strategy focuses on compliance with regulatory and industry standards, as well as on the organization's policies and procedures. In this environment management typically performs self-assessments, monitoring and audits. For the compliance strategy the approach is rule-based and not an integral part of the operations across the organization.

Figure 1. Security culture strategies



Security Culture And Small- and Medium-size Enterprises

A security culture applies to large organizations as well as small- and medium-size (SMEs) enterprises (organizations). In the same way that an organization has an organizational culture, each organization has a unique security culture. While the concept also applies to SMEs, one needs to take cognizance of the fact that SMEs might not process the same volumes of information, have the same governance structures

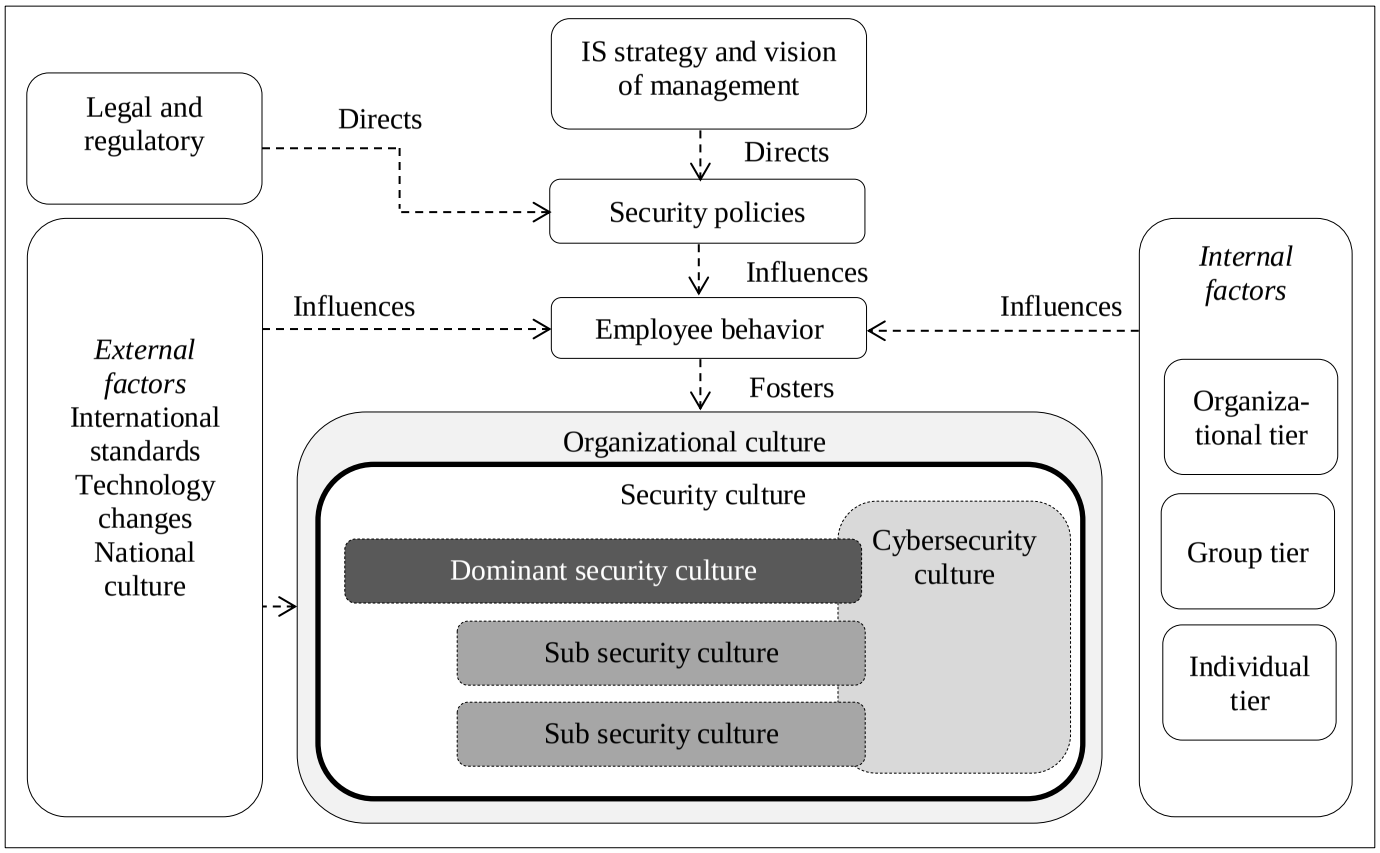
or level of information security policies in place, but are exposed to the same information security and cyber risks as large organizations. SMEs experience different challenges to large organizations in that they often do not have sufficient resources to invest in information security such as having a lack of skills, budget and time (Dojkovski, Lichtenstein & Warren, 2010). It is, however, also important for SMEs to ensure that they have a strong security culture to aid them in mitigating the risk from a human perspective. SMEs should also concentrate on addressing the factors discussed in the next section that influence a security culture as it is part of the foundational elements to implement information security. Whilst it is important to assess the security culture in SMEs, it is important to ensure that SMEs use their resources to implement the necessary technology and process controls for information security and progress to focus on training, awareness and education of employees to further strengthen the security culture.

FACTORS THAT INFLUENCE A SECURITY CULTURE

Security culture is regarded as a subset of the organizational culture (Schlienger & Teufel, 2003; Van Niekerk & Von Solms, 2005). One can therefore refer to the development of an organizational culture to understand what influences the development of a security culture has in an organization. Hellriegel, Slocum and Woodman (1998) explain the development of an organizational culture as a process over time, initiated by the strategy and vision of senior management in an organization. Their direction is conveyed through policies and procedures in the organization, which influence employee behavior. Over time the employee behavior becomes part of the organizational culture and as such also the way in which information is processed and secured, being the security culture. Figure 2 illustrates the development of a security culture with the embedded cybersecurity culture and related dominant or subcultures. The security culture is not rigid and can be influenced by a number of external and internal factors.

Factors external to the employee and organization play a role in influencing the security culture in an organization, such as regulation (AlHogail, 2015) and the national culture (G. Hofstede, G. J. Hofstede & Minkov, 2010). Internal factors such as the personality of the employees and their perceptions can also contribute to influence their behavior and in turn influence the security culture (Padayachee, 2012). Organizations need to ensure that the external and internal factors are considered as part of the security program to ensure that a holistic approach is followed to promote compliance in a consistent and effective manner.

Figure 2. Developing and influencing a security culture (adapted from Da Veiga & Martins, 2017)



Internal Influences

The internal influences refer to factors internal to the organization. They can be grouped under the organizational tier where formal structures are defined, the group tier where employees operate in groups and the individual tier where individuals each have a unique personality, background and traits. The next section gives an overview of each.

Organizational Tier

Formal structures that influence employee attitude and behavior are added on the organizational tier (Robbins, 2001). These could relate to formal roles assigned to the board of directors, executive management, senior management and security practitioners to govern security in an organization (ISACA, 2017). Executive management defines the manner in which security is managed in the organization, with top management leading by example to enable employees to follow (ISACA, 2017; Mohelska & Sokolova, 2015). According to ISACA (2017) top management should endorse security requirements and follow through on disciplinary action where employees do not comply. Their expectations should be communicated through various channels, including awareness and education programs. To further direct the security culture, executive management should provide the necessary resources such as cybersecurity practitioners with sufficient skills and experience as well as sufficient financial resources to implement security requirements and to educate employees.

Group Tier

There are various compositions of groups in organizations, each with unique views and ways of functioning (Robbins, Odendaal & Roodt, 2003). These groups relate to the composition of subcultures that are evident in organizations and could include members of a group in a department, a committee, a certain age group, gender or educational background (Robbins, 1997). The Chief Security Officer (CSO) should ensure that awareness programs specifically target groups of employees that exhibit behavior that are not in compliance with the security policy or that is not aligned with the expected security culture.

Individual Tier

Employees (individuals) have various characteristics that vary in terms of their demographics, background, nationality, age, personalities, attitudes and assumptions (Robbins, 2001). The characteristics of individuals could influence the manner in which they behave and comply with security requirements in an organization (Robbins et al., 2003). The security awareness programs of organizations should therefore also make provision for individual training and education.

