# Factors associated with the cybersecurity culture: a quantitative study of public e-health hospitals in South Africa

Emilia N Mwim[1][0], Jabu Mtsweni [2][1] and Prof Bester Chimbo [3][1]

[1] Department of Information System, School of Computing, College of science Engineering and technology, Unisa, Florida, South Africa
[2] Head of Information and Cyber Security Centre, CSIR, Pretoria, South Africa
SILGA, Stellenbosch University, Stellenbosch, South Africa
[3] Department of Information System, School of Computing, College of science Engineering and technology, Unisa, Florida, South Africa

mwimen@unisa.ac.az, mtsweni@gmail.com, chimbb@unisa.ac.za

**Abstract.** The healthcare sector has become a high target of cyber threats due to the nature of the industry and potential of personal and confidential information. Human related factors have proven to be the major contributor to the challenges confronting cybersecurity across different domains. Addressing the human problem in cybersecurity calls for a coordinated and an inclusive cybersecurity measure like Cybersecurity Culture (CSC). CSC has been argued as an essential cybersecurity measure that contributes to changing humans' behaviour in terms of their attitude, beliefs and values as well as their performance towards security that may impact positive security behaviour. Research work in CSC is limited in healthcare sector as existing works focus on financial and insurance sectors. Following a quantitative research method, this paper conducted an empirical study to identify CSC factors that are associated with public e-health hospitals in South Africa. The findings revealed that under the element of preparedness are issues of awareness and competency as factors that are highly associated with CSC. Under management, lack of cybersecurity team, top management support as well as rewards and punishment were identified. Factors relating to responsibility and environmental elements were also identified to have association with CSC among Information Technology users. Identifying the factors would assist in the development of a framework for establishing CSC in the hospitals which can form a base for hospitals in developing CSC in their settings.

**Keywords:** Healthcare, cybersecurity culture, cybersecurity culture factor, e-health

# 1 Introduction

The positive effect of technological innovations in the modern business process has grown rapidly causing operation at various sectors of life including the healthcare sector to rely vastly on Information Technology (IT) systems. Growing reliance on IT systems in the delivery of healthcare (e-health) has proven to improve quality of health care through increased healthcare efficiency, patient accessibility, empowerment, effectiveness, participatory consultation and medical diagnosis [1]–[3]. The European Union 2012-2020 e-health Action plan indicates e-health ability to benefit variety of stakeholders starting from citizens, patients, healthcare professionals to health organisations and public authorities [4]. Over the years, the benefits of e-health has grown to include: patient diagnosis, treatment and care, improve efficiency, effectiveness and quality of health services to patients, faster & easier access and sharing of healthcare data, decrease healthcare cost through administrative cost, system accuracy, participatory consultation, time saving and patient monitoring [3], [5]–[7].

However, the increasing dependence on IT systems has made the sector highly vulnerable to cyber threats and risks affecting the security, privacy, availability and integrity of healthcare data and systems. Recently, healthcare institutions have become a heavy target of cyber threats like ransomware, Denial of Service attacks (DoS)) and data breaches [8], [9] placing the sector at number 2 of the largest data breach industry according to reports by [8], [10], [11]. Security reports and other researchers have showed that a substantial proportion of cybersecurity incidents in this sector are due to human related issues and factors [9], [12]–[15].

The challenge is that the cybersecurity solutions applied towards addressing cyber threats had predominately focused on technological measures [16], [17] and this had proven insufficient on its own in addressing cybersecurity issues due to lack of or limited inclusion of the human factor [16], [18]–[21]. This intensifies the call for all-inclusive cybersecurity measures in the sector and research has argued that cybersecurity culture is the solution as it accommodates element of human factors and their culture (beliefs, value, and attitude) [22]–[24].

Although research in the area of cybersecurity culture is still at its infancy stage [25]–[27], it is beginning to gain moment, but the healthcare sector is not receiving sufficient attention as a highly targeted sector by cyber criminals since work in CSC tend to focus on sectors like finance and insurance sectors [28], [29].

To contribute to this area, empirical work was conducted to identify the CSC factors that are associated with the public healthcare institutions. The paper presents the research aim and question in section 2. Background on CSC including CSC factor elements are provided in sections 3 and 4. The method followed in conducting the empirical research and the results are presented in section 5. In section 6, we present the discussion and the contribution made by this research. Finally, section 7 indicate the future work and concludes the paper.

