The Concept of Cybersecurity Culture

Kine Reegård

Human-Centered Digitalization, Institute for Energy Technology, Norway. E-mail: Kine.Reegard@ife.no

Claire Blackett

Automation and User Monitoring, Institute for Energy Technology, Norway. E-mail: Claire.Blackett@ife.no

Vikash Katta

Risk, Safety and Security, Institute for Energy Technology, Norway. E-mail: Vikash.Kattta@ife.no

Due to a growing understanding that cybersecurity needs to be addressed also through organizational measures and not by technical measures alone, cybersecurity culture is attracting increasing attention. In this paper, we present findings from a narrative literature review of 69 papers with the purpose to identify the dimensions of cybersecurity culture and how these may be targeted by the organization. The results show that cybersecurity culture is understood as a sub-component of organizational culture comprised of layers that are increasingly more observable. Further, key practices for developing cybersecurity culture resemble those highlighted in the literature on safety culture: management support; policy; awareness and training; involvement and communication; and learning from experience. We conclude with a brief discussion of whether cybersecurity culture and safety culture are two distinct sub-components of organizational culture or can be understood to be overlapping.

Keywords: Cybersecurity, information security, cybersecurity culture, organizational culture, safety culture, literature review.

1. Introduction

With the increased use of new technologies, systems with more connectivity and less isolated from the outside world, the risk of cyber-attacks is high (NSM 2018), and the number of cybersecurity incidents continue to increase as reported by the Online Trust Alliance (2018). The increase in cybersecurity risk is due to several factors ranging from inadequate security and technological development to increasing complexity and sophisticated attacks (NSM 2018).

Maintaining the cybersecurity of an organization is no longer solely the remit of the IT department (NIST 2018; ENISA 2017). Instead it is increasingly understood that cybersecurity needs to be addressed also through organizational measures and not by technical measures alone. Metalidou et al. (2014) report that "Many times organizations overlook the human factor, a factor that security depends upon. Technology is often falsely perceived as the immediate answer to Information Security problems. Information Security is primarily a human factors problem that remains unaddressed" (p. 425). Individuals must also take responsibility for maintaining a secure and vigilant culture at work. Humans do themselves pose a threat and vulnerability to the protection of information (NSM 2018; Ismail & Yusof 2018). Therefore, there is a need to develop and maintain a cybersecurity culture.

Although cybersecurity culture is attracting increasing attention, it is a relatively new concept. Reid & Van Niekerk (2014) argue that there are differences between cybersecurity culture and the more established concept of information security culture, and that the former lacks widely accepted definitions or guidelines. Similarly, Gzaca and von Solms (2017) conducted a literature review of cybersecurity culture and found it to be an ill-defined problem that lack widely accepted key concepts that delimit the culture. They believe that is partly due to the concept being subject to different researchers' perspectives and contexts of applications. This paper seeks to contribute in clarifying the concept of cybersecurity culture in organizations.

In this paper, we present findings from a narrative literature review on state-of-the-art with respect to cybersecurity culture. The purpose of the literature review was to identify the dimensions of cybersecurity culture and how these may be targeted by the organization. In the following we first describe how the review was performed. We then present our main findings in terms of how cybersecurity culture is conceptualized and its content. Finally, we discuss potential links between cybersecurity culture and the more established concept of safety culture.

Proceedings of the 29th European Safety and Reliability Conference.
Edited by Michael Beer and Enrico Zio

Published by Research Publishing, Singapore.
ISBN: 978-981-11-2724-3; doi:10.3850/978-981-11-2724-3_0761-cd

2. Method

A narrative literature review was carried out in two phases. The first phase was performed between October 2017 and January 2018 to understand the state-of-the-practice and state-of-the-art in research and industry in terms of addressing human behavior in cybersecurity culture. A literature search was performed using electronic journal databases that are accessible by the Institute of Energy Technology (IFE) researchers. These were: Google Scholar, IEEE Explore, ScienceDirect, SpringerLink and Elsevier. A general web search was also performed for relevant published literature, using the Google search engine. The searches were conducted using keywords such as: "safety culture"; "security culture"; "cybersecurity culture"; "culture maturity model"; and "information security". A total of 83 documents were identified, of which 59 were selected for screening. The main criteria used to determine relevance were: acknowledgement and discussion of the human role in security culture; experience with implementing security or cybersecurity measures; adaptation or use of culture maturity models; and identification of knowledge gaps and/or research needs in this area.

