A Change Management Perspective to Implementing a Cyber Security Culture

Trishana Ramluckan, Brett van Niekerk and Isabel Martins
University of KwaZulu-Natal, Durban, South Africa
ramluckant@ukzn.ac.za
vanniekerkb@ukzn.ac.za
MartinsM@ukzn.zac.za
DOI: 10.34190/EWS.20.059

Abstract: There has been an increasing prevalence of global cyber-attacks. Because of the possible breaches in information security, it has become pertinent that organisations change organisational and individual cultures to become more secure. However, there are challenges regarding the implementation of these processes within organisations. Organisations have become dependent on information systems, which stores large quantities of data and can be considered as one of an organisation's greatest assets. Whilst employees are considered as the next important asset, their negligence, whether intentional or not, and due to their possible lack of knowledge regarding information security, have also become one of the biggest threats to information security. Employees often fall victim to phishing scams, malware and ransomware attacks. Whilst many consider the implementation of information security awareness initiatives as a solution to this impending threat, more often than not organisations utilize presentations to address information security awareness training. This approach has not been successful as the target audience has difficulty in retaining the knowledge, and this often hinders its proper implementation. Change management not only involves the change in processes and tools but also focuses on the techniques used to manage the cultural change within organisations. This paper 'encodes' awareness training for information security and cyber security from a change management approach and provides best practice approaches in changing an organisation's culture from an insecure culture to a secure one.

Keywords: Information security, change management, training and development, organisational culture, threat mitigation

1. Introduction

With reference to the SANS Institute (n.d.) information security can be defined as, "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction" Information security consists of three main elements namely technology, processes, and people. Although security measures including passwords, firewalls and biometric controls are important, they are not sufficient when attempting to mitigate vulnerabilities of systems and threats to information. The general requirement for the prevention or mitigation of threats to information relies on a combination of measures. With the three main elements of information security being technology, people and processes, there is a shift towards the people-oriented element. This places importance on areas of training and governance (Da Veiga and Eloff, 2007).

Change management plays a vital role in instituting an information security culture. The change management process consists of various stages which includes everything from change identification through to post-implementation review and request closing (INFOSEC, 2020). The purpose of the change management process is to ensure that all changes follow a controlled and systematic implementation process. Furthermore, the key objective of change management within information security is the alignment of people and culture to information security best practices while at the same time mitigating any resistance to change (Kortan and von Solms, 2012)

This paper aims to propose a framework/model for the change management process to instil a cyber security culture within and organisation. Section 2 presents the literature review, which provides background information to secure cultures and introduces the Resource Based View (RBV) and ADKAR (Prosci, n.d.) change management frameworks/models. Section 3 provides a discussion on the culture and proposes the framework. The paper is concluded in Section 4.

2. Literature

The relevant literature is discussed in this section which includes information security culture, change management and a brief overview of the change management models.

2.1 Information Security Culture

The organisational culture within any business is important as it defines the way in which the employee views the organisation (Ulich, 2001, cited in Schlienger and Teufel, n.d; van Niekerk and von Solms, 2006; Kortan and von Solms, 2012). It can be described as a collective but adaptable phenomenon and can be easily influenced by company executives over time. The two main elements of organisational culture are assumptions and beliefs, which are often expressed in the collective values, norms and knowledge in an organisation's environment. The resulting factor that emerges is that these collective norms and values promote or instil a particular behaviour of the employees in the environment. Ultimately, the organizational culture has a crucial impact on the corporate success (Rühli, 1991, cited in Schlienger and Teufel, n.d.; van Niekerk and von Solms, 2006; Kortan and von Solms, 2012).

An organizational culture usually consists of varying subcultures founded on functions. Information security culture can be considered as a subculture or function of the organisation. Generally, the organisational culture should support all activities and with it information security as a subculture should become a normal element in employees' daily activities (Zaini, Masrek, Sani, and Anwar, 2018). With reference to Zaini et al., (2018) the three layers of Information Security Culture and their interactions are illustrated in Figure 1.