## 2 Research aim and Question

In this study, an empirical research was conducted using a quantitative research method with a research aim to identify factors of CSC elements that are associated with cybersecurity culture in the public e-health setting in South Africa. The main research question answered in this paper is:

> What are the factors that are associated with cybersecurity culture in the public e-health institutions in South Africa?

## 3 Background

### 3.1 Cybersecurity culture and its factors

Based on the systematic review conducted by [30], an informed and a comprehensive definition of cybersecurity culture was developed. This research adopts the definition as it provides an understanding of what constitutes cybersecurity culture.

"Cybersecurity culture is defined in this research as a measures (e.g. cybersecurity education, training and awareness) used as a performance tool by management (guided by policies and procedures) to change human characteristics and their socio-cultural measures (e.g. attitudes, assumptions, beliefs, norms, knowledge, perceptions, skills, behaviors and practices) to achieve cybersecurity at all levels of cybersecurity culture (i.e. international, national and organizational) to hinder intentional and unintentional cyber-harms"

The above definition was developed in [30] and adopted in this research because it emerged from definitions [28], [31]–[35] that have their basis on the related concepts of security culture, information security culture, and organizational culture.

The components that emerge out strongly in the existing definitions of cybersecurity culture [23], [31], [36] are the importance of human characteristics, context (environment) and CSETA (Cybersecurity Education, Training and Awareness). The above definition was developed to center around these elements that are considered important when cybersecurity culture is discussed.

Significant efforts have been made to address cybersecurity challenges, however there is a concern that the majority of those efforts have primarily been on technological solutions [16], [18], [34], which have independently proven insufficient to address cybersecurity issues because of threats emerging from human-related problems [16], [18], [37], [38]. This necessitates the implementation of non-technical (human factor) solutions, and cybersecurity culture is one of such options.

A number of factors have been identified to be critical in relation to cybersecurity culture development, maintenance, best practices and frameworks [22], [23], [26], [29], [39]. Examples of the top 10 cybersecurity culture factors highlighted in literature are depicted in Table 1. For the full list of the identified factors and for the full explanations of all the factors together with their related literature, see [30].

**Table 1.** Cybersecurity culture factors.

| Cybersecurity Culture | |
|---|---|
| Training and education | Cybersecurity champion or team |
| Awareness | Organisational culture |
| Leadership support | Budget and resource |
| Cybersecurity policy | Human behavior |
| Knowledge and understanding | Engagement and encouragement |

The identified factors are not only elements or factors that constitute CSC; factors that characterize, challenge, influence, and are used in the development of CSC can also be considered. The absence of these factors are (1) regarded as challenges that inhibit the cultivation and improvement of cybersecurity culture [26], [40] and (2) are considered critical source factors for developing and strengthening of CSC [40], [41]. Cybersecurity culture is an emerging field of research that is beginning to gain momentum recently with the development of factors, frameworks, models and implement steps [28]–[30], [42]–[44]). Not-with-standing that, majority of empirical research in the literature on cybersecurity culture focused attention on other sectors [28], limited empirical work exists in the e-health [45]. This is considered a limitation in research which calls for more work and this research is positioned towards contributing in bridging the gap.

## 4 Cybersecurity culture factors and elements framework

With the help of existing cybersecurity culture frameworks or models and the framework of Human Factors Domain (HFD) [28], [34], [35], [42], [43], [46] the consolidated cybersecurity culture factors were identified, mapped and categorized into four elements of *preparedness, responsibility, management* and *environment*. Preparedness, responsibility, and management elements relate to factors that are found at the internal organizational level while environment element factors are found at the external non-organisational level.

Preparedness and responsibility relate to the organisational cybersecurity culture factors that are associated with individuals (employees). The elements of preparedness and responsibility relate to the way employee acts towards cybersecurity as such they are associated with human and behavioural factor or dimensions of beliefs, values and attitude which are the ground of organizational culture model layers [27], [28], [35], [42], [47], [48] Ultimately employees' behaviours which influence and are influenced by the culture of the organization as argued diversely by [28], [35] together with other factors (internal and external) play important role in achieving cybersecurity. Employees can be anyone operating at the leadership, group (department) and individual layer of the organization [28], [35], [42]. This means that employees' behaviour can be official or unofficial and intentional or unintentional cybersecurity behaviours portrayed by individual at the leadership, departmental and individual level [28], [35], [42] and added competency to the human individual level elements which supports the dimension of knowledge that extended the information security model [47], [48].