External Influences

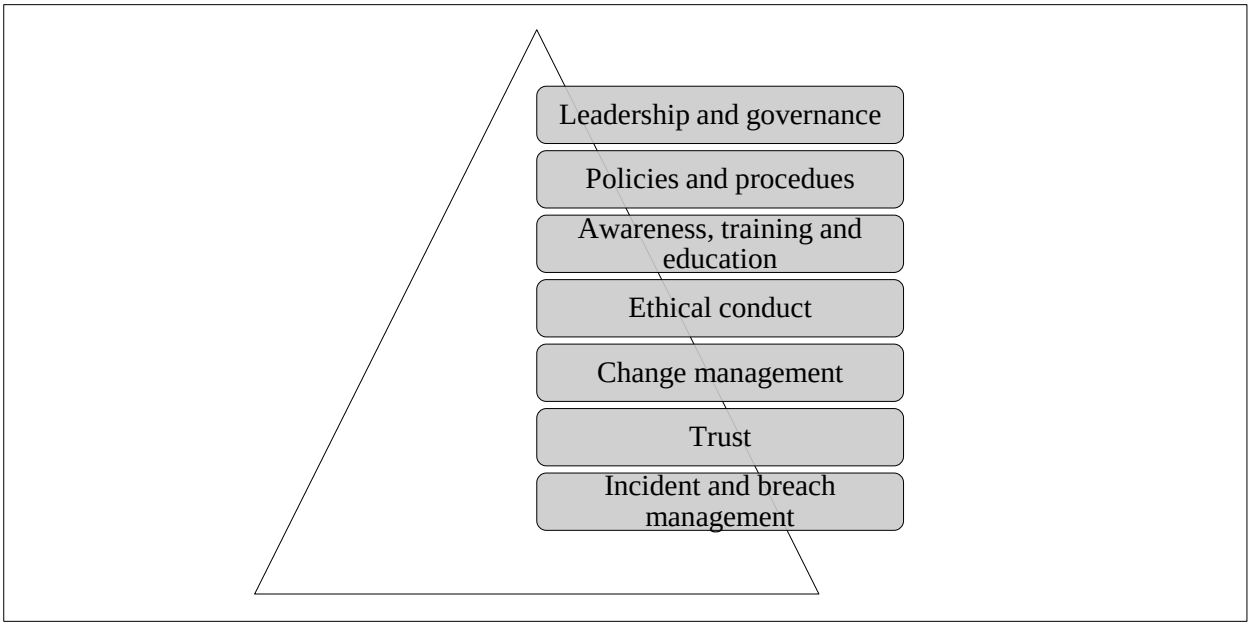
External influences on the organization relate to factors that can influence the security culture from outside the organization such as competitors, changes in the economy, new technological developments, national culture, industry standards and legal requirements. For example, organizations with offices in jurisdictions with data protection regulation have to implement controls to protect personal information and ensure compliance with the processing requirements of the respective privacy laws. Employees will be expected to process personal information according to the organization's privacy policies and necessary legal requirements. Offices in jurisdictions without data protection legislation will not be required to adhere to the same strict legal requirements for the processing of personal information and as such the culture towards privacy might vary from highly, moderated to low, across jurisdictions (DLA Piper, 2018). New technology also influence the manner in which employees share and process information that could either contribute to the protection of information or introduce risk. New technology like the Internet of Things (IoT), Bring Your Own Device (BYOD), cloud computing, and social media usage introduce new risks to the integrity, confidentiality and availability of information. Employees have, for example, been found to share too much information over social media and in some cases confidential information, which can lead to litigation (He, 2012). While external factors emanate from outside the organization, it often has an impact on a strategic and operational level in an organization where internal policies have to be formulated to minimize risks from external factors.

As the focus is on the security culture from within the organization and what management can do to direct it purposefully, the next section will discuss the internal factors – referred to as the foundational elements – that form the cornerstone of a desired security culture in an organization.

THE FOUNDATIONAL ELEMENTS FOR A DESIRED SECURITY CULTURE

Figure 3 outlines the foundational elements of a security culture. While all these elements and external factors play a role to influence and direct the security culture, it should be noted that security training, education and awareness are among the most critical elements. The security culture of employees who have attended or who have been exposed to either security training or awareness has been found to be higher or more positive compared to those employees who were not (Da Veiga, 2016a). However, the elements such as the role of leadership and change management are also critical to embed security values in the organization.

Figure 3. Foundational elements of a security culture



Leadership and Governance

Management and leadership in security are required to cultivate a strong security culture (Glaspie & Karwowski, 2018). Management should set the strategic direction, policy principles, lead by example, provide the necessary resources to implement security across the organization, and implement appropriate governance structures to support the security culture on the organizational level (Glaspie et al., 2018). Top management support, buy-in and direction can positively influence the security culture (Alnatheer, 2012; Dojkovski et al., 2010; Kraemer & Carayon, 2005). Top management also plays a role in creating awareness amongst employees regarding what is expected to protect information in line with the desired security culture (Dojkovski et al., 2010). Their expectations are typically documented in the security policies as the "overall intention and direction as formally expressed by management" (ISO/IEC, 2013 pp.13). To further govern security in the organization, management should display their commitment by giving clear direction and explicitly assigning roles and responsibilities while also acknowledging their security responsibilities (ISO/IEC, 2013).

Policies and Procedures

Security policies and procedures are regarded as critical success factors for an information security program (ISO/IEC, 2013). However, creating a security policy alone neither ensures employee awareness nor compliance (Glaspie et al., 2018). The ISO/IEC 17799 (2013) international standard includes the distribution of guidance about the policies as well as appropriate awareness, training and education as critical success factors to implement information security in an organization. The positive impact of being aware of the security policy contents is illustrated by research that have found that the security culture is more positive (or stronger) for employees who have read the security policy, as opposed to those who have not (Da Veiga, 2016b).

Encouragement to comply with the security policies have also been found to improve security across the organization (Tang, Li & Zhang, 2015). It has been found that compliance levels to policies are influenced by rewards as well as punishment for non-compliance (Chen, Ramamurthy & Wen, 2015; Whittman & Mattord, 2012). The same approach can however not be used for all organizations as each organization's security culture is unique. For example, in a security culture case study conducted in a

bank, only 55.4% of employees indicated that security requirements should be part of their performance appraisal; however, in an audit and tax firm, 79.3% of employees were comfortable with incorporating security requirements in their performance appraisal with the aim of improving security policy compliance.

Awareness, Training and Education

Security awareness, training and education (SETA) are aimed at empowering employees through knowledge, skills and guidance to protect information (Whitman & Mattord, 2017). Awareness activities focus on ensuring that employees remain conscious of information security requirements (Whitman & Mattord, 2019). Security education focuses on a formal delivery of security requirements while security training is training tailored for employees to use the organizational resources in the context of their job role (Whitman & Mattord, 2019).

Security education (Al Hogail, 2015) and training (Glaspie et al., 2018) are critical to creating a security culture (Chen & Wen, 2015). Similarly, security awareness is regarded as one of the most important factors to create a strong security culture (Al Hogail, 2015; ENISA, 2017; Ruighaver, Maynard, & Chang, 2007), which has also been emphasized by the Organization for Economic Cooperation and Development (OECD, 2002). Security awareness is regarded as focusing on "what" as opposed to "how", which relates to training (Herold, 2011). Security awareness is typically less formal than training, with a variety of delivery methods (e.g. posters, e-mails, newsletters, speakers, logos, banners, promotional items) and is conducted on a continuous basis by the organization to update employees about security policy requirements (Herold, 2011).

Targeted SETA programs are required to address the "human error or failure" effectively (Whitman & Mattord, 2019, pp. 268). A security culture assessment can be used to identify the job levels or departments that require SETA as well as the most preferred method of delivery. This can aid management to direct the SETA programs effectively to match the needs of the employees and to address the gaps identified. While the security culture assessment can inform SETA programs, it is key to use a holistic approach whereby the effectiveness of SETA programs is also assessed by using different techniques. Whitman and Mattord (2019) recommend an approach whereby awareness outcomes can typically be assessed with true/false or multiple-choice scales, training outcomes can be assessed through applied learning, and educational outcomes can be assessed through essay-style questions relating to interpretive learning. It is important to note that a security culture assessment does not measure the learning outcomes of SETA programs, but rather the perception and attitudes of employees towards security in the organization.

Ethical Conduct

In the information security field, information security professionals are guided by codes of ethics such as those of the Association for Computing Machinery (ACM, 2018), the Information Systems Security Association (ISSA, 2018) and the Information Systems Audit and Control Association (ISACA, 2018). All employees are not necessarily guided by these codes of ethics. They will typically be guided by the ethics code of the organization. However, employees from different nationalities or countries could have different perceptions towards ethics (Whitman & Mattord, 2012). To complicate the matter even more it has been found that attitudes towards ethics in the use of computer resources differ among individuals in the same country or even in one organization (Whitman & Mattord, 2012). Whitman and Mattord (2012) emphasize that education can be used to overcome the challenge of diverse ethical attitudes. It is therefore critical for the organization to understand the perceptions and attitude of their workforce in order to identify employee groups whose attitudes and perceptions are not in line with the organization's code of

ethics and security policies. The information security culture assessment as discussed in this chapter can be used to identify such groups and to establish what interventions are required.