A second search was conducted in June 2018 in which the outcome of interest was to identify dimensions of cybersecurity culture and state of art in managing cybersecurity culture in organizations. The search was performed in the databases of ScienceDirect, IEEE Explore and Web of Science using the search string "cybersecurity OR information security AND organizational culture". The search produced a total of 391 papers, of which 70 were considered relevant for abstract screening. The inclusion criteria used were: Published in 1995 or later; written in English; industry manuals, technical reports, empirical studies, theoretical studies or experience reviews; organizational focus; full text available; and institutional access. 59 papers were selected for full review. Among these, four papers overlapped with the selected papers from the first phase. In total, 69 papers were reviewed.

3. Results

Cybersecurity is a relatively new concept that first appears in literature within the last twenty years or so. Cybersecurity culture is an even newer phenomenon. Ruighaver et al. (2007) confirm that "It was not until the start of this century that researchers first began to recognize that an organization's security culture might be an important factor in maintaining an adequate level of information systems security in that organization" (p. 56). As such, there is relatively little written about this phenomenon.

The terms "cybersecurity" and "information security" are often used interchangeably in the literature, although there are differences between the two. Von Solms & van Niekerk (2013, p. 101) argue that "Information security is the protection of information, which is an asset, from possible harm resulting from various threats and vulnerabilities. Cyber security, on the other hand, is not necessarily only the protection of cyberspace itself, but also the protection of those that function in cyberspace and any of their assets that can be reached via cyberspace." They further state that "In information security, reference to the human factor usually relates to the role(s) of humans in the security process. In cybersecurity this factor has an additional dimension, namely, the humans as potential targets of cyber attacks or even unknowingly participating in a cyber attack" (ibid, p. 97). Throughout this paper, the terms will be used interchangeably as it often is in the literature, but with a focus on the more encompassing cybersecurity definition.

Ashenden (2008) consider management of information security to be a "human challenge", referring to a need to understand that individual members of an organization not only have a social identity related to their work, but also bring with them an identity to the workplace. Therefore, any attempt to change or improve cybersecurity must also address the cultural aspects of the organization. It is important, then, to understand what creates and influences culture to effectively understand human behavior and why employees act as they do with respect to cybersecurity.

3.1 *Conceptualization of cybersecurity culture*

The literature on cybersecurity culture views culture as something that can be changed and partly managed. Among the papers we reviewed, the most frequently used conceptualization of organizational culture stems from Schein (1996) who defines culture as "a set of basic tacit assumptions about how the world is and ought to be that a group of people share and that determines their perceptions, thoughts, feelings, and, to some degree, their overt behavior" (p. 11). Organizational culture, then, is viewed as manifested in three levels: tacit assumptions that are beliefs about reality and human nature; espoused values which refers to social principles, philosophies, goals and standards; and artefacts that are visible, tangible, and audible results of activity grounded in values and assumptions (Hatch 1993). This three-layered conceptualization of organizational culture has been the basis for most models or frameworks of information security culture (Connolly & Lang 2012). However, in cybersecurity, some add an additional fourth layer of knowledge, arguing that knowledge will influence the assumptions, values and behaviors (ENISA 2017; Van Niekerk & von Solms 2010). Figure 1 illustrates the proposed layers in cybersecurity culture.

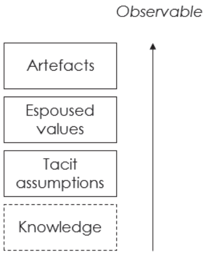


Fig. 1. Illustration of the layers in cybersecurity culture, increasingly more observable at the top layers.

