An Empirical Evaluation of the Main Factors of a Cybersecurity Culture in South African E-health Institutions Using Multiple Linear Regression

Nwanneka E. Mwim[1,*], Jabu Mtsweni[2,3], Bester Chimbo[1]

[1]Department of Information System, School of Computing, College of Science Engineering, South Africa

[2]Head of Information and Cyber Security Centre, CSIR, Pretoria, South Africa

[3]SILGA, Stellenbosch University, Stellenbosch, South Africa

Emails: mwimen@unisa.ac.za; jmtsweni@csir.co.za; chimbb@unisa.ac.za

Abstract

E-health institutions are prominent targets for cybercriminals due to their reliance on information technology systems and issues related to the users have been identified as the biggest security weakest. Hence, while cybersecurity culture (CSC) research emphasizes the necessity of the human factor, limited empirical work has been done in the context of e-health in Africa. Therefore, an empirical evaluation was conducted to identify how preparedness, responsibility, management, technology and environment influence cybersecurity in South African e-health institutions. This quantitative research studied e-health institutions in the Mpumalanga province of South Africa. Various methods were used to investigate the multiple linear regression effects of the main factors of CSC and the results show that although the preparedness (Beta = 0.281; p-value < 0.05) and environment (Beta = 0.500; p-value < 0.05) factors had the greatest influence, management, technology and environment had a positive effect on CSC. These factors contributed 48.2 % to the variance (R-Squared). The study seems to be the first empirical study that combines the human factor domain framework (HFD) with other theoretical frameworks to identify critical factors of CSC. Furthermore, the impact of technology on CSC was empirically tested. The study is significant as it identified key factors that contributed to the institution's CSC and quantified their impact. These results can enable e-health institutions to make decisions based on evidence regarding their cybersecurity interventions, strategy and practices. However, the empirical evaluation was limited to one context, namely the Mpumalanga province in South Africa and at two hospitals selected based on easy access (convenience) and purposive sampling with criteria based on work experience and knowledge of CSC limited the number of participants eligible to participate.

Keywords: Cybersecurity culture; E-health; Preparedness; Responsibility; Management; Environment; Technology

1. Introduction

This study was conducted in public e-health institutions in the Mpumalanga province of South Africa. The province was chosen as the research context because of its large rural population, inadequate healthcare facilities, and diverse degree of e-health adoption. Additionally, Mpumalanga received a poor assessment in the Healthcare Security Audit Reports [1] indicating that the province's Department of Health is failing to introduce and be accountable for implementing Cybersecurity Culture (CSC).

E-health is the use of technology in healthcare. It supports the provision of accessible and reliable healthcare by using e-health technologies and the Internet and health records are maintained in secure, digital formats and can easily be accessed and shared by appropriate stakeholders quickly and from almost any location. This increases

DOI: https://doi.org/10.54216/JCIM.170213
Received: April 10, 2025 Revised: June 23, 2025 Accepted: August 22, 2025

the effectiveness and quality of healthcare treatment, research, education and knowledge [2]. Recent research reaffirms the significant contribution of e-health in streamlining healthcare processes, services and products, resulting in improved medical treatment outcomes and more generally a better stakeholder experience [3]. The proper application of e-health systems results in accurate and complete information that can easily be shared and can enable significant transformation and development of healthcare at a national level.

The use of innovative technologies for the delivery of healthcare increases as the recognition the benefits and opportunities it offers to various stakeholders becomes almost universal; these stakeholders include medical professionals, administrators in healthcare organizations, public authorities (government) and patients. However, the increasing reliance on information technology (IT) systems makes the healthcare sector vulnerable to cyber threats which affect the confidentiality, integrity and availability (CIA) of healthcare systems and data [4 -5]. The sector has become one of the prime targets of cyber criminals, with data breaches, ransomware, phishing and denial of service attacks dominating [6]. The growing number of breaches related to healthcare data is a serious problem [7]; almost 90% of healthcare institutions have experienced one or more data breach incidents within the last ten years. Furthermore, healthcare has the second largest number of data breaches after business, and has the highest number of sensitive records exposed [8]. Since e-health institutions are highly vulnerable to ransomware related threats and struggle to keep up with evolving cyber threats, they need to increase their efforts to strengthen cybersecurity [9].

Cybersecurity has become an issue of global concern and an obligation that is shared across all levels of society (country/national, organizational and individual level) to tackle cyber threats [5].

It is defined as *"[t]he approach, and actions associated with security risk management processes followed by organizations and states to protect CIA of data and assets used in cyber space. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its users" [10]*.

Cybersecurity efforts have included the development and publication of national cybersecurity strategies and cybersecurity agendas [11], but these are only part of what is needed to tackle cyber threats [12]. In the past cybersecurity efforts have focused predominately on technological solutions including antivirus software, firewalls and other network solutions but neglected issues related to human behavior [13,14].

More recently authors have argued that human factors are the weakest link in the security chain [5,15]. Accommodating human characteristics in the cybersecurity process requires recognizing the influence of human culture. Hence, creating a strong organizational CSC has been proposed as a critical requirement in addressing the human factor problem [12,16].