Change Management

Change management is important to instill a strong information security culture (Ashenden & Sasse, 2013; Ruighaver et al., 2007). A formal change management approach should be followed to direct the security culture purposefully. Change can only be initiated through a formal process during which the security culture is assessed to gain an understanding of it (Berry & Houston, 1993; Byars & Rue, 1997; Herold, 2011). The assessment serves as an organizational diagnosis to identify the as-is security culture and any prevailing issues or risks in the dominant culture or subcultures with the objective of improving or directing the culture. The data can be used to "stimulate and guide desirable changes" (Martins, 2017, pp. 1) in the security culture. Security culture changes should be implemented in such a manner that the changes are embedded and over time become part of the overall organizational culture. Change management approaches such as Prosci's ADKAR (Hiatt, 2006) change management model have been applied successfully in projects (Kazmi & Naarananoja, 2014; Kiani & Shah, 2014; Sheperd, Harris, Chung & Himes, 2014) and can also be applied to conduct the security culture assessment and to implement related changes.

The ADKAR change management model includes five phases, namely awareness (about the necessity for change), desire (to be part of and to support the change), knowledge (of how to bring about the change), ability (to be capable of implementing changes) and reinforcement (to maintain the implemented changes). These phases can be used to implement the change management actions as identified from the security culture assessment. Knowledge of the survey data and findings can be used to create awareness amongst stakeholders and employees for the need to change, which will also support the desire to change. Knowledge of how to change can be derived from the survey data by focusing on the most negative concepts and groups as identified in the data. The ability to change should be supported by management resources that also extend to a follow-up assessment to monitor the change and impact of the actions, which can be used to reinforce changes. Interestingly, in the security culture case studies conducted employees indicated their willingness to change and preparedness to accept some inconvenience to change. For example, in one of the financial organizations, 96% of employees indicated that they were prepared to change their working practices in order to secure information assets, with another 97% indicating that they were willing to accept inconvenience to secure important information. This might, however, not be the case in all organizations and a structured change program can aid management to implement security changes in a constructive manner.

Trust

When implementing security in an organization, a trusting relationship should be in place between management and employees so that compliance with security policies is facilitated and commitment to information security is illustrated by management – especially, as trust is regarded as one of the fundamental characteristics of leadership (Robbins, 1997; Flowerday and Von Solms, 2006). Trust is necessary in organizations to facilitate the sharing of knowledge (Rossouw & Van Vuuren, 2013), which also relates to knowledge of how to secure information. To facilitate an environment of knowledge-sharing through security training, education and awareness, a trusting relationship should be in place to contribute to the development of a strong security culture. Trust as a construct is also assessed during the security culture assessment to establish if it could be hampering the development of a totally aligned security culture.

Incident and Breach Management

Incident and breach management relates to the plan of the organization to respond in the event of a security incident or data breach in terms of the detection, reaction and recovering (Whitman & Mattord 2019). From the employees' perspective it is important that they know what a security incident is, who to report it to and what to do in the event of such an incident. In previous security culture assessments conducted in organizations, employees indicated in many of the case studies that they did not know who to report security incidents to and also did not know what an incident is. Table 1 portrays the results of one of these case studies in which employees were asked who they should report security incidents to. In this case study the majority believed they should report to the Group Information Security Officer, followed by their manager, where in actual fact they were required to report security incidents to the Helpdesk. In this same case study 72.1% of employees knew what a security incident is. In the follow-up surveys this improved to 87.6%, following targeted interventions.

Table 1. Reporting security incidents responses

Response option	Frequency	Percentage of responses
Helpdesk	206	9.5%
Immediate manager	1 287	59.6%
Group information security officer	1 596	73.9%
Human Resources	61	2.8%
Information Technology	225	10.4%
I don't know	92	4.3%
Whistle-blowing process	138	3.6%

A PROCESS TOWARDS CHANGING THE SECURITY CULTURE IN AN ORGANIZATION

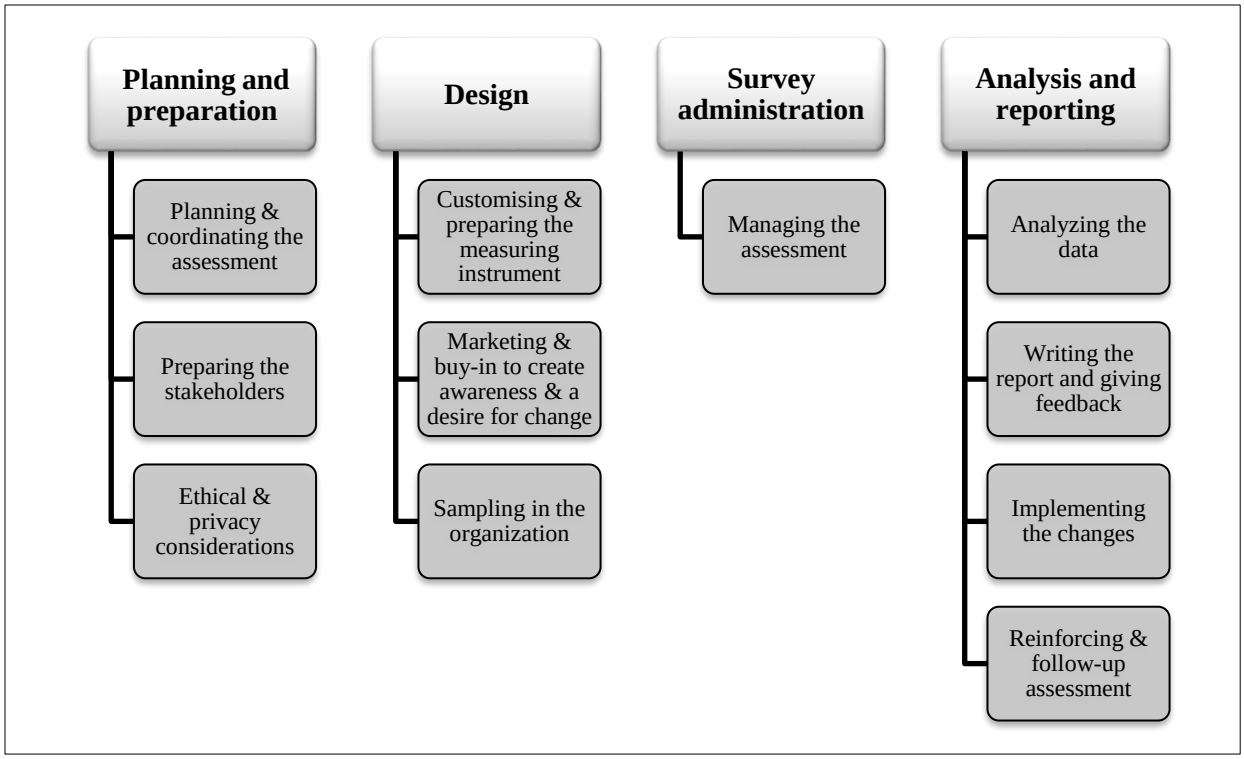
There are various reasons why organizations might want to conduct a security culture assessment. They might need data to prove a suspicion that the behavior of employees in a certain department or biographical group is not in line with the expected culture. The organization might want to identify aspects of risk in the security culture to prioritize and tailor interventions, or to monitor the impact and success of change after the implementation of interventions. One benefit of the security culture assessment is that the data can be used to inform the content and focus of awareness, training and education programs. Follow-up assessments can provide management with data to benchmark and compare progress to further identify awareness, training and education needs.

The Security Culture Assessment Approach

Organizations that embark on a security culture assessment project can use the approach outlined in figure 4 as a guideline to conduct the assessment. This approach has four phases to conduct the assessment in a planned, structured and organized manner with the objective of obtaining valid and reliable data that management can use for strategic decisions to improve the security culture. It is a quantitative approach whereby a questionnaire is deployed in an organization by using a survey strategy. Questionnaires work well when deployed to assess attitude towards and opinions about an organizational practice (Saunders, Lewis & Thornhill, 2016), such as the security culture. The results can be generalized across the organization if a statistical representative sample is used and surveys are also a cost-effective approach (Saunders et al., 2016). A mixed method approach can also be used, such as incorporating documentary research where communications, contents of security policies and audit reports are reviewed. More in-depth information can be obtained if interviews or focus groups are used to confirm data from the security

culture survey, for example to explore reasons for certain answers provided by the various demographical groups. The steps in each of the four phases are discussed below to give organizations a high-level overview of how to conduct the security culture assessment.