The layers of cybersecurity culture are interconnected (Van Niekerk & von Solms 2010); Understanding each may be necessary for ensuring implementation of adequate measures. For example, Hedström et al. (2011) find that understanding the values that drive people's actions can contribute to a greater understanding of compliance issues with information security policies in that non-compliance may be a result of competing values between the policies and the values that employees emphasize in conducting work. However, values and assumptions are often the more difficult layers to address as these must be inferred from what members of the organization say and do. Consequently, most literature on cybersecurity culture address the observable layer of artefacts and behaviors.

3.1.1 *Content of cybersecurity culture*

As previously noted, some add a fourth layer of knowledge in their models of cybersecurity culture instead of treating it as a sub-component of the three original levels. Van Niekerk & von Solms (2010, p. 486) argue that "this adaptation is necessary because in an information security culture the requisite knowledge cannot be assumed to be present." However, there is little specific mention of the content of such a fourth layer in the literature on cybersecurity culture in general, or it is indirectly addressed through the three other layers. Therefore, in the following, we adhere to the original three layers.

Ashenden & Sasse (2013) argue that viewing information security as an integral part of conducting business is important for avoiding contradictory narratives in the organization that can reduce the effectiveness of cybersecurity roles and measures. A related assumption is whether cybersecurity is primarily an organizational issue, or a technical issue. The view of cybersecurity as something static versus dynamic (Ruighaver et al. 2007) is also an example of tacit assumptions and "change" is therefore included as a dimension in some cybersecurity frameworks (Da Veiga & Eloff 2010; Da Veiga & Martins 2017). As cybersecurity essentially deals with risks, it is frequently emphasized that cybersecurity is a continuous process of identifying, assessing and responding to risks (ENISA 2017; Knapp et al. 2009; NIST 2018; Trim & Lee 2010). Consequently, a mature cybersecurity culture is associated with fostering security awareness and risk perception and being sensitive to changes in threats. The beliefs regarding humans and their behavior in cyberspace is a highly relevant assumption when addressing cybersecurity culture. Employees are often seen as the weak link in cybersecurity. Different approaches to reducing the insider threat can be related to the organizations' belief regarding humans as a liability versus an asset in cybersecurity: to ensure technical controls to reduce or mitigate the risks posed by employees, or to focus on empowering the employees to contribute to the organization's security.

The assumptions matter as these are linked to the espoused values and the rationale of the organization in how to best manage cybersecurity and cybersecurity culture (Barton et al. 2016; Al-Izki & Weir 2016). For example, an organization that views cybersecurity as integral to business is likely to strive for balance between cybersecurity goals and goals of other business areas. Such goal and value congruence are frequently mentioned as important for successfully implementing cybersecurity measures (Ashenden 2008; Ashenden & Sasse 2013; Flores et al. 2014; Greig et al. 2015; Hedström et al. 2011; Karlsson & Hedström 2017; Kearney & Kruger 2016; Kolkowska & Dhillon 2013; Kolkowska et al. 2017). Another related value is whether cybersecurity is seen as a responsibility of the whole organization or specific parts of it. Some literature addresses the issues that technical personnel may have if they are left to manage cybersecurity in isolation. For example, Ashenden & Sasse (2013) provide an account of Chief Information Security Officers' (CISO) struggle between contradictory pulls in the organization that rendered their role and efforts in cybersecurity less effective by needing to seek constant buy-in from employees.