**Preparedness** includes human individual factors like their knowledge, awareness, self-efficacy, training and change of old practice [28], [42], [46]

**Responsibility** includes attitudinal factors such as employee practices and personality like the priority given to cybersecurity culture, their perception, acceptance, norms, and participation in relation to cybersecurity culture activities. Responsibility also relates to performances like monitoring and control, compliance as well as rewards and punishment [28], [46].

**Management** just like preparedness and responsibility is an internal cybersecurity culture element, management refers to actions and steps taken at the organizational level. Organisational factors are also referred to as organisational mechanisms [28]. Therefore, the factors related to this element are under the control and authority of organization management [28], [34], [42], [46]. Examples of management factor element include cybersecurity policy, practices, security governance, organizational learning, assets, cybersecurity culture leadership, and communication issues [28], [42], [46].

**Environment** relates to the external non-organisational factors of cybersecurity culture. The element of environment includes factors outside the organization that the organization has limited control over. Examples of environment factors include emergence of new technology, laws and regulatory requirements, competition from peer institutions, national or societal culture [28], [34], [35], [46].

### 4.1 Model of the cybersecurity culture elements

The various elements of the cybersecurity culture factors discussed above are depicted using the model in Figure 1.

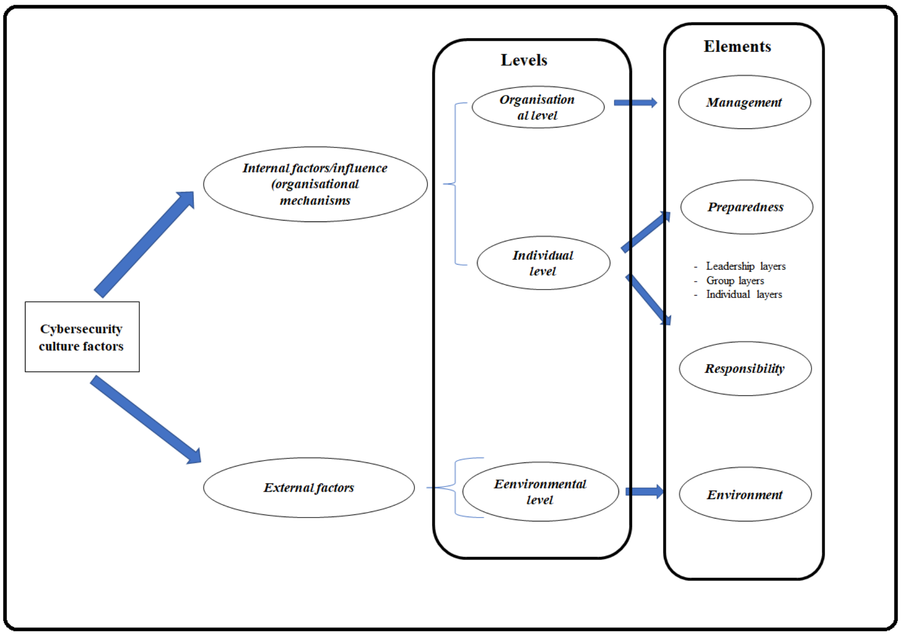

**Figure 1.** Model of cybersecurity culture elements

It is evident from the figure 1 that cybersecurity culture factors correspond to the domains (called elements in figure 1) of HFD framework. As indicated in section 3, the management domain relates to factors that are performed at the organisational level by the management of the organization. Preparedness and responsibility are associated with factors performed by humans and their culture at the individual level. Lastly the environment domain relates to factors at the environmental level.

The comprehensiveness of the CSC factors elements modelled in figure 1 is improved by relating them to the different categories of CSC factors. Organisational and individual level factors are related to the internal organizational factors while environmental level factors are connected to the external organizational factors. This is also mostly true with categorization of the domains on the HFD framework. According to the framework, responsibility and preparedness are regarded as employee (individual) dimension and management domain falls under organization dimension. The limitation is with environment domain which the authors categorised under organization dimension as a theme. With the help of well-established CSC frameworks, this is reformulated to a new thematic name called external factors in this paper. These CSC factors elements were used as the based construct upon which the research empirical instruments were grouped for the instrument design, data collection and analysis. The next section presents the method that was followed in conducting the empirical work.