Figure 4. Security culture assessment approach



Planning And Coordinating The Assessment

There are a number of aspects to consider when planning the security culture assessment, such as the objective of the assessment, the scope, data protection legislation and project management. Firstly, management should identify the objective of conducting a security culture assessment. Usually, the two most common reasons for assessments are to measure and to change (Borg & Mastrangelo, 2008). The objective could relate to understanding the current security culture to integrate the findings as part of the risk profile of the organization, or to follow up on audit findings in certain business units or regions where employee behavior resulted in security incidents or breaches, or to identify what the content and focus of the security awareness program should be for various departments. Ultimately, the objective is to purposefully change the security culture to the desired culture in which less incidents and data breaches are occurring owing to employees' behavior.

Management should also agree on the scope of the project, such as whether all the organization's offices in the various regions and countries should be included. It should also be determined whether all employees have access to computers to be able to access and complete the questionnaire electronically, and/or whether paper-based questionnaires will be required. Another factor to consider is whether the questionnaire should be translated into more than one language, especially if offices in other countries are included.

Many organizations prefer to host the survey internally, while others make use of third parties or consultants. When third parties or consultants are used, organizations usually have to engage in a third-

party contract process and agree on the privacy and security requirements of the data. This could take some time to negotiate and agree on, especially if different data protection regulations are to be considered for cross-border transfer of the data. For example, if the offices of the organization are located across the United States as well as Europe, the employees' biographical data, as captured in the questionnaires, will be saved in the third party database, which could reside in the United States. The General Data Protection Regulation (GDPR) (European Parliament, 2016) requirements for cross-border transfer of European citizens' data must then be considered and applied in the survey process.

The assessment process does not only relate to sending out the questionnaire and analyzing the data. The project should be managed using aspects of project management principles, such as defining specific tasks and assigning roles and timelines to them. For example, the timeline of activities; the survey timeframe (typically not during a holiday or year-end as the response rates will be lower); the stakeholders to include; the different roles; the budget; which tasks can run concurrently; planning the feedback method and timeframe for feedback to management, employees and stakeholders; and so on should be determined (Martins, 2017).

Preparing The Stakeholders

The management of stakeholders in the security culture assessment is critical and often impacts on the success of organizational diagnoses projects. Ledimo (2017) emphasizes that the stakeholders should be identified upfront and engaged with to manage resistance and concerns. A number of stakeholders, which include the Information Security Officer (ISO) or Chief Information Officer (CIO) and departments in the organization, such as training or human resources, should be part of the team to increase the success of the project (ENISA, 2017).

The ISO or CIO is often the security culture assessment project sponsor that either drives the project or allocates the responsibility to someone in his or her team. When an organization conducts an assessment, the output will result in change plans that have to be implemented (Ledimo, 2017). The stakeholders tasked with implementing the change should therefore be involved from the start. These stakeholders could relate to the marketing and communications team that designs and delivers awareness material, the training team that might need to compile and deliver customized and focused training based on the results, the Information Technology Department that might need to work with the training team to assist in defining the training content or to implement/revise technological controls, and the risk and compliance team that might need to follow up on high-risk departments or integrate the findings in their reports. In some instances trade union representatives should be included as they might need to give input for the planning and should receive feedback on the results as it could impact their members.

The stakeholders comprising individuals or committees (e.g. Risk and Compliance Committee) should be identified upfront and their buy-in should be obtained. This could be done by presenting the project to them and discussing the benefits and potential use of the results to institute change. The board or executive representation might also be required to support the security culture assessment project (ENISA, 2017).

Ethical And Privacy Considerations

Questionnaires usually include a section where demographical data is collected in order to segment the data for comparison purposes and to identify priority groups across the organization to target interventions. While the questionnaires should be anonymous, personal identifiable data such as department name, age, job level, language, years of employment and gender is still collected. When these data fields are combined, it might be possible to identify individuals especially in demographical groups

in which there are only a few staff members. Ethical and privacy requirements should therefore be considered, as listed below in alphabetic order (Da Veiga, 2017):

- Autonomy: Employees' decision to participate or not to participate in the security culture assessment should be respected (Mitchell & Jolley, 2007; Oates, 2012; Saunders et al., 2016).

- Best interest: The participants should be informed of the security culture assessment through a proper communication channel such as a meeting, e-mail of informed consent agreement where their interests and role are described (HPCSA, 2008).

- Benevolence: A risk assessment can be conducted to evaluate the type of personal identifiable information and attitude, or opinion information that will be collected to ensure that the rights of participants are respected, and that confidentiality and privacy requirements are met. Ultimately the benefits should outweigh the risk of the assessment (Miller & Brewerton, 2003, Saunders et al., 2016).

- Compassion: The organizations should illustrate compassion if participants from vulnerable groups, such as those with disabilities, are included. Measures should be implemented to enable them to participate (HPCSA, 2008).

- Confidentiality: The personal identifiable information and all responses should be treated as confidential by all parties, including any third parties involved in the planning, hosting, data cleansing, statistical analysis and report writing (Miller & Brewer, 2003; HSRC, 2017; Oates, 2012; Saunders et al., 2016). Adequate security measures should be in place to protect the electronic survey data when sent across the organizational or third party networks, in the database as well as when being e-mailed or statistically analyzed.

- Consent: Employees should give consent for their data being transferred cross-border, or if their data will be used for other purposes (European Parliament, 2016; Oates, 2012; Saunders et al.; 2016).

- Excellence and competence: The questionnaire should be validated statistically to ensure that the data and findings are reliable and valid (ISACA, 2016; HPCSA, 2008; HSRC, 2017).

- Honesty: The project team should ensure that the data used in reports and feedback sessions is reported on in an honest and accurate manner (Miller & Brewerton, 2003; Singapore Statement, 2010, Saunders et al., 2016).

- Human rights: The human rights of all participants and stakeholders should be considered, for example to have fair selection criteria representing all groups across the organization when defining the selection criteria if a sampling approach is used (HPCSA, 2008).

- Impartiality and independence: The stakeholders involved must declare any conflicts of interest, such as being a shareholder of the company that will host the data (ALLEA, 2017).

- Integrity: The assessment must be conducted in line with the organizational values considering fairness, honesty and quality of the data collection, analysis and reporting (Singapore Statement, 2010; HPCSA, 2008).

- Justice: The project team and stakeholders must treat all the participating employees with respect, sensitivity and fairness, especially if the employees are compensated to participate (HSRC, 2017; HPCSA, 2008).

- Objectivity and independence: The project team should conduct the assessment in line with their organizational codes of ethics and professional codes of ethics (Babie, 2004; ALLEA, 2017; ISACA, 2016). If the project is audited or monitored, the reviews should be conducted independently from the project team. Objective decisions should be made based on the data and facts and not on opinions.

- Transparency: The participants must be informed of the survey objective, any possible risks and expectations. Results should be communicated to the relevant stakeholders to ensure transparency (Mitchell & Jolley, 2007).

Customizing And Preparing The Measuring Instrument

There are a number of security culture questionnaires available, which can be used for the assessment of security culture. The most prominent ones are listed below in alphabetical order:

- AlHogail (2015) proposed the Information Security Culture Framework (ISCF), which comprises five dimensions, namely strategy, technology, organization, people and environment (STOPE). Four domains of human behavior factors (preparedness, responsibility, management, and society and regulations) are assessed in each of the dimensions. This questionnaire has a reliability score **(**Cronbach alpa) of 0.619 to 0.928.

- The Information Security Culture Assessment (ISCA) questionnaire has been designed to assess the as-is security culture in an organization (Da Veiga & Eloff, 2010). The questionnaire is based on the Information Security Culture Framework (Da Veiga & Eloff, 2010) and comprises ten dimensions, namely change management, information asset management, information security leadership, information security management, information security policies, information security program, trust, user management, training and awareness, and privacy perception. The reliability score (Cronbach alpa) is between 0.764 and 0.877 (Da Veiga & Martins, 2015b). This questionnaire was used successfully in five financial institutions in South Africa, in a mining organization as well as consumer market organization. In one of the financial institutions the questionnaire was deployed across twelve countries at four different occasions during a period of eight years to monitor the impact of the interventions and change on the information security culture (Da Veiga & Martins, 2015a, 2015b, 2017) and in another it was deployed twice. Furthermore, it was implemented in a government parastatal and in an audit, tax and advisory firm. The results obtained from these assessments were found to be valid and reliable to facilitate changes in employee attitude and related behavior, and to inculcate a positive information security culture.