The beliefs and values of the organization about cybersecurity translate into observable behaviors and practices (or non-practices). Within the observable layer of cybersecurity culture, several behaviors and practices are addressed in the literature. Of the most frequently mentioned are top management support through active participation, championing and/or financing of cybersecurity activities (Al-Izki & Weir 2016; Ashenden 2008; Ashenden & Sasse 2013; Barton et al. 2016; Bernik & Prislan 2016; Da Veiga & Martins 2017; Karyada et al. 2005; Knapp et al. 2009; Said et al. 2014; Soomro et al. 2015; Steinbart et al. 2018), cybersecurity awareness and training programs (Al-Izki & Weir, 2016; Ashenden & Sasse, 2013; Da Veiga & Martins 2017; Knapp et al. 2009; Ruighaver et al. 2007; Soomro et al., 2015), and cybersecurity policy (Al-Izki & Weir 2016; Bernik & Prislan 2016; Choi 2016; Da Veiga & Eloff 2010; Da Veiga & Martins 2017; Karlsson et al. 2017; Knapp et al. 2009; Ruighaver et al. 2007; Soomro et al. 2015).

3.2 *Cybersecurity culture practices*

The literature on cybersecurity culture often aim to identify how organizations can develop their cybersecurity culture. In the following, we describe the main practices that are addressed.

3.2.1 *Management support*

One of the most reported key influencing factors is the support of management. Such support can come in a variety of ways, from willingness to financially invest in initiatives and advocating for cybersecurity, to the organization of the cybersecurity function and follow up on cybersecurity work and status. Management support is crucial for creating and maintaining focus on cybersecurity and heavily influential on the performance of other cybersecurity practices. For example, Karyada et al. (2005) found active participation and visible support by top management to be of major importance to formulation and implementation of information security policies.

The importance of management support is further explained by Van Niekerk & Von Solms (2010) who argue that the observable behavior in the organization stem from employees attempting to meet management demands and the knowledge they possess that enable them to do so. They argue that it is primarily knowledge that provides the employees with means to change their behavior. Consequently, management set the focus and demands of the organization, but they need also to empower employees to comply with those demands. Knowledge is also likely to be important in shaping management's support. Barton et al. (2016) provide interesting results that suggest that senior management's observations and perceptions of information security implementation in other organizations influence their own beliefs regarding information security.

3.2.2 *Cybersecurity policy*

With the understanding that cybersecurity culture is a management issue, it follows that one of the key practices is to establish an internal policy to demonstrate management intent and the importance of cybersecurity, as well as to provide overall guidance (Knapp et al. 2009).

Karlsson et al. (2017) note the importance of finding a balance between the management and employee perspectives to make such policies useful. From the employee perspective, they propose ten quality criteria that are centered around the policy's external and internal congruence with current work practice, that it does not introduce any goal conflicts, and that it has clear target groups and clarifies responsibilities and expectations. Knapp et al. (2009) outline a cyclical process model that demonstrates how information security policy is an artefact that results from a dynamic process and that should itself be dynamic, i.e. frequently updated in accordance with the information provided from other activities and changing risks. Similarly, Karyada et al. (2005) argue that the application of information security policies is dynamic in nature and that it is necessary to understand the contextual factors that may affect its adoption. In line with the point made by Karlsson et al. (2017) regarding the employee perspective in policy development, Hedström et al. (2011) argue that "Information security management has to more clearly involve users in the design and implementation of information security controls. […] it is important to identify areas of conflict between security procedures and legitimate professional work values and involve professionals in reconciling these conflicts" (p. 381). Hence, the employee perspective is part of the contextual factors that may influence policy adoption and should be addressed through the policy process.

3.2.3 *Cybersecurity awareness and training*

One of the cornerstones in shaping cybersecurity culture is knowledge, both of management and employees. Metalidou et al. (2014) identified five factors that can seriously impact how people behave with respect to information security: lack of motivation, lack of awareness, inaccurate beliefs about behaviors or risks, risky behavior and inadequate use of technology. They conclude that "information security awareness is the key to mitigate security threats caused by human weaknesses" (ibid, pp. 427).

Brattås (2015) points to a significant weakness in attitudes towards cyber security in the maritime industry in that "cyber security is often considered a technical issue that is delegated to the IT department or Chief Information Officer (CIO) of companies" and "that there often is doubt about whether cyber threats actually are real, and if they are relevant to own [sic] company" (p. 30). Cone et al. (2007) argue that users may also have apathy towards cyber security threats and "often take an ostrich-like attitude toward the security of the information systems they use, believing that there is little that they can do to mitigate this onslaught of problems" (p. 63).