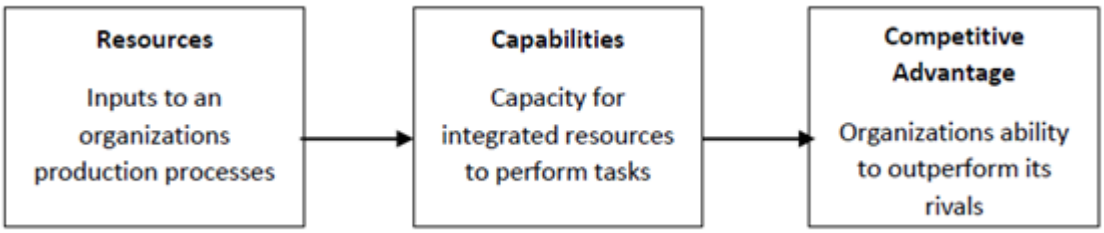

Figure 1: Three Layers of Information Security Culture

Source: Zaini, Masrek, Sani and Anwar (2018)

According to the International Telecommunications Union (2008), there is a new reality of cyber space and as such cybersecurity or information security requires the creation of an information security culture, with its foundations based on the norms of proper behaviour as well as the ability to prosecute online criminals. However, it must be noted that with the dependency on the cyber realm, more security challenges are created.

Zakaria (2006) indicates that employees require basic information security knowledge for a secure culture to successfully be instilled in the organisation. Ruighaver and Maynard (2006) indicate that the focus of security culture is on the end-user, however there is a management component, and it needs to be considered from a management perspective. Da Veiga (2016) also considers the individual and organisational levels of security culture, and also includes national and international culture. It is therefore important to consider both the organisational and individual levels when instilling a security culture. The Organisation for Economic Co-Operation and Development (2002) (cited by Kortan and von Solms, 2012) provides a few guidelines on the components that constitute a cybersecurity/information security culture. These include:

- The promotion of a secure online environment for all users
- Creating awareness about online risks and the counter measures available
- Increasing the confidence and knowledge of users in information systems and networks, as well as the way in which they are provided and utilised;
- Acting as a frame of reference for the development and implementation of cyber/information security measures
- Encouraging co-operation and information sharing, as appropriate, amongst all the participants in the development and implementation of security policies, practices, measures and procedures.
- Promoting the consideration of security as an important objective amongst all participants involved in the development or implementation of standards.

Ryttare (2019) provides key themes for change management related to cyber security, including: senior management awareness, involvement of all employees, security needs to be highlighted in a positive manner,

there needs to be understanding of roles and consequences, customised training to ensure relevance, interactive learning, feedback channels, rewards, and continuous change efforts. Jobraj and van Niekerk (2015) reflected on an organisational cyber security awareness approach following the ADKAR change management model, where the focus was on the individual, departmental, and organisational levels. The main themes corresponded to those highlighted by Ryttare (2019), and the activities to achieve these considerations were: an interactive roadshow with activities, articles in internal publications, e-mail alerts, flyers and posters, screen savers and pop-ups, and table-top exercises for the executives (Jobraj and van Niekerk, 2015).

2.2 Change Management

Change management can be defined as the processes, tools and techniques involved in managing the people approach to change with the objective of achieving a successful business outcome (Prosci, 2020).

With reference to Burnes (2004) change is a continual characteristic of the organisational environment, at both the operational and strategic levels. It is important to note that organisational change and organisational strategy must be aligned to each other (Barney, 2004). According to Graetz (2000: 550) many would agree that the primary task for management today is the leadership of organisational change especially with increasing global deregulation and the rapidly changing nature of technological innovation. According to By (2005) are three main phases to change management which includes:

Phase 1: Preparing for Change
This Phase entails defining the change management strategy, preparing the change management teams and the development of the change model. The key objective to Phase 1 is to identify the points of resistance and establish mitigating mechanisms for the resistance to the change.

Phase 2: Managing the Change
This Phase involves the creation of change management plans and the action plan to be implemented. The main objective of Phase 2 is the development and implementation of the resistance to change management plan.

Phase 3: Reinforcing the Change
Phase 3 entails ensuring the success of the change that has been implemented by collecting and analysing feedback, identifying gaps while managing resistance as well as implementing any corrective actions.

The Resource Based View and the ADKAR frameworks/models conceptualise the ideals of the change management process and are discussed further in Sections 2.3.1 and 2.3.2.

2.3 The Change Frameworks/Models

There are two relevant frameworks/ models pertaining to change management that will be briefly described in Sections 2.3.1 and 2.3.2. The two frameworks/ models are the Resource Based View (RBV) model and the ADKAR model.