- In a book Lance Haydon (2016) published he included a security culture survey with ten questions to measure security culture. He proposes that a security culture can be defined as the Competing Security Cultures Framework (CSCF), being either a process culture (with tight control and internal focus), a compliance culture (with tight control and external focus), a trust culture (with loose control and internal focus) or a autonomy culture (with loose control and external focus). The objective is to assess and identify the cultural traits and values relating to security in the organization in order to map the culture in one of the four quadrants of the CSCF. This approach follows a survey method.

- Schienger (Schlienger & Teufel, 2003; 2005) developed an information security culture questionnaire and corresponding tool. He defined questions focusing on the individual's attitude, the organization's attitude and the possible solution where after the results are triangulated. The questionnaire is currently available in German as part of Schlienger's consulting services of Tree Solution (2018).

In this chapter the ISCA questionnaire is used for illustration purposes as it is statistically validated and produced positive results in case studies, which were published. The full questionnaire is available in an

2018 publication by Da Veiga, titled "An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture" in the Information and Computer Security Journal.

The theoretical questionnaire dimensions (constructs) are as follows (Da Veiga & Martins 2015a, Da Veiga & Martins 2015b):

1. *Information asset management: Assesses users' perceptions of the protection of information assets*
2. *Information security management: Assesses management's perceptions of information security management*
3. *Change management: Assesses the perceptions about change and the willingness of users to change in order to protect information*
4. *User management: Assesses user awareness and training with regard to the requirements to protect information*
5. *Information security policy: Assesses whether users understand the information security policy and whether communication thereof was successful*
6. *Information security program: Assesses the effectiveness of investing in information security resources*
7. *Trust: Assesses the perceptions of users regarding the safekeeping of private information and their trust in the communications of the organization*
8. *Information security leadership: Assesses users' perceptions of information security governance (e.g. monitoring) to minimize risks to information*
9. *Training and awareness: Assesses employees' perception of additional needs for information security training*
10. *Privacy perception: Assesses employees' perception of privacy principles*

While this questionnaire's questions are defined, it is important to customize the terminology and perhaps add or remove one or two questions that might be relevant/not relevant in the background section of the questionnaire, and include specific biographical questions relating to the structure of the organization and profile of the employees. It is advisable not to change too much of the questionnaire as it affects its reliability and validity. Should this be the case, statistical analysis, such as the Cronbach Alpha and factor analysis should be conducted to validate the questionnaire again (Martins & Ledimo, 2017).

The questionnaire can be developed in an online tool such as SurveyTracker (Scantron, 2018), SurveyMonkey (2018) or Qualtrics (2018). These tools include electronic distribution of the questionnaire, automatic data capturing and also the analysis and exporting of the data.

Marketing And Buy-in To Create Awareness And A Desire For Change

It is important to market the security culture survey to the employees and stakeholders in order to get enough responses for the survey across the organization. The questionnaire can be accompanied by an invitation or cover letter from management such as the Chief Information Officer or the Chief

Information Security Officer, explaining the objective, why to participate, how long it will take, confidentiality and anonymity and any further instructions. This is typically sent via e-mail with the hyperlink to the electronic questionnaire. Regular reminder emails help to obtain responses; so does incentives such as receiving a small gift on completion, or standing a change to win a prize (Martins & Ledimo, 2017b).

Sampling In The Organization

Various sampling techniques, such as simple random, stratified, clustered, convenience or snowball sampling can be used (Cresswell, 2014; Oates, 2012; Saunders, Lewis, & Thornhill, 2016). If the objective is to obtain insight into the dominant and subcultures, all employees can be invited to participate, thereby including the entire organization as the sample. The method of Krejcie and Morgan (1970) can be applied to obtain a 95% confidence that the results can be generalized across the organization. Using this method an organization can calculate how many responses are required for the overall results, as well as per biographical group such as a department, as long as the organization can determine the number of employees in each department. For example, an organization with 100 employees requires a response rate of 80, an organization with 500 employees requires a response rate of 217, an organization with 1 000 employees require a response rate of 278 and an organization with 10 000 employees require a response rate of 370. If an organization with 10 000 employees calculate the response rate per job level or department, the overall responses required will be more than 370 as the responses should be calculated separately per department, which will add up to more than the overall figure. Where sufficient responses are not obtained, the results can be validated with interviews or focus groups.

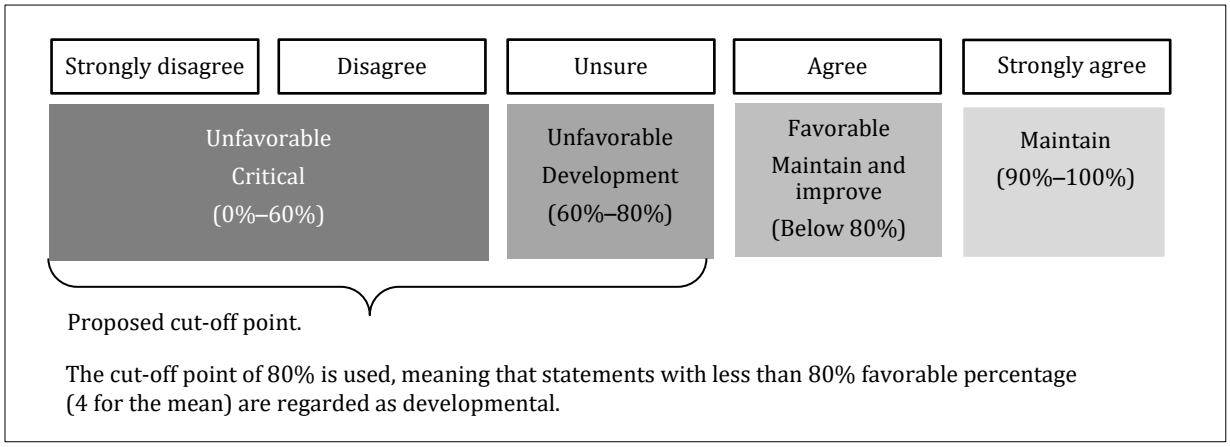
Managing The Assessment

The security culture assessment should be managed by tracking the responses received on a weekly basis, identifying departments or groups with insufficient responses, sending out reminders and establishing if additional communication is required to motivate employees to respond. The various stakeholders, such as the technical team hosting the survey, the communication team that might post notices on the intranet or that sends out reminders require updates on the progress. The process for the completion of paper-based questionnaires should also be planned and managed, for example if facilitators will be used and for data capturing.

Analyzing The Data

It is advisable to use a statistical analysis program such as IBM SPSS Statistics (IBM Analytics 2018) to analyze the data. A Likert scale is used for the ISCA questions. Scores below a mean of 4.00 (Da Veiga & Martins 2015a) can be flagged for improvement, as indicated in figure 5.

Figure 5. Likert scale application for the ISCA



The security culture data can be analyzed by conducting the following as a minimum:

- The number of responses (frequencies) for each of the biographical groups should be calculated, as well as whether a representative response rate was obtained. Table 2 gives an example of the responses received per job level in one of the security culture assessments. In the last column the means for all the security culture questions are listed, showing a close resemblance between the job levels.

  Table 2. Responses and means per job level

Response	Percentage of responses	Means
Executive	2.4%	3.94
Manager	20.8%	3.90
Non-managerial employee	76.5%	3.89
No response	0.3%	N/A

- The means of each of the statements in the ISCA can be calculated. These can be listed from the highest to the lowest to identify the most positive and most negative statements to prioritize interventions. Scores below a mean of 4.00 can be flagged for improvement where actions plans should be defined. Table 3 illustrates the top five results of a security culture assessment comparing the means for four of the surveys conducted. The "*" indicates a significant improvement from the 2010 to 2013 data.