# 5 Research method

The paper followed a quantitative research method conducted through a manual and emailed based survey. Consent to participate was included as part of the questionnaire which was designed using the four CSC factor elements as the basis of the survey sections. The questionnaire consisted of five sections. Section A was used to collect demographic information of the participants. Section B, C, D and E measured the elements of preparedness, responsibility, management and environment respectively using agreement legend. The rating scale consists of five statements that participants responded to. The statements are based on five agreement points indicating 1- strongly disagree to 5-strongly agree.

The survey instrument was piloted with 12 participants in a similar setting being a hospital to evaluate the instrument and the feedback received was used to correct and improve the instrument for research data collection. The categories of participants who contributed to the survey included only medical and administrative workers who make use of internet-based IT systems in their daily operations in the hospital and who have access to important confidential information. A total of 99 participants completed the questionnaire from the two hospitals in the Mpumalanga province. The questionnaire was distributed manually to the participants in their place of work, and some were emailed to doctors who were too busy to complete it manually at their facility. The small sample size was because only limited number of targeted audiences makes use of internet-based IT systems in their daily operations in the hospitals where the data was collected.

Statistical Package for Social Sciences (SPSS) and Analysis of Moment Structures (AMOS) version 28.0 were used for the data analysis. Frequency tables were created to represent the demographic information of the participants. Cronbach's Alpha (α) was used to measure the internal consistency of the elements questions and an acceptable threshold value of 0.70 according to [49], [50] was considered. Descriptive statistics were used to summarize the mean and standard deviation of the elements measured and their individual items. Finally, Pearson correlation was used to measure the relations between the elements.

# 6 Results

## 6.1 Demographical Information

Table 2 shows the demographic information of the 99 participants that responded to 120 questionnaires that were distributed. The demographic analysis covered includes the age, and gender. The analysis depicted in terms of gender, 43.4% of the participants were male and 56.6% were female. in Table 2 shows that the research participants are spread across the different age ranges. Majority of the participants 32.3% fall between 21 – 30 age range. While 29.3% of them are under the age of 31 – 40, 20.2% percent are aged 41- 50, and the measure participants between the age of 51 – 60 and 60+ contributed 15.2% and 3% respectively.

**Table 2.** Demographics of the participants

| | | Frequency | Percentage |
|---|---|---|---|
| | Male | 43 | 43.4 |
| | Female | 56 | 56.6 |
| Gender | Total | 99 | 100.0 |
| | 21- 30 | 32 | 32.3 |
| | 31- 40 | 29 | 29.3 |
| Age | 41- 50 | 20 | 20.2 |
| | 51- 60 | 15 | 15.2 |
| | 60+ | 3 | 3.0 |
| | Total | 99 | 100.0 |

### 6.2 Construct reliability

The Cronbach Alpha values of all the research constructs were above or equal to the acceptable value of 0.7. The result in Table 3 shows that the values range from 0.786 to 0.900.

**Table 3.** Construct reliability

| Constructs (factors) | Cronbach's Alpha |
|---|---|
| Awareness and Competency (A&C) (preparedness) | 0.900 |
| Attitude and Behaviors (A&B) (responsibility) | 0.786 |
| Management Cybersecurity Practices (MCP) (management) | 0.855 |
| Healthcare Environment (HE) (Environment) | 0.786 |

### 6.3 Descriptive statistics for the cybersecurity culture factors

Table 4 depicts the descriptive statistics mean and standard deviation for the constructs studied. Table 4 also shows a combined mean and standard deviation of the elements of preparedness, responsibility, management, and environment measured respectively.

The descriptive statistics for the preparedness show that participants are mostly not in agreement that they have necessary awareness, knowledge and training of all cybersecurity items that tested this element. The indication is shown with a mean score of 2.496. The score of 2.7119 depicted for responsibility on Table 4 indicates that the participants are neutral in most of the cybersecurity attitude and behavioural items that measured the element of responsibility. For management, a mean of 2.5170 was depicted on Table 4 as a signal that participants are largely neutral on management elements items. On the items that measure environment element, a mean of 3.3902 was shown which indicating that participants are neutral on the items of elements.