2.3.1 The Resource Based View (RBV) Framework/Model

RBV is often regarded as a common approach used by organisations to achieve competitive advantage. The approach emerged in the 1980s as its supporters believed that the sources of competitive advantage were based internal to the organisation. The supporters are of the opinion that it is much easier in the exploitation of external opportunities through existing internal resources. Within the RBV model resources become an imperative element in assisting companies achieve better organizational performance. According to Zaini, Masrek, Sani, & Anwar (2018), the foundation for competitive advantage lies in the application of valuable tangible or intangible resources available to a company. Tangible assets refer to the physical which includes property (land and buildings), equipment (machinery) and capital. These physical resources can simply be acquired and provide little to no real advantage to companies on a long-term basis, as competitors can easily obtain similar if not identical assets.

Intangible assets are considered as having no physical presence; however, these can still be owned e.g. brand reputation, intellectual property. These intangible assets accumulate over time and is not easily available in the open market. Intangible resources usually stay within a company and are the main source of sustainable competitive advantage. With reference to Zaini, Masrek, Sani, & Anwar (2018), information security is built on

the notion that an organization has the capability to extend its competitive advantage by simply providing information resources confidentially and immobile through practices that would enhance its secrecy and security (Nelson & Romer, 1996). Within a cyber security context, there can be two different competitors: rival corporations in traditional business competitions, and those who have malicious intent against the organisation, for instance to steal funds through scams. Therefore, a security culture can form a competitive advantage against rival companies in that clients are more confident in the organisation's ability to maintain operations and protect their personal details compared to rival companies. In a pure security sense, improved security awareness or culture makes it more difficult for scams to be effective, providing improved competitive capability against hackers (i.e. greater resilience).

RBV consists of two main assumptions on the resources, which entail them being heterogeneous and immobile.

Heterogeneous refers to the assumption that the skills, capabilities and other resources that organizations own varies between organisations, thereby allowing varying strategies to promote competitive advantage. Companies usually reuse or replicate what each one does, allowing for perfect competition. However, in reality this does not occur as some companies, which are exposed to the same external and competitive forces (same external conditions), are able to implement different strategies and outperform each other. Therefore, RBV assumes that companies achieve competitive advantage by using their different bundles of resources.

Immobile refers to the assumption that resources are not mobile. Therefore, they cannot move between companies in a short period. Because of the resources' immobility, it becomes extremely difficult for a competitor to replicate strategies. Intangible resources including processes, knowledge and/or intellectual property are usually considered as immobile (Jurevicius, 2013). However, with basic information security knowledge, this may not strictly be the case as this knowledge is universal. Human resources moving corporations may benefit the new employer if the skills and knowledge allow for the new employer to improve its security capability.

2.3.2 ADKAR Framework/Model

The ADKAR model was created by Jeff Hiatt in 2003, with the intention of the developer for it to become a coaching and change management tool to assist employees with the change processes within organisations. The change process within organisations is generally met with contempt and resistance. The ADKAR model assists in the form of a management tool to identify the issues of the change process. ADKAR is an acronym representing the five building blocks instituting successful change illustrated in Figure 2. The building blocks are Awareness, Desire, Knowledge, Ability and Reinforcement.

Figure 2: The Five Building Blocks of ADKAR

Source: Adapted from Prosci (2020)

The five stages can be briefly described as follows (Prosci, 2020):

- **Awareness** refers to the awareness of the need to change. This stage relates to the communication of the vision for the future as well as any other information about the change.
- **Desire** refers to the desire participate and support the change which is often influenced by a number of factors. These may include dissatisfaction in its various forms, personal experience, intrinsic forms of motivation and the possible acquisition of status and/or authority.
- **Knowledge** of how to change. Knowledge empowers staff to understand what the change is as well as the outcome of the change which may include their role in the change. Education and training are usually required to enhance the knowledge, skills, and behaviours of employees. Training and

education are important to ensure the smooth functioning in the "changed" environment. Training and education may be provided through a combination of activities e.g. workshops, retreats, on-line modules. Information provided should be easily available and accessible.

- **Ability** refers to the ability to implement the change on a daily basis and focuses on the application of new skills, processes and behaviours. This stage also takes into consideration the potential issues that may arise with the implementation. During this phase, staff are offered practice time while being coached. Areas of coaching may include for staff to develop an understanding of their new role and responsibilities, process and system changes, and new technology. Generally, activities that will support their function and team dynamics within the organisation. Managements' role is important in this phase for assisting in the elimination or mitigation of any barriers, and in addition may provide expertise to eradicate any obstacles.
- **Reinforcement** to keep the change in place. This stage involves recognition of employees and rewards. The recognition and rewards for employees may include anything from personal recognition, to compensation, and benefits.