To increase awareness of cybersecurity, the organization must ensure that the training is tailored to the target population as "it cannot be assumed that the average employee has the necessary knowledge to perform his/her job in a secure manner" (Van Niekerk & Von Solms 2010, p. 478). Pfleeger & Caputo (2012) agree, stating that most practitioners (i.e. users and developers) "do not have a common understanding of security" and "do not have a heightened awareness of how security can affect all of their job functions and roles" (p. 602). Cybersecurity awareness training should consider that different roles may have different knowledge and training needs. For example, Choi (2016) found that educating and training information security managers to exert transformational leadership positively affected information security effectiveness. Consequently, training that supports their change agent role can positively impact the overall awareness in the organization by empowering them to explain and persuade people at all organizational levels about what cybersecurity is and how the risks can affect their areas of responsibility. Furthermore, Thsohou et al. (2015) argue that "people interpret and internalize risk-related information through the lenses of cognitive and cultural bias. […] Without acknowledging and addressing their effect in human information processing and decision making, security awareness programs fail to address individual behavior traits and learning needs" (p. 139). Consequently, care should be taken to ensure that the content and type of training is fitting to the target group(s).

It is also important that cybersecurity training is interesting and engaging. Cone et al. (2007) note that "many forms of training fail because they are rote and do not require users to think about and apply security concepts" (p. 63). They claim that gamification, in addition to keeping trainees engaged, can enable trainees to develop tacit knowledge through role-playing and scenario-based application of skills and technologies that enhance their understanding.

A third point to note with training is that it should be considered a continuous effort and part of the overall awareness campaign. Pfleeger & Captuo (2012) explain that "behavioral changes take time, so plans for initiating change should include sufficient time to propose the change, implement it, and have it become part of the culture or common practice" (p. 598). Eminağaoğlu et al. (2009) reinforce the need for continuous awareness campaigns and supporting materials to ensure that employees do not forget what they have learned during the initial training and note that that the campaigns must also change over time.

3.2.4 *Involvement and communication*

According to Ruighaver et al. (2007), motivating the organizational members is important because this promotes a continuous reflection on own behavior, how that may influence security, and what they themselves can do to improve security. Lin and Wittmer's (2017) study showed that employees have the potential to positively contribute to information security if their participation is encouraged which, in turn, promotes proactivity: "In their own work experience, employees can identify information security issues as they emerge and creatively address them based on their work experiences and knowledge" (p.5).

Ruighaver et al. (2007) argue that one of the best ways to improve motivation is through broad horizontal participation (i.e. peer-to-peer participation). Ashenden and Sasse (2013) support this argument based on their study of CISO's perceptions and attitudes that may impact on their effectiveness in changing organizational behavior. They conclude that "CISOs need to take a more participative approach if they are to be effective. This will require genuine two-way communication with employees, negotiation and involvement to overcome the often observed 'them' and 'us' relationship" (p. 404). Furthermore, Ruighaver et al. (2007) highlight the importance of having staff responsible for particular security areas with a strong sense of ownership and that this ownership can be influenced by the amount of participation they have in security. Discussing decisions and providing feedback to the roles who have security responsibilities is equally important to ensure accountability.

Similarly, Flores et al. (2014) argue that security knowledge sharing can contribute to mitigate risks. They found that formal security structures and steering committees contribute to knowledge sharing, but that it is really the underlying coordinating processes related to risk management and performance monitoring that are essential for the establishment of knowledge sharing mechanisms. The importance of such knowledge sharing in the organization is further underscored by the reporting of Kearney and Kruger that "the differences in perceptions pertaining to control measures, risks, and severity of risks, are in many cases consistent […]" (2016, p. 54), referring to the intra-organizational groupings of Management, Technology and Users. They conclude that perceptual alignment between the three is a prerequisite for a safe and secure information environment. Consequently, involvement and participation should occur on all levels of the organization, both vertically and horizontally, to facilitate cybersecurity awareness and empower the organizational members to positively contribute to the organization's security.