**Table 4.** Descriptive Statistics

| Constructs | Mean | Std |
|---|---|---|
| Awareness and Competency (A&C) (preparedness) | 2.4963 | .78282 |
| Attitude and Behaviors (A&B) (responsibility) | 2.7119 | .52159 |
| Management Cybersecurity Practices (MCP) (management) | 2.5170 | .61890 |
| Healthcare Environment (HE) (Environment) | 3.3902 | .72256 |

## 6.4 Pearson correlation coefficients analysis

Pearson correlation was used to measure the association between research variables. The aim was to determine the significance of the association between the research variables [51].

**Table 5.** Correlations

| | | A&C | A&B | MCP | HE |
|---|---|---|---|---|---|
| A&C | Pearson Correlation | 1 | | | |
| | Sig. (2-tailed) | | | | |
| | N | 99 | | | |
| A&B | Pearson Correlation | .600** | 1 | | |
| | Sig. (2-tailed) | <,001 | | | |
| | N | 99 | 99 | | |
| MCP | Pearson Correlation | .555** | .536** | 1 | |
| | Sig. (2-tailed) | <,001 | <,001 | | |
| | N | 99 | 99 | 99 | |
| HE | Pearson Correlation | .027 | .287** | .070 | 1 |
| | Sig. (2-tailed) | .788 | .004 | .493 | |

| | | | | |
|---|---|---|---|---|
| N | 99 | 99 | 99 | 99 |

**. Correlation is significant at the 0.01 level Sig (2-tailed).

**. N = the number of participants

Observed correlation depicted on Table 5 are discussed below.

**Preparedness and Responsibility**: The Pearson correlation of preparedness and responsibility was positive (r = .600) and the relationship is statistically significant (p-value < 0.001). This indicates that a more prepared hospital in terms of cybersecurity by providing staffs with the necessary cybersecurity training, education, awareness there would be a more positive attitude and behaviour towards cybersecurity (responsibility) among employee in their institution.

**Preparedness and Management**: These two elements also show a positive correlation (r = .555) and they are statistically significant (p-value < 0.001). This relationship shows that a healthcare institution with a more established cybersecurity practices by their management are likely to be more prepared in terms of cybersecurity issues.

**Preparedness and Environment**: These two elements show no Pearson correlation between them (r = .027) and the (p – value = 0.788) greater than 0.05 significant threshold is sign of statistically insignificant outcome. This is an indication that in the healthcare institution, environmental factors are not regarded as central in relation to how the institutions prepare employees on cybersecurity matters.

**Responsibility and Management**: Although at a moderate level, a positive relationship was also found to exist between responsibility and management indicating a Pearson correlation of (r = .536) and the elements are statistically significant (p-value < 0.001). This is an indication that the more there is a positive or negative action from the management in terms of cybersecurity practices, the more likely there are management engagement and support, exitance of cybersecurity term which could lead to a positive or negative responsibility from employees with regards to their attitude and behaviour towards cybersecurity actions.

**Responsibility and Environment**: The Pearson correlation between these variables were found to be positive but a weak relationship (r = .287) exist. The correlation is found to be significant (p-value < 0.004). This relationship shows that with an increase in the healthcare environment factors that influences employees there could be an increase in the positive or negative attitudes and behaviours of the employee towards cybersecurity.

**Management and Environment**: The result on Table 5 found that no correlation exists between these variables (r = .070) and they were found to be insignificant (p – value > 0.05). This suggests that an increase in the healthcare environment issues could not lead to increase in MCP within the hospital.

# 7 Discussion and contribution

In this section, the research question is addressed in relation to the results presented in the preceding section. This is followed by the contribution of the researchers in this paper.

The main question asked in this paper was
*What are the factors that are associated with cybersecurity culture in the public e-health institutions in South Africa?*

Overall indication based on the Pearson correlation analysis is that the dominating positive correlation between the elements and the highly significant indication are evidence that meaningful association exist between the elements except for correlation between preparedness and environment, and management and environment. A conclusion can be reached that these elements are significantly important in relation to CSC. Therefore, the factors of these elements can be associated with CSC in the e-health organizations.

The results from the analysis of the data further show evidence that preparedness is highly associated with CSC in e-health setting. The preparedness factors which were identified to play a role and therefore need to be taken into consideration when hospitals develop flamework that would assist them in establishing CSC include: providing appropriate cybersecurity awareness, education, and training. This finding confirms what is indicated in e-health literature which highlight lack of training and awareness as among the serious reasons why the healthcare institutions are targeted by cyber-criminals [52], [53]. On the similar note, lack of cybersecurity awareness, education and training which are factors under preparedness was also indicated as among the factors that make the achievement of cybersecurity challenging to the e-health institutions [14], [54].