  Table 3. Five most positive statements

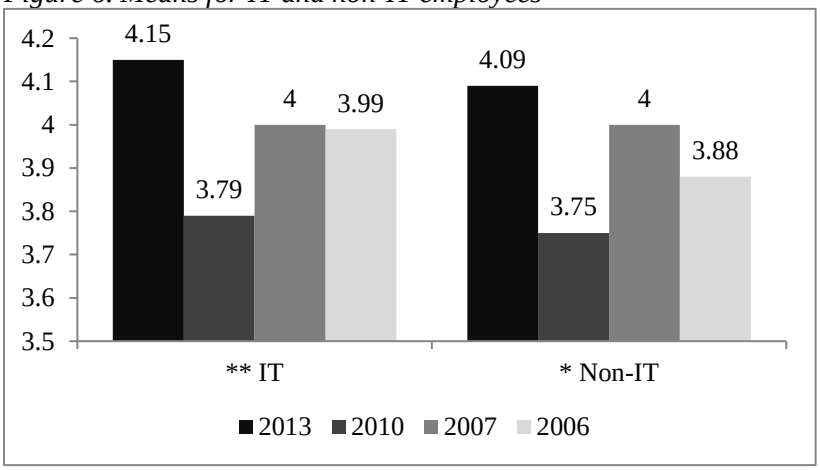
Statements	Dimension	2013	2010	2007	2006
It is important to understand the threats (e.g. theft of equipment, alterations or misuse of information) to the information assets in my division.	Information asset management	* 4.53	4.48	4.48	4.43

Statements	Dimension	2013	2010	2007	2006
I accept that some inconvenience (e.g. changing my password regularly, locking away confidential documents or making back-ups) is necessary to secure important information.	Change	4.43	4.40	4.43	4.37
I am aware of the information security aspects relating to my job function (e.g. how to choose a password or handle confidential information).	User management	* 4.44	4.36	4.36	4.22
I believe it is necessary to commit people to information security.	Information security program	* 4.38	4.33	4.33	4.26
I am prepared to change my working practices in order to ensure the security of information assets (e.g. computer systems and information in paper or electronic format).	Change	4.30	4.29	4.25	4.20

- The means of each of the ten dimensions can be calculated. The dimensions with the lowest mean score should be prioritized for interventions.

- T-tests and analysis of variance (ANOVA) tests can be conducted to identify significant differences among biographical groups such as departments or age groups. This will give management an indication of which group to prioritize for the interventions as well as how to customize interventions for each group based on the specific aspects that scored low as identified in the data. Figure 6 presents the data of one of the security culture assessments where the data was segmented among employees in the Information Technology (IT) department, compared with employees who are not working in IT. The t-tests indicated that there was a significant difference between the means of these groups. For example, in 2013 the IT group, with a mean of 4.15, was significantly more positive than the non-IT group with a mean of 4.09. The implication is that the non-IT group should be prioritized if management plans interventions, which would typically be defined where means are below 4 for the mean.

Figure 6. Means for IT and non-IT employees



T-tests can also be used to identify significant improvements from one survey to the next as indicated in table 4. The "*" indicates that the means of the 2013 statements were significantly more positive when compared with the 2010 means.

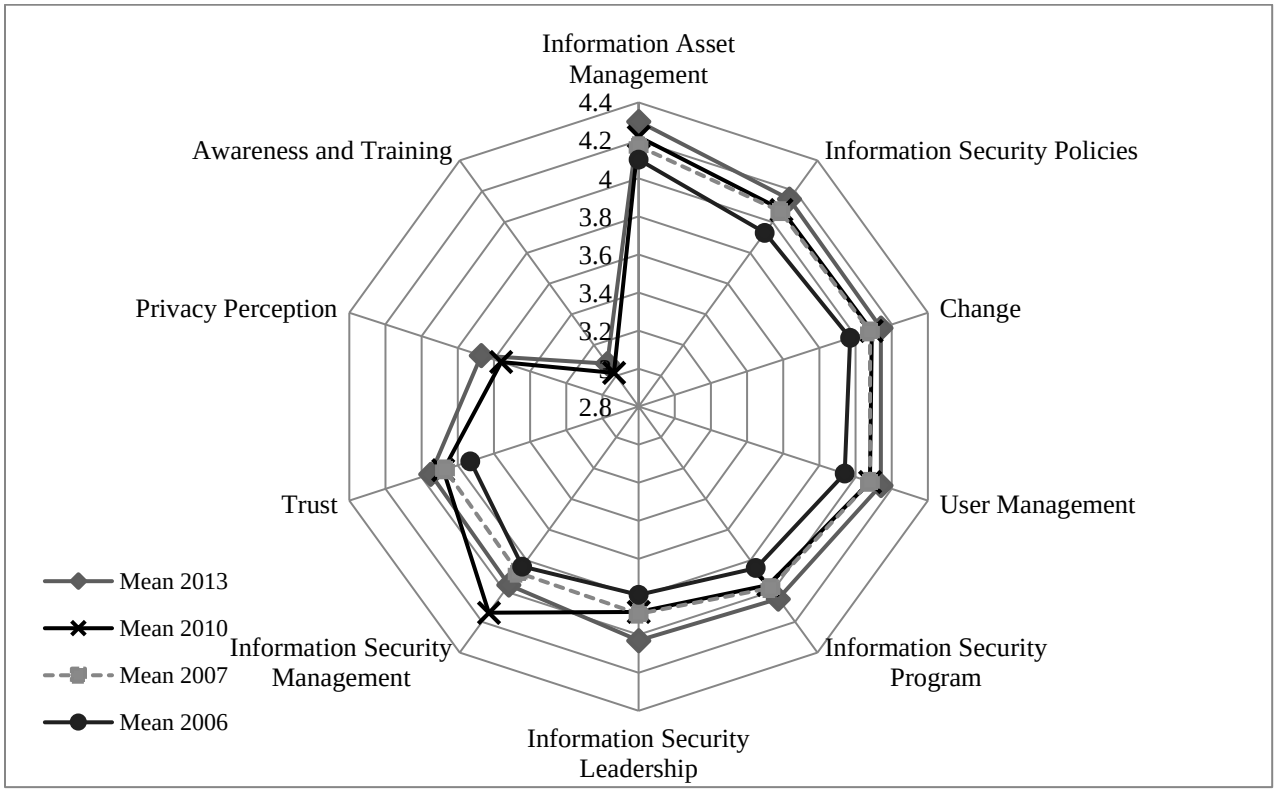
Table 4. Significant differences for individual statements

Statements	Dimension	2013	2010
My division clearly outlines what is expected of me with regard to information security.	Information security leadership	* 3.82	3.66
I believe employees adhere to the information security policy.	Information security leadership	* 3.81	3.66
The contents of the information security policy were effectively communicated to me.	User management	3.73	3.69
I am informed in a timely manner as to how information security changes will affect me.	Change	3.75	3.71
The contents of the information security policy are easy to understand.	Information security policies	* 3.81	3.76

- If the survey was repeated, comparison analysis can be done to identify improvement or changes from the previous results. The means per dimension for each of the years when the survey was conducted can be displayed on a radar chart as depicted in figure 7. The overall mean for 2013, 4.10, indicates an improvement from the 2010 overall mean, 3.76. The ten dimensions of the ISCA questionnaire, used in this specific case study, are displayed with the means of the questions for each dimension. For most of the dimensions, the same trend is visible with awareness and training being the dimension where the most intervention and improvement is required compared to the information access management dimension that remained one of the most positive dimensions. The privacy dimension was only included in the 2010 and 2013 survey and hence no data is available for the other two years.

  The advantage of the longitudinal analysis is to track and monitor the change over time to establish if interventions were successful and where corrective action is required. This type of analysis can be done per department, job level or office area to also track over time whether the security culture is improving or if not, and where intervention is required. The data can also aid management to motivate for budget aimed at awareness, training and education initiatives or to showcase success of corrective actions.

Figure 7. Means per dimension for four assessments



Writing The Report And Giving Feedback

Once the data analysis is complete, the next step is to compile a report of the results with the recommendations. Typically the report should include aspects such as the security culture assessment (survey) objective, the methodology followed, the number of response received compared to the sample sizes required, the overall results per dimensions, the results per statement, the results per biographical group (positive and negative results), recommended action plans and an implementation plan (Martins, 2017). The report can also be summarized in PowerPoint to be presented to the various stakeholder groups. Feedback should also be given to employees to ensure transparency and for employees to understand the necessity to change where improvement is required.

Table 5 gives an extract of recommendations that were made in one of the security culture assessments. For more examples please refer to the article "Defining dominant and sub security cultures", in *Computers & Security* by Da Veiga and Martins published in 2017.

Table 5. Example of recommendations

Intervention	ISCA finding	Recommendation
Communication about the sharing of passwords	Employees believe they can share their passwords with (2010): Helpdesk Managers Secretaries	**Action:** Communicate to employees that no passwords should be shared **Demographical group:** Non-IT employees and non-managerial

Intervention	ISCA finding	Recommendation
	Colleagues	**Method:** E-mail, presentation and web-based training (in order of method preferred by employees)
Communication of the security policy	31.9% of respondents believe that the security policy was not explained and communicated to them effectively 38.9% of respondents have not read the security policy 32.2% of respondents do not know where to get a copy of the security policy	**Action:** Conduct additional policy communication and awareness **Demographical groups:** Non-IT department, South Africa, United Kingdom and Australia **Method:** Develop a security policy brochure with content overview and link Send out monthly e-mails with policy content messages Conduct face-to-face policy overview presentations

Implementing The Changes

The security culture assessment results provide management with a view of the security culture and which aspects or groups require change to improve the culture. A change management process such as that of ADKAR can typically be used to implement the change. Awareness about the change can be created through the feedback to stakeholders, focusing on the offices or groups that scored the lowest. The desire to change can be motivated by illustrating aspects that require improvement which, for example, can be discussed in focus groups. This can be reinforced through the use of role models, change agents in departments, incorporating security aspects in performance appraisals or incentives. The transition phase includes the focus of education, training and awareness for employees in the aspects identified in the ISCA assessment, starting with the priority audiences. Organizations should ensure that they have the necessary resources and ability to change, such as training the ISO and CISOs, or making use of external consultants to implement some of the changes required. Reinforcing the change can be facilitated by conducting a follow-up ISCA survey.