3.2.5 *Learning from experience*

Ruighaver et al. (2007) state that "any beliefs that the decision makers within the organization have about the quality of security, and about the quality of the different processes used to manage security, are often much more important than the end-user's beliefs about security" (p. 57).

Kearney and Kruger (2016) propose monitoring of specific outcomes to validate or falsify current beliefs regarding the organization's security. Auditing is another example of such a mechanism that can help in increasing the organization's awareness of its internal security environment. However, Ruighaver et al. (2007) note that organizations may succumb to an external focus when having an external audit in which the organization is primarily focused on passing the audit rather than achieving the security they need. Vroom & von Solms (2004) offer a further critique of auditing in that it often does not consider the behaviors of employees, and, instead, propose to use assessment of organizational culture and organizational behavior in parallel. Others also join the proposal of focusing on culture to define targeted improvement initiatives. For example, Da Veiga and Martins (2017) used a measurement tool to establish a baseline of the information security culture in an organization and to infer the effects of targeted interventions as part of a general process of organizational diagnosis. The use of maturity models is another example of how some organizations attempt to establish their current level of security and identify further focus areas for improvement.

An important mechanism that enables learning is incident reporting systems whose primary purpose is to share information on incidents to avoid their reoccurrence or limit the damage they can cause. Sveen et al. (2007) argue that the effectiveness of such systems is often limited by non-technical constraints, and that organizations must take care in implementing such systems to enable its effective use.

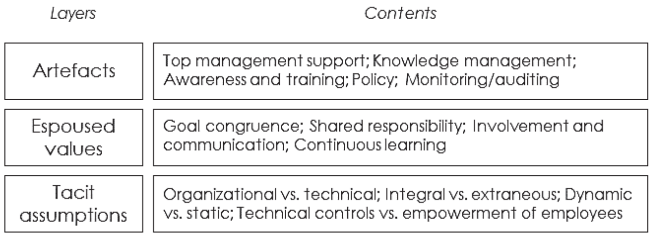
4. Discussion and conclusion

In figure 2 we illustrate the concept of cybersecurity culture in organizations based on the literature we have reviewed.

Cybersecurity culture seems to bear a lot of resemblance to safety culture, both in terms of its conception and the mangerial practices that are emphasized. Wiegmann et al. (2002) summarizes the common attributes referred in the research literature related to safety culture:

- Refers to shared values among a group or organization.
- Is concerned with formal safety issues and is closely related to management and supervisory systems.
- Emphasizes contribution of everyone in the organization.
- Impacts how individual members of the organization behaves at work.
- Is reflected in contingency between reward systems and safety performance.
- Is reflected in an organization's willingness to learn from errors, incidents and accidents.
- Is relatively enduring, stable and resistant to change.

Choudhry et al. (2007) explain that "it is the safety culture of the organization that will influence the deployment and effectiveness of the safety management resources, policies, practices and procedures as they represent the work environment and underlying perceptions, attitudes, and habitual practices of employees at all levels" (p. 1003). The word "safety" could be exchanged with "cybersecurity" to describe what we have found in the literature thus far. It is not surprising, then, that the same managerial practices that are frequently identified to reflect safety culture also apply to cybersecurity culture. The similarity between safety culture and cybersecurity culture is not surprising given that they are both seen as sub-components of the overarching organizational culture (Choudry 2007; Edwards et al. 2013; Guldenmund 2000). As such, one can ask whether these are two distinct sub-components, or partly overlapping. Edwards et al. (2013) state that "the exact nature of safe and unsafe behaviors may differ between organizations, industries, and the targeted level of an organization, thereby permitting different focuses between researchers. However, it is questionable whether culture and, therefore, safety culture, is so differentiated." Knowles et al. (2015) argue that security has a functional purpose related to safety in most industrial control systems and that this aspect has received little, if any, attention in existing standards, guidelines and best practices. Clarifying how these two concepts relate to each other therefore seems appropriate for further research.