With reference to ADKAR change consists of two elements namely the organisation and the employees. The change process will only succeed if these two elements occurs work symbiotically. The stages of the ADKAR model function in a modular manner meaning the stages work independently of each other so if there is an issue with any particular stage, it can be resolved without causing much disruption to any of the other stages. It can be considered as a targeted approach as the ADKAR model focuses on the element/stage with the highest success rate (By, 2005). The ADKAR model can be considered as an evaluative model, providing feedback insight as well as hindsight of the stages.

3. Discussion and Proposed Framework

As part of this paper, a framework has been developed which proposes a combination of the RBV and ADKAR models. The RBV and ADKAR frameworks/models have been considered in line with the three levels of management namely the strategic, tactical and operational levels. Further to this the three elements of information systems and information security are included, people, process and technology. These three can be aligned as the actual systems and corresponding technical controls as a mitigating element; governance, which acts as the control of processes; and, culture referring to the people-oriented element.

As illustrated in **Figure 3**, RBV falls within the ambit of strategic management and for the purposes of an information security culture consists of resources and capabilities which may lead to competitive advantage as previously illustrated in **Figure 1**. The Resources consist of technology, processes and people. The corresponding Capabilities consist of the technical controls, governance and security culture, while competitive advantage consists of increased resilience at the strategic level and improved detection and the minimalization of compromises at the tactical level (assuming the governance, technical controls and culture are effectively implemented). Culture, while pitched at the strategic level, branches down to the tactical level, where the stages (Awareness, Desire, Knowledge, Ability and Reinforcement) of the ADKAR are placed. The possible activities to enable a culture change are aligned to the ADKAR model and are placed in the operational level. The activities (following from Ryttare (2019) and Jobraj and van Niekerk (2015)) consisted of interactive roadshows, roadshows through presentations, table-top exercises for executives, email, posters and on-screen notifications.

At the operational level, a matrix was developed to illustrate the coverage of the elements of the ADKAR model at the tactical level with the activities at the operational level. The full cross represents full relevance, with the half cross representing only partial relevance. As is illustrated in the matrix, the table-top exercises for executives appears most successful in relation to culture as it is relevant for Awareness, Desire, Knowledge, Ability stages and partial relevance for Reinforcement of the ADKAR model due to the interactive nature of the activity. This is followed by the interactive roadshows (full relevance for Awareness, Desire, Knowledge, Ability), which due to the tasks performed as part of the roadshow increases enjoyment and the learning of skills. This is followed by emails, posters and on-line notifications (full relevance for Awareness and Reinforcement and partial relevance for Knowledge), which are particularly useful for reminders of what was covered in the Interactive Roadshows; these also are useful for alerts of specific threats that are imminent or underway. The Roadshows by presentation demonstrate least success with full relevance for Awareness and partial relevance for Knowledge; the impact of these is low due to 'death by PowerPoint'.

The proposed matrix can be expanded with more relevant activities, assessed according to the specific audience(s) within an organisation. The matrix will assist in selecting a range of activities to cover all areas of the ADKAR model for all audience groups.