Factors under the element of management was also identified to have a correlation with CSC particularly issues relating to lack of cybersecurity team or champions that handle cybersecurity issues, internal communication problem, and the fact that top management provides limited support in relation to cybersecurity issues. Top management support and the existence of cybersecurity team was among the top ten CSC factors [30] that organization need to serious in relation to CSC [22], [29], [34], [55] as it has link with other factors like budget, resource and cybersecurity policy. The responsibility factors identified include lack of collaboration and interaction on cybersecurity issues among employees and between departments of the hospitals. These factors were also highlighted as factors of CSC in the review conducted by [30].

Lastly, environmental factors include the changing landscape of cybersecurity threat that confronts the sector, cybersecurity regulations of the country, as well the fact e-health professionals have many industry regulations and guidelines to adhered to. Emerging new cybersecurity threats was identified as one of the challenges of cybersecurity in e-health sectors [54] and reason why the sector is targeted [56]. Governance and control (legal and regulatory).

By answering the research question asked in this paper, through quantitative research method, the study contributes to the body of knowledge by identifying the CSC factors of the CSC elements that are associated with the public healthcare institutions. In this study, a new theme was formulated to replace environmental factors which are categorized under organization, which is replaced by external factors that are classified under organization as well. This is also a contribution to the field of CSC.

## 8 Limitations and future work

The major limitation with the work is the small sample size. This will be complimented by conducting qualitative research which the researchers are busy with to get the perspective of ICT staffs in the same hospitals on the factors of the elements that are associated with CSC. The information obtained with the qualitative data will be compared with information obtained from participants in this research for more information decision on the factors for the development of CSC contextual framework that the researchers are busy with for the establishment of CSC in the e-health settings.

## 9 Conclusion

This research conducted an empirical study using a quantitative research method to identify factors of CSC elements that are associated with CSC in e-health public hospitals in South Africa. The findings revealed the existence of meaningful correlation and high significance between the elements except for correlation between preparedness and environment, and management and environment. Factors related to awareness, education, and training under preparedness; top management support and establishment of cybersecurity team under management; lack of collaboration for responsibility; and lastly emerging of new threats and regulations under environment were examples of factors that are associated with CSC in the e-health public setting.

## References

1 Horner, A., Rautenbach, P., Mbananga, N., Mashamba, T., Kwinda, H.: An e-Health Decision Support System for Improving Compliance of Health Workers to the Maternity Care Protocols in South Africa. Applied Clinical Informatics, 4(1), 25–36, (2013).

2 Krüger, K., Strand, L., Geitung, J., Eide, G., Grimsmo, A.: Can Electronic Tools Help Improve Nursing Home Quality?. International Scholarly Research Notice, 2011, 1–8, (2011).

3 Mandava, M., Lubamba, C., Ismail, A., Bagula, A., Bagula, H.: Cyber-healthcare for public healthcare in the developing world," In Proceedings of 2016 IEEE Symposium on Computer and Communications, pp. 14–19, (2016).

4 Europaean Commisson.: eHealth Action Plan 2012-2020: Innovative Healthcare for the 21st Century, (2012). [Online]. Available: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0736:FIN:EN:PD

5 An Roinn Slainte department of Health.: eHealth Strategy for Ireland, (2013).

6 Wikler, E., Bausch, P., Cutler, D.: Paper Cuts : Reducing Health Care Administrative Costs, Center for American Progress, Washington, DC, (2012). [Online].Available: https://dash.harvard.edu/bitstream/handle/1/17190515/33796/papercuts_final.pdf?sequence=1

7 B. Yüksel, A. Küpçü, and Ö. Özkasap, "Research issues for privacy and security of electronic health services," Futur. Gener. Comput. Syst., vol. 68, pp. 1–13, 2017, doi: 10.1016/j.future.2016.08.011.

8 ITRC.: 2018 END-OF-YEAR DATA BREACH Report, (2019). Accessed: Jun. 23, 2020. [Online]. Available: https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

9 Ponemon Institute.: 2017 Cost of Data Breach Study Global Overview, (2018), [Online]. Available: https://www.ponemon.org/blog/2017-cost-of-data-breach-study-united-states%0Ahttps://www.ibm.com/security/data-breach.