Layers	Contents
Artefacts	Top management support; Knowledge management; Awareness and training; Policy; Monitoring/auditing
Espoused values	Goal congruence; Shared responsibility; Involvement and communication; Continuous learning
Tacit assumptions	Organizational vs. technical; Integral vs. extraneous; Dynamic vs. static; Technical controls vs. empowerment of employees

Fig. 2 The concept of organizational cybersecurity culture consisting of layers adhering to Schein's model and the key contents addressed in the literature

In this paper, we present our findings from a literature review seeking to clarify the concept of organizational cybersecurity culture. In contrast to previous literature reviews, we find that the theoretical understanding of cybersecurity culture is mainly consistent, and that it bears resemblance to that of safety culture. However, safety, as well as information security, is mainly within the organization’s control. Cybersecurity, in contrast, extends beyond the organizational boundaries. The existing literature addresses this aspect to little extent. We hope that future research on organizational cybersecurity culture will address this further and investigate the potential influence of factors external to the organization on the organization’s cybersecurity culture and practices.

References

Al-Izki, F. & Weir, G.R.S. (2016). Management attitudes toward information security in Omani public sector organizations. *2016 Cybersecurity and Cyberforensics Conference*

Ashenden, D. (2008). Information security management: A human challenge? *Information Security Technical Report 13*, 195-01.

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

Barton, K.A., Tejay, G., Lane, M. & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers & Security 59*, 9-25.

Bernik, I. & Prislan, K. (2016), Measuring information security performance with 10 by 10 model for holistic state evaluation, *PLoS ONE 11* (9).

Brattås, M. N. (2015). An assessment of cyber security awareness and measures in the Norwegian maritime sector: A focus on shipping companies and equipment suppliers. Master Thesis, Vestfold and Buskerud University College, Norway. Submitted May 2015.

Choi, M. (2016). Leadership of information security manager on the effectiveness of information systems security for secure sustainable computing. *Sustainability 8*, 638-659.

Choudhry, R.M., Fang, D. & Mohamed, S. (2007). The nature of safety culture: A survey of state-of-the-art. *Safety Science 45*, 993-1012.

Cone, W. D., Irvine, C. E., Thompson, M. F. and Nguyen, T. D., (2007). A video game for cyber security training and awareness. *Computers & Security 26*, 63 – 72.

Connolly, L. & Lang, M. (2012). Investigation of cultural aspects within information systems security research. *The 7th international Conference for Internet Technology and Secured Transactions*

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

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

Edwards, J., Davey, J.D. & Armstrong, K.A. (2013). Returning to the roots of culture: a review and re-conceptualisation of safety culture. *Safety Science 55*, 70-80.

Eminağaoğlu, M., Uçar, E. and Eren, S. (2009). The positive outcomes of information security awareness training in companies – A case study. *Information Security Technical Report 14*, 223 – 229.

ENISA (2017). Cybersecurity Culture in Organizations. European Union Agency for Network and Information Security, ISBN 978-92-9204-245-5.

Flores, W.R., Antonsen, E. & Ekstedt, M. (2014). Information security knowledge sharing in organizations: investigating the effect of behavioral information security governance and national culture. *Computers & Security, 43*, 90-110.

Gcaza, N., & von Solms, R. (2017). Cybersecurity Culture: An Ill-Defined Problem. *IFIP World Conference on Information Security Education,* 98-109.

Glendon, A.I. & Stanton, N.A. (2000). Perspectives on safety culture. *Safety Science 34*, 193-214.

Greig, A., Renaud, K. & Flowerday, S .(2015). An ethnographic study to assess the enactment of information security culture in a retail store, *2015 World Congress on Internet Security*

Guldenmund, F.W. (2000). The nature of safety culture: a review of theory and research. *Safety Science 34*, 215-257.