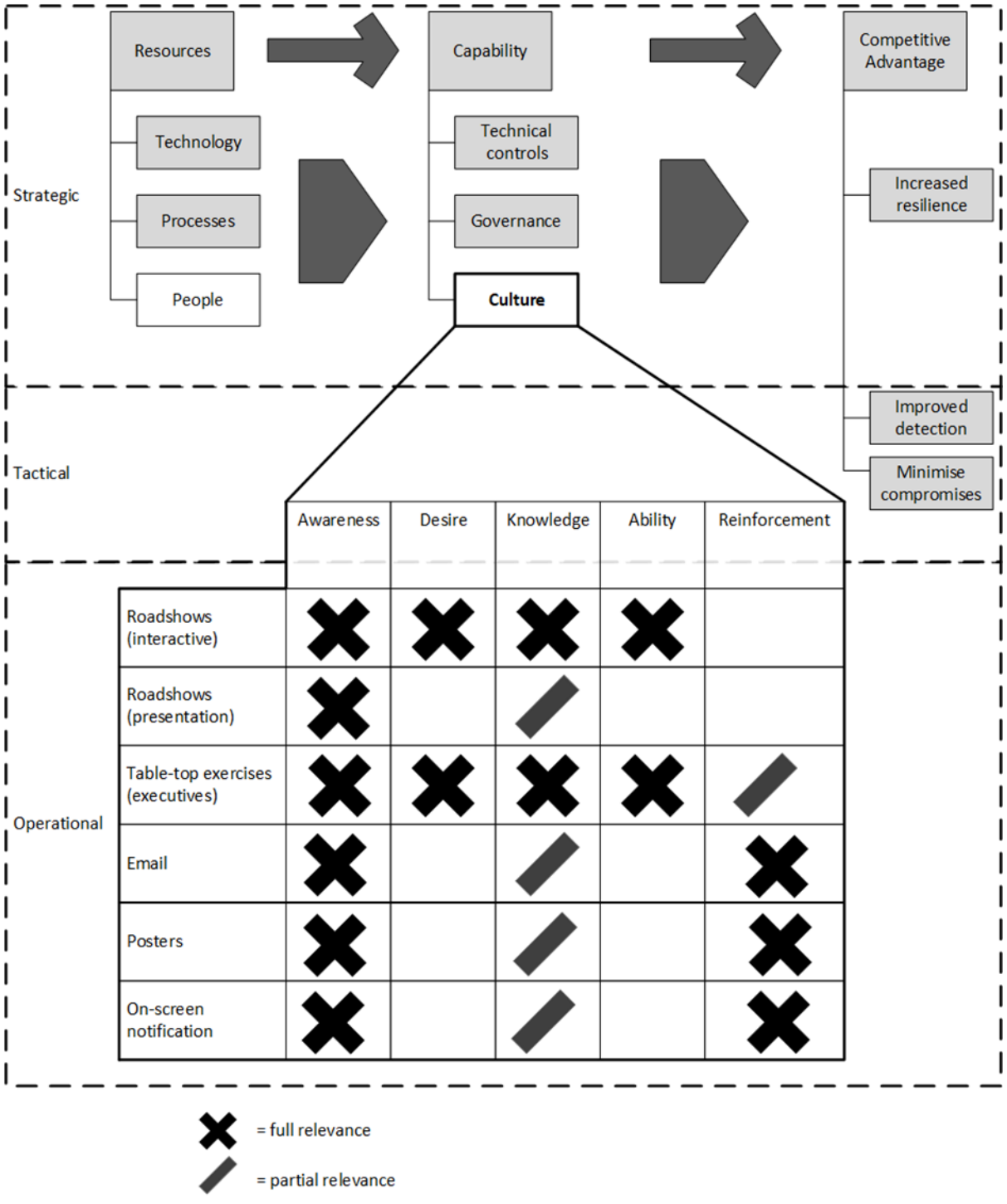

Figure 3: Proposed Framework

4. Conclusion

This paper has provided some insight into the importance of the implementation of an information security culture within organisation. The proposed framework presented a combination of the RBV and ADKAR change management models that may assist in the implementation of an information security culture. An information security culture must consider the human factors in order for an organisation to improve its overall information security efforts. With reference to van Niekerk and von Solms (2006) an understanding of the

various elements of an information security culture is required as the relationships between these elements can become problematic when considering corporate culture. Schein, quoted in Cecil (2013), defines organizational culture as "the formation of a pattern consisting of shared basic assumptions. These assumptions have been studied by a group on the basis that it has found resolutions to the problems of external adaptation and internal integration which can be considered as a product of joint learning". This definition can be used to aid understanding of an information security culture. From this definition, it can be understood that knowledge forms the foundation of corporate culture without which information security cannot be guaranteed. The RBV and ADKAR models combined provides the human factors or elements that need to be considered when implementing an information security culture.

References

Barney, J. B. (1991) "Firm Resources and Sustained Competitive Advantage", *Journal of Management*, 17(1), pp. 99–120.

Burnes, B. (2004) Managing Change: A Strategic Approach to Organisational Dynamics, 4th ed. Prentice Hall: Harlow

By, R. (2005) "Organizational Change Management: A Critical Review", *Journal of Change Management*, 5(1), pp. 369-380.