10 Identity Theft Resource Center (ITRC).: 2019 END-OF-YEAR DATA BREACH REPORT, (2020). [Online]. https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf

11 Statista.: Statistis U.S. data breaches by industry 2019 | Statista, (2020). https://www.statista.com/statistics/273572/number-of-data-breaches-in-the-united-states-by-business/ (accessed Jun. 25, 2020).

12 Murphy, S.: Healthcare Information Security and Privacy, 1st edn. McGraw -Hill Education Group, New York (2015).

13 Ponemon Institute.: Cost of a Data Breach Report 2019, IBM Security, (2019).

14 Ghafur, S., Grass, E., Jennings, N., Darzi, A.: The challenges of cybersecurity in health care: the UK National Health Service as a case study, Lancet Digital Health, 1(1), 10–12 (2019).

15 Roohparvar, R.: 5 Industries that top the hit List of Cyber Criminals in 2017, Infoguard Cyber Security, (2017). http://www.infoguardsecurity.com/5-industries-top-hit-list-cyber-criminals-2017/ (accessed May 10, 2019).

16 Van 't Wout, C.: Develop and maintain a cybersecurity organisational culture. In: 14th International Conference onCyber Warfare and Security (ICCWS 2019), pp. 457–466, (2019).

17 Holdsworth, J., Apeh, E.: An effective immersive cyber security awareness learning platform for businesses in the hospitality sector. In: Proceedings of 2017 IEEE 25th International Requirements Engineering Conference Workshops, REW 2017, pp, 111–117. (2017).

18 Gcaza, N., Von Solms, R., Van Vuuren, J.: An ontology for a national cybersecurity culture environment. In: Proceedings of the Ninth International

Symposium on Human Aspects of Information Security & Assurance (HAISA 2015), pp, 1–10 (2015).

19 Kotz, D., Gunter, C., Kumar, S., Weiner, J.: Privacy and Security in Mobile Health: A Research Agenda. Computer 49(6), 22–30, (2016).

20 Grobler, M., van Vuuren, J.: Broadband broadens scope for cybercrime in Africa. In: Proceedings of 2010 IEEE Information Security for South Africa conference, pp. 1–8. (2010).

21 Marotta, A., Pearlson, K.: A Culture of Cybersecurity at Banca Popolare di Sondrio. 25th Americas Conference on Information Systems (AMCIS 2019), pp, 1–10 (2019).

22 Branley-bell, D., Coventry, L., Sillence, E.: Promoting Cybersecurity Culture Change in Healthcare. In: The 14th PErvasive Technologies Related to Assistive Environments Conference, pp, 544–549 (2021).

23 Corradini, I.: Building a Cybersecurity Culture. In: Building a Cybersecurity Culture in Organizations. Berlin/Heidelberg, Germany: Springer International Publishing, pp, 63–86 (2020).

24 Ismail, W., Yusof, M.: Mitigation Strategies for Unintentional Insider Threats on Information Leaks. International Journal of Security and Application 12(1), 37–46 (2018).

25 Gcaza, N.: A National Strategy towards Cultivating a Cybersecurity Culture in South Africa. PhD thesis, Nelson Mandela Metropolitan University Port Elizabeth, South Africa 1–380 (2017).

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

27 Reid, R., Van Niekerk, J.: From information security to cyber security cultures. In: 2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference, pp, 1–7 (2014).

28 Huang, K., Pearlson, K.: For What Technology Can' t Fix : Building a Model of Organizational Cybersecurity Culture. In: Proceeding of the 52nd Hawaii International Conference on System Sciences, pp, 6398–6407 (2019).

29 Alshaikh, M.: Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security 98 (2020).

30 Mwim, E., Mtsweni, J.: Systematic review of factors that influence the cybersecurity culture Research aims. In: Proceeding of International Symposium on Human Aspects of Information Security and Assurance (HAISA 2022), pp. 147–172. Springer, Heidelberg (2022).

31 Abeyratne, R.: Rulemaking in air transport: A deconstructive analysis. Switzerland: Springer International publishing. 252 (2016).

32 Ciuperca, E.M., Vevera, V., Cirnu, C.: Social Variables of Cyber Security Educational Programmes. In: In The 15th International Scientific Conference eLearning and Software for Education Bucharest, Bucharest, pp, 190–194 (2019).