Hatch, M.J. (1993). The dynamics of organizational culture. *The Academy of Management Review 18*, 657-693.

Hedström, K., Kolkowska, E., Karlsson, F. & Allen, J.P. (2011). Value conflicts for information security management. *Journal of Strategic Information Systems 20*, 373-384

Ismail, W.B.W. & Yusof, M. (2018). Mitigation strategies for unintentional insider threats on information leaks. *International Journal of Security and Its Applications 12*, 37-46

Karlsson, F., Hedstöm, K., Goldkuhl, G. (2017). Practice-based discourse analysis of information security policies. *Computers & Security 67*, 267-279

Karyada, M., Kiountouzis, E. & Kokolakis, S. (2005). Information systems security policies: A contextual perspective. *Computers & Security 24*, 246-260

Kearney, W.D. & Kruger, H.A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organization? *Computers & Security 61*, 46-58.

Knapp, K. J., Morris Jr., R.F., Marshall, T.E. & Byrd, T.A. (2009). Information security policy: An organizational-level process model. *Computers & Security 28*, 493-508

Knowles, W., Prince, D., Hutchison, D., Disso, J.F.P. & Jones, K. (2015). A survey of cybersecurity management in industrial control systems. *International Journal of Critical Infrastructure Protection 9,* 52-80.

Kolkowska, E. & Dhillon, G. (2013). Organizational power and information security rule compliance. *Computers & Security 33*, 3-11

Kolkowska, E. , Karlsson, F. & Hedström, K. (2017). Towards analysing the rationale of information security non-compliance: Devising a value-based compliance analysis method. *Journal of Strategic Information Systems 26*, 39,57

Lin, C. & Wittmer, J.L.S. (2017). Proactive information security behavior and individual creativity: Effects of group culture and descentralized IT governance. *2017 IEEE International Conference on Intelligence and Security Informatics.*

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C. & Giannakopoulos, G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. *Social and Behavioral Sciences 147*, 424 – 428.

Nasjonal sikkerhetsmyndighet (NSM). Et sikkert digitalt Norge – IKT-risikobilde 2018

NIST (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. National Institute of Standards and Technology, https://doi.org/10.6028/NIST.CSWP.04162018

Online Trust Alliance (2018). Cyber Incidents & Breach Trends Reports. Review of and analysis 2017 cyber incidents, trends, and key issues to address.

Pfleeger, S. L. and Caputo, D. D., (2012). Leveraging behavioural science to mitigate cyber security risk. *Computers & Security 31*, 597 – 611.

Reid, R. and Van Niekerk, J., (2014). From Information Security to Cyber Security Cultures Organizations to Societies. *Inf. Secur. South Africa (ISSA), IEEE*, 1-7.

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

Said, A.R., Abdullah, H., Uli, J. & Mohamed, Z.A. (2014). Relationship between organizational characteristics and information security knowledge management implementation. *Procedia - Social and Behavioral Sciences 123*, 433-443.

Schein, E.H. (1996). Three cultures of management: The key to organizational learning. *Sloan Management Review 38*, 9-20.

Soomro, Z.A., Shah, M.H. & Ahmed, J. (2015). Information security management needs more holistic approach: A literature review. *International Journal of Information Management 36*, 215-225

Steinbart, P.J., Raschke, R.L., Gal, G. & Dilla, W.N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations & Society*, 1-15

Sveen, F.O., Rich, E. & Jager, M. (2007). Overcoming organizational challenges to secure knowledge management. *Inf Syst Front 9*, 481-492.

Thsohou, A., Karyda, M. & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & Security 52*, 128-141.

Trim, P.R.J. & Lee, Y-I. (2010). A security framework for protecting business, government and society from cyber attacks, *2010 5th International Conference on System of Systems Engineering*

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

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

Wiegmann, D.A., Zhang, H., von Thaden, T., Sharma, G. & Mitchell, A. (2002). Safety culture: A review. Technical Report ARL-02-3/FAA-02-2. Illinois: Aviation Research Lab, Institute of Aviation.