Reinforcing And Follow-up Assessment

The follow-up ISCA assessment can be used to monitor the implemented changes and to identify where the results improved. Additional data in the organization can also be used, for example to track the number of incidents related to employee error and negligence prior to and after interventions.

CONCLUSION

In this chapter the concept of a security culture was discussed as being the unconscious manner in which things are done in an organization to secure information. The security cultures vary among organizations and even within an organization with dominant and sub security cultures that emerge. The intrinsic and extrinsic factors that influence a security culture are discussed in this chapter, emphasizing the importance of education, training and awareness.

This chapter further outlined a process to assess the security culture by discussing the key aspects to consider – from identifying the stakeholders to the report writing and feedback phase. The Information

Security Culture Assessment (ISCA) instrument was discussed as a questionnaire that can be used to establish the level of the security culture with the objective of identifying biographical groups or areas, such as business units or age groups in the organization where intervention is required to direct the security culture purposefully through interventions that can be conveyed by training, awareness and education.

The importance of focusing on the human element is emphasized to aid with security policy compliance and ultimately to establish a strong security culture. An information security culture will be evident in employees that exhibit compliance behavior and have coherent values towards protecting information, thereby minimizing the threat the human element poses to the protection of information. The aim is to achieve a totally aligned security culture.

REFERENCES

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

AlHogail, A. (2015). Cultivating and Assessing an Organizational Information Security Culture: An Empirical Study. *International Journal of Security and Its Applications*, 9(7), 163–178.

All European Academics (ALLEA). (2017). *The European Code of Conduct for Research Integrity*. Retrieved from https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf

Alnatheer, M. (2012). Understanding and Measuring Information Security Culture in Developing Countries: Case of Saudi Arabia. In *Proceedings of the Pacific Asia Conference on Information Systems (PACIS) (paper 144)*. Ho Chi Minh City, Vietnam: Association of Information Systems.

Ashenden, D., & Sasse, A. (2013). CISOs and organizational culture: Their own worst enemy? *Computers & Security*, 39(2013), 396–405.

Association for Computing Machinery (ACM). *ACM code of ethics and professional conduct*. Retrieved from www.acm.org/about/code-of-ethics.

Babie, E. (2004). *The practice of social research* (10th ed.). Belmont, CA: Thomson Wadsworth.

Berry, M. L., & Houston, J. P. (1993). *Psychology at work*. Wisconsin: Brown and Benchmark Publishers.

Borg, I., & Mastrangelo, P.M. (2008). *Employee surveys, tools and practical applications. Employee surveys in management: theories, tools and practical applications*. Cambridge, MA: Hogrefe.

Byars, L. L., & Rue, L. W. (1997). *Human resource management* (5th ed.). Boston: McGraw-Hill.

Chen, Y., Ramamurthy, K., & Wen, K. (2015). Impacts of comprehensive information security programs on information security culture. The Journal of Computer Information Systems, 55(3), 11.

Cresswell, J. W. (2014). *Research design – Qualitative, quantitative, and mixed methods approaches* (4th ed.). Los Angeles: SAGE Publications.

Da Veiga, A. (2016a). Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study *Information & Computer Security*, (24)22, 139-155.

Da Veiga, A. (2016b). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. In *Proceedings of 2016 Science and Information Computing Conference* (SAI2016) (pp. 1006-1115), London, United Kingdom: IEEE.

Da Veiga, A. (2017). Ethical and privacy considerations for research. In N. Martins, E. Martins, & R. Viljoen (Eds.), *Organizational Diagnosis: A guide for practitioners* (pp. 273–298). Randburg, South Africa: Knowledge Resources.

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), 196–207.

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

Da Veiga, A., & Martins, N. (2015b). Information security culture and information protection culture: A validated assessment instrument. *Computer Law and Security Review*, 31(2), 243–256.

Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security*, 70(2017), 72–94.

DLA PIPER. (2018). *Data protection laws of the world*. Retrieved from https://www.dlapiperdataprotection.com/index.html

Dojkovski, S., Lichtenstein S., & Watten, M.J. (2010). Enabling information security culture: Influences and challenges for Australian SMEs. In *Proceedings of the Australasian Conference on Information Systems, (ACIS)* (paper 61). Australia, Brisbane: Qld.

European Union Agency for Network and Information Security (ENISA) (2017). *Cyber security culture in organizations*. Retrieved from https://doi.org/10.2824/10543

Flowerday, S., & Von Solms, R. (2006). Trust an element of information security. In *Proceedings of Security and Privacy in Dynamic Environments (IFIP/ SEC2005)* (pp. 87-98). Boston: Kluwer Academic Publishers.

Gcaza, N., & Von Solms, R. (2017). A strategy for a cybersecurity culture: A South African perspective. *Electronic Journal of Information Systems in Developing Countries*, 80(1), 1–17.

Geeling, S., Brown, I., & Weimann, P. (2016). Information systems and culture – a systematic hermeneutic literature review. In *Proceedings of the International Conference on Information Resource Management (CONF-IRM)* (paper 40). South Africa, Cape Town: Association for Information Systems.

The European Parliament (2016). The European Council. General Data Protection Regulation (GDPR), Regulation (EU) 2016/679. Official Journal of the European Union.

Health Professions Council of South Africa (HPCSA). (2008). *General Ethical Guidelines for the Health Professions Council of South Africa, Annexure 12*. Retrieved from http://www.hpcsa.co.za/conduct/Ethics

Hiatt, J. M. (2006). *ADKAR: A Model for Change in Business, Government and our Community*. Loveland, Colorado: Library of Congress.

Haydon, L. (2016*). People centric security – Transforming your enterprise security culture*. United States of America: McGraw-Hill Education.

He, W. (2012). A review of social media security risks and mitigation techniques. *Journal of Systems and Information Technology*, 14(2), 171-180.

Herold, R. (2011). *Managing an information security and privacy awareness and training program* (2nd ed.). Boca Raton: Taylor and Francis Group.

Hellriegel, D., Slocum, J. W. Jr, Woodman, R. W. (1998). *Organizational behavior* (8th ed.). Cincinnati, OH: South-Western College.

Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). *Cultures and Organizations: Software of the mind* (3rd ed.). US: The McGraw-Hill Companies.

Human Sciences Research Council (HSRC) (2018). *Code of Research Ethics*. Retrieved from http://www.hsrc.ac.za/en/about/research-ethics/code-of-research-ethics

IBM Analytics (2018). *IBM SPSS Statistics*. Retrieved from https://www.ibm.com/analytics/data-science/predictive-analytics/spss-statistical-software

Information Systems Audit and Control Association (ISACA) (2017). *Cybersecurity Fundamentals Study Guide* (2nd ed.). Rolling Meadows, United States of America: ISACA.

Information Systems Audit and Control Association (ISACA) (2018). *Code of Professional Ethics*. Retrieved from http://www.isaca.org/certification/code-of-professional-ethics/pages/default.aspx

ISO/IEC. (2013). *ISO/IEC 27002: Information technology – security techniques – code of practice for information security management.* Kay Westlake: BSI.

Glaspie, H. W., & Karwowski, W. (2018). Human Factors in Information Security Culture : A Literature Review Human Factors in Information Security Culture : A Literature Review. In *Proceedings of Advances in Intelligent Systems and Computing* (pp. 269–280). Florida, United States: Springer.

Kazmi, S. A. & Naarananoja, M. (2014). Collection of change management models – an opportunity to make the best choice from the various organizational transformational techniques, *GSTG International Journal on Business Management (GBR)*, (3)3, 71–79.

Kraemer, S., & Carayon, P. (2005). Computer and Information Security Culture: Findings from two Studies. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (pp. 1483-1487). Orlando, Florida: Human Factors and Ergonomic Society.

Kiani, A., & Shah, M. H. (2014). An application of ADKAR change model for the change management competencies of school heads in Pakistan, *Journal of Managerial Sciences*, VIII (1), 77–95.