33 da Veiga, A., Astakhova, V., Botha, A., Herselman, M.: Defining organisational information security culture - Perspectives from academia and industry, Computer Security, 92, 101713, (2020).

34 European Union Agency for Network and Information Security (ENISA): Cyber Security Culture in Organisations. (2017). www.enisa.europa.eu.

35 Da Veiga, A.: Achieving a Security Culture. In: Cybersecurity Education for Awareness and Compliance, 72-100. IGI Global, (2018).

36 Reid, R., Van Niekerk, J.: Towards an Education Campaign for Fostering a Societal, Cyber Security Culture. In: 8th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014), pp, 174–184 (2014).

37 Ponemon Institute.: The Rise of Ransomware. Ponemon Institute LLC, January (2017) Accessed: Jul. 11, 2020. [Online]. Available: https://www.ponemon.org/local/upload/file/Ransomware Report Final 1.pdf.

38 Gcaza N., Von Solms, R., Grobler, M.M., Van Vuuren, J.J.: A general morphological analysis: Delineating a cyber-security culture. Information & Computer Security 25(3), 259–278 (2017).

39 Ogden, S.E.: Cybersecurity: Creating a Cybersecurity Culture. Master thesis. California State University, San Bernardino (2021).

40 Information Systems Audit and Control Association (ISACA).: The Business Impact of a Cybersecurity Culture. ISACA, (2018).

41 Gundu, T., Maronga, M.I, Boucher, D.: Industry 4. 0 Business Perspective: Fostering a Cyber Security Culture in a Culturally Diverse Workplace. In: Proceedings of 4th International Conference on the Internet, Cyber Security and Information Systems. Kalpa Publication in Computing, PP, 85–94 (2019).

42 Georgiadou, A., Mouzakitis, S., Bounas, K., Askounis, D.: A Cyber-Security Culture Framework for Assessing Organization Readiness. Journal of Computer & Information Systems, 1–11(2020).

43 Bounas, K., Georgiadou, A., Kontoulis, M., Mouzakitis, S., Askounis, D.: Towards a cybersecurity culture tool through a holistic, multi-dimensional assessment framework. In: Proceedings of the 13th IADIS International Conference Information Systems 2020 (IS 2020), pp, 135–139 (2020).

44 Jansen Van Vuuren, J.: Methodology and Model to Establish Cybersecurity for National Security in Africa using South Africa as a Case Study. PhD thesis, (2016).

45 Georgiadou, A., Mouzakitis, S., Askounis, D.: Designing a Cyber-security Culture Assessment Survey Targeting Critical Infrastructures During Covid-19 Crisis. International Journal of Network Security & ITs Application 13(1), 33–50 (2021).

46 Alhogail, A., Mirza, A., Bakry, S.H.: A comprehensive human factor framework for information security in organizations. Journal of Theoretical and Applied Information Technology 78(2), 201–211(2015).

47 Schein, E.: Organizational Culture and Leadership, 3rd edition. San Francisco, California: Jossey-Bass, (2004).

48 Van Niekerk, J., von Solms, R.: Information security culture: A management perspective. Computer Security 29(4), 476–486, (2010).

49 DeVillis, F. Scale development: theory and applications, FOURTH. Los Angeles: SAGE, (2017).

50 Streiner, D.: Starting at the Beginning An Introduction to coefficient Alpha and internal consistency. Journal of personality assessment 80(1), 99–103 (2003).

51 Chalil, K.: Statistical Methods for Development Research: Correlation. (2020).

52 Zetter, K.: Why Hospitals Are the Perfect Targets for Ransomware. WIRED, (2016). https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/ (accessed Jul. 02, 2020).

53 Mello, J.: Healthcare Security $65 Billion Market. Cybersecurity Ventures, (2017). https://cybersecurityventures.com/healthcare-cybersecurity-report-2017/ (accessed Oct. 06, 2020).

54 Kruse, C., Frederick, B., Jacobson, T., Monticone, D.: Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care 25(1), 1–10, (2017).

55 Uchendu, B., Nurse, J.R.C., Bada, M., Furnell, S.: Developing a Cyber Security Culture: Current Practices and Future Needs. Computer & Security 109, 102387 (2021).

56 Martin, G., Martin, P., Hankin, C., Darzi, A., Kinross, J.: Cybersecurity and healthcare: How safe are we? BMJ, 358 (2017).