Cecil. (2013) "Edgar Schein: Organizational Culture and Leadership", #Hypertextual, [online], accessed 18 January 2020, https://thehypertextual.com/2013/01/17/edgar-schein-organizational-culture-and-leadership/

Da Veiga (2016) "A Cybersecurity Culture Research Philosophy and Approach to Develop a Valid and Reliable Measuring Instrument", SAI Computing Conference 2016, July 13-15, London, UK, pp. 1006-1015.

Da Veiga, A. and Eloff, J. H. P. (2007) "An Information Security Governance Framework", *Information Systems Management*, 24(4), pp. 361 – 372.

Graetz, F. (2000)" Strategic change leadership", *Management Decision*, 38(8), pp. 550–562.

INFOSEC Institute. (2020). "Change Management and The CISSP" [online], accessed 18 January 2020, https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-operations/change-management/#gref

ICT Applications and Cybersecurity Division Policies and Strategies Department ITU Telecommunication Development Sector. (2009). "Understanding Cybercrime: A guide for Developing Countries" [online], accessed 18 January 2020, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf

Jobraj, T., and van Niekerk, B. (2015) "Information Security Awareness at a South African Parastatal: Challenges and Successes", presented at the 10th International Conference on Cyber Warfare and Security, 24-25 March, Kruger Park, South Africa.

Jurevicius, O. (2013) "Resource Based View: What makes your company unique?" *Strategic Management Insights*, 14 October, [online], accessed 18 January 2020, https://strategicmanagementinsight.com/topics/resource-based-view.html

Kortan, N. and von Solms, R. (2012) Fostering a cyber-security culture: a case of South Africa, *Proceedings of the 14th Annual Conference on World Wide Web Applications*, 7-9 November 2012, Durban, South Africa.

Nelson, R. and Romer, P. (1996) "Science, Economic Growth, and Public Policy", *Challenge*39(1), pp. 9–21.

PROSCI. (n.d) The PROSCI ADKAR Model, [online], accessed 18 January 2020, https://www.prosci.com/adkar

Ryttare, E. (2019) Change Management: A Key in Achieving Successful Cyber Security, Master's project, Luleå University of Technology, [online], accessed 27 January 2020, https://pdfs.semanticscholar.org/ea5b/1370d1919a50b8830661090df6376a2fe9dc.pdf

Ruighaver, A.B., and Maynard, S.B. (2006) "Organizational Security Culture: More Than Just an End-User Phenomenon", In: Fischer-Hubner, S., Rannenberg, K., Yngstrom, L., Lindskog, S. (eds.), *Security and Privacy in Dynamic Environments*, IFIP International Federation for Information Processing, Volume 201, Springer: Boston, pp. 425-430.

Ruhli, E. (1991) Unternehmungskultur - Konzepte und Methoden. In: E. Riihli and A. Keller, Eds. Kulturmanagement in schweizerischen Industrieuntemehmunnen. Bern und Stuttgart, Paul Haupt Verlag: 11-49, cited in Schlienger, T and Teufel, S. (n.d) Tool Supported Management of Information Security Culture [online], accessed 18 January 2020, https://link.springer.com/content/pdf/10.1007%2F0-387-25660-1_5.pdf

SANS Institute. (2020) Information Security Resources, [online], accessed 18 January 2020, https://www.sans.org/information-security/

Ulich, E. (2001) Arbeitspsychologie. Zurich, vdf, Hochschulverlag an der ETH Zurich,cited in Schlienger, T and Teufel, S. (n.d) Tool Supported Management of Information Security Culture [online], accessed 18 January 2020, https://link.springer.com/content/pdf/10.1007%2F0-387-25660-1_5.pdf

Van Niekerk, J and von Solms, R. (2006) "Understanding Information Security Culture: A Conceptual Framework", *Proceedings of the ISSA 2006 from Insight to Foresight Conference*, 5-7 July 2006, Balalaika Hotel, Sandton, South Africa

Zaini, M. K., Masrek, M. N., Sani, M. K. J. A., and Anwar, N. (2018) "Theoretical Modeling of Information Security: Organizational Agility Model based on Integrated System Theory and Resource Based View", *International Journal of Academic Research in Progressive Education and Development*, 7(3), pp. 390–400.

Zakaria, O. (2006) "Internalisation of Information Security Culture amongst Employees through Basic Security Knowledge", In: Fischer-Hubner, S., Rannenberg, K., Yngstrom, L., Lindskog, S. (eds.), *Security and Privacy in Dynamic Environments*, IFIP International Federation for Information Processing, Volume 201, Springer: Boston, pp. 437-441.