Krejcie, R. V., & Morgan, D.W. (1970). Determining Sample Size for Research Activities. *Education and Psychological Measurement*, 30, 607–610.

Ledimo, O. (2017). Preparing and involving all stakeholders. In N. Martins, E. Martins, & R. Viljoen (Eds.), *Organizational Diagnosis: A guide for practitioners* (pp. 25-38). Randburg, South Africa: Knowledge Resources.

Luiijf, E., Besseling, K., & De Graaf, P. (2013). Nineteen national cyber security strategies. International Journal of Critical Infrastructures, 9, 2–31.

Mahfuth, A., Yussof, S., Baker, A. A., & Ali, N. (2017). A systematic literature review: Information security culture. In *Proceedings of the International Conference on Research and Innovation in Information Systems* (ICRIIS) (pp. 456-463). Langkawi, Kedah, Malaysia: IEEE.

Martins, E. C. (2017). Planning and coordinating an organizational diagnosis. In N. Martins, E. Martins, & R. Viljoen (Eds.), *Organizational Diagnosis: A guide for practitioners* (pp. 1–23). Randburg, South Africa: Knowledge Resources.

Martins, E. C. & Ledimo, O. (2017). Developing and sourcing assessment instruments. In N. Martins, E. Martins, & R. Viljoen (Eds.), *Organizational Diagnosis: A guide for practitioners* (pp. 39-83). Randburg, South Africa: Knowledge Resources.

Martins, E. C. & Ledimo, O. (2017b). Survey administration process. In N. Martins, E. Martins, & R. Viljoen (Eds.), *Organizational Diagnosis: A guide for practitioners* (pp. 85-112). Randburg, South Africa: Knowledge Resources.

Martins, E. C. & Martins, N. (2016). Organizational culture. In S.P. Robbins, A. Odendaal & G. Roodt (Eds), *Organizational Behaviour* (3rd ed.) (pp. 606-641). Cape Town, South Africa: Pearson Education.

Martins N. (2017). Survey administration process. In N. Martins, E.Martins, & R. Viljoen (Eds.), *Organizational Diagnosis: A guide for practitioners* (pp. 1810–202). Randburg, South Africa: Knowledge Resources.

Miller, R. L. & Brewerton, J. D. (2003). *The A-Z of Social Research*. London: Sage Publications.

Mitchell, M. L. & Jolley, J. M. (2007). *Research design explained* (6th ed.). London: Thomson Wadsworth.

Mohelska, H., & Sokolova, M. (2015). Organizational culture and leadership – joint vessels? *Procedia – Social and Behavioral Sciences*, 171(2015), 1011-1016.

Oates, B. J. (2012). *Researching Information Systems and Computing*. London, United Kingdom: SAGE Publications, Inc.

Organization for Economic Co-Operation and Development (OECD). (2002). *Guidelines for the security of information systems and networks. Towards a culture of security*. Retrieved from http://www.oecd.org/internet/ieconomy/15582260.pdf

Okere, I., Van Niekerk, J., & Carroll, M. (2012). Assessing Information Security Culture: A Critical Analysis of Current Approaches. In *Proceedings of the Information Security for South Africa Conference (ISSA)* (pp. 136-143). South Africa: IEEE.

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security*, 31(2012), 673–680.

Pfleeger, C. P., Pfleeger, S. L. and Margulies, J. (2015). *Security in Computing* (5th ed.). Upper Saddle River, NJ: Prentice Hall.

Qualtrics (2018). Qualtrics Research Core. Retrieved from https://www.qualtrics.com/research-core/

Robbins, S. P. (1997). Essentials of Organizational behavior (5th ed.). Upper Saddle River, NY: Prentice Hall.

Robbins, S. P. (2001). Organizational behaviour (9th ed.). New Jersey: Prentice Hall.

Robbins, S. P., Odendaal, A. & Roodt, G. (2003). *Organizational behaviour – Global and Southern African perspectives.* South Africa, Cape Town: Pearson Education.

Rossouw, D. & Van Vuuren, L. (2013). *Business ethics* (5th ed.). South Africa: Oxford University Press.

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organizational security culture: Extending the end-user perspective. *Computers & Security*, 26(2007), 56–62.

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research methods for business students* (7th ed.). England: Pearson Education Limited.

Scantron (2018), SurveyTracker. Retrieved from http://www.scantron.com/software/survey/surveytracker-plus/overview

Schein, E. H. (1985). *Organizational culture and leadership*. San Francisco: Jossey-Bass Publishers.

Schlienger, T. & Teufel, S. (2003). Analyzing information security culture: Increased trust by an appropriate information security culture. In *Proceedings of the International Workshop on Trust and Privacy in Digital Business (TrustBus 2003) in conjunction with the 14th International Conference on Database and Expert Systems Applications (DEXA 2003)*. Prague: IEEE.

Schlienger, T. & Teufel, S. (2005). Tool supported management of information security culture. In *Proceedings of IFIP 20th International Information Security Conference proceedings* (pp.65-77). Japan: Springer.

Sheperd, M. L., Harris, M. L, Chung, H., & Himes, E. M. (2014). Using the Awareness, Desire, Knowledge, Ability, Reinforcement Model to build a shared governance culture, *Journal of Nursing Education and Practice*, (4)6, 90–104.

SurveyMonkey (2018). SurveyMonkey. Retrieved from http://www.surveymonkey.com

Tang, M., Li, M., & Zhang, T. (2015). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management*, 17(2), 1–8.

Tree Solution. (2018). Sicherheitskultur. Retrieved from http://www.treesolution.ch/10-0-Smart-Tools-fuer-mehr-Sicherheit.html

The Singapore Statement on Research Integrity. (2010). Retrieved from www.singaporestatement.org

The Information Systems Security Association (ISSA) (2018). *ISSA code of ethics*. Retrieved from www.issa.org/?page=codeofethics

Verizon. (2017). *Data breach investigations report* (10th ed.). Retrieved from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

Whitman, M. E. & Mattord, H. J. (2012). *Principles of information security* (4th ed.). Australia: Course Technology Cengage Learning.

Whitman, M. E. & Mattord, H. J. (2017). *Management of information security* (5th ed.). Australia: Course Technology Cengage Learning.

Whitman, M. E. & Mattord, H. J. (2019). *Management of information security* (6th ed.). Australia: Course Technology Cengage Learning.

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, 29(2010), 476–486.

Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security*, 26(1), 2–9.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38(2013), 97–102.

ADDITIONAL READING

Information Security Culture Assessment Questionnaire

The Information Security Culture Assessment Questionnaire can be accessed at:

Da Veiga, A. (2018). An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture. *Information and Computer Security Journal*, 2018(5).

Dominant and sub security cultures

Additional reading about dominant and sub cultures as well as examples of recommendations and actions plans based on the ISCA data, please read: Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers and Security*, 70, 72–94.

Health and safety culture

The relation to health a safety culture can be investigated by considering projects such as the Keil project following a maturity model approach.

Keil Centre, (2018). *Keil centre*, chartered psychologists and ergonomists, Retrieved September 14, 2018, from http://www.keilcentre.co.uk/products-services/safe-people/safety-culture/safety-culture-maturity-model/

National culture

National culture, as an external influence to a security culture, should be considered when assessing the security culture of global organizations. For further reading refer to the work of Hofstede.

Hofstede G., Hofstede G.J. & Minkov M. (2010). *Cultures and Organizations - Software of the Mind*. New York, USA: McGraw-Hill.

Minkov M. & Hofstede G. (2013). Cross-cultural analysis – The science and art of comparing the world's modern societies and their cultures. California, USA: Sage Publications.

Geert Hofstede (2018). *Geert Hofstede*. Retrieved September 14, 2018, from https://geerthofstede.com/.

Hofstede Insights (2018). *Hofstede Insights*. Retrieved September 14, 2018, from https://www.hofstede-insights.com/.

KEY TERMS AND DEFINITIONS

Security culture: A security culture can be seen as the unconscious manner in which things are done in an organization to secure information. The security culture is synonymous with the information security culture and includes cybersecurity culture in the context of an organization.

Cybersecurity culture: The cybersecurity culture is the unconscious way things are done by users to protect information in cyberspace. This culture extends to home users, employees in organizations or entities, users in communities as well as users from a national or international context.

Information security culture: The information security culture is the unconscious way things are done by employees to protect information throughout its life cycle and in various formats, typically in the context of an organization or entity. The information security culture includes cybersecurity culture in the context of an organization.

Information Security Culture Assessment (ISCA): A validated security culture questionnaire with ten constructs to assess the security culture in an organization.