In the study presented here it was seen that there was a challenge due to the lack of a suitable and comprehensive framework that would guide the establishment of CSC in the public e-health institutions in South Africa. Various authors have pointed out that the available CSC theoretical framework lacks important components, namely contextual consideration and inclusion of environment [12], and technology [13]. Furthermore, the CSC theoretical framework's dimensions were not categorized. In contrast, the human factor domain (HFD) framework identifies the organizational level which can be seen as management, while the individual level reflects preparedness and responsibility. Additionally, there is a lack of research with an empirically evaluated multiple linear regression and logistic regression model. It is in these two respects that this research planned to contribute.

This research was guided by the following questions:

- What insights does multiple linear regression provide in the empirical evaluation of factors affecting establishment of CSC in e-health in South Africa?
- What are the most dominating factors that influences CSC?

Answering these questions was intended to assist decision makers to understand the critical factors, which need to be prioritized when establishing CSC as an approach to solving the human factor challenge facing cybersecurity. In the next section, the literature is discussed and includes the definitions, frameworks and emerging constructs related to CSC. This is followed by a description of the research method and the results of the empirical study. The discussion, implication and contribution sections include recommendations for public e-health institutions wishing to cultivate a strong CSC. The last section of the paper, the conclusion, acknowledges the research limitations and future work.

DOI: https://doi.org/10.54216/JCIM.170213
Received: April 10, 2025 Revised: June 23, 2025 Accepted: August 22, 2025

2. Motivation

CSC research remains underexplored, with a particularly notable scarcity of empirical studies focusing on CSC in Africa. In South Africa, there is also a noticeable shortage of CSC research in the context of e-health institutions. Addressing this gap is crucial, as incorporating human-centric solutions is important for tackling CSC in South Africa as well as globally. In addition, there is an urgent need to establish guidelines for e-health institutions so that they can enhance the assessment, development and sustainability of CSC. This study is significant in that it crafted a comprehensive framework by addressing issues arising from the insights from prior research on CSC across diverse organizations. The resulting instrument has been methodically devised, assessed and validated, offering a valuable resource for public healthcare organizations to evaluate the CSC prevailing within their entities.

3. Literature Review

a. Concepts leading to cybersecurity culture

As noted above, human factors have been highlighted by established researchers as significantly influencing the way in which individuals and groups interact with technologies in an organization. While human factors pose a challenge to cybersecurity, this has not received sufficient attention as previous studies focused almost entirely on applying a technological solution. Addressing these challenges requires a change in human behaviors and the underlying organizational culture.

It is widely acknowledged that organizational culture has a substantial impact on how well an organization performs. There is a mutual influence between culture and people's behavior as aspects of cultural influence how people behave and patterns of behavior become part of the organizational culture. A strong positive culture plays a major role in security success as it encourages employees to behave in a way that earns respect. **Figure 1** depicts the sequence of concepts leading to the phenomena of CSC. The figure was achieved by reviewing the concept of culture, organizational culture, security culture and information security culture [17–20].

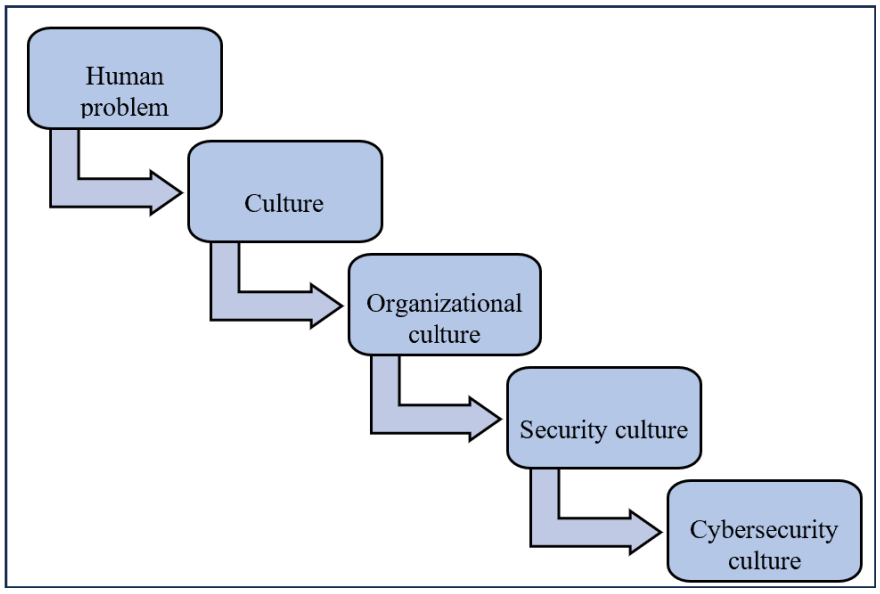

Figure 1. Order of Concepts Leading to the Phenomenon of CSC

The security culture that organizations exhibit plays an important role in achieving a strong positive CSC within the organization. In order to address cybersecurity problems related to human behavior, organizations need to invest in the development of their security culture. The next section discusses CSC.

b. Cybersecurity culture

In this paper, the motivation for investigating aspects of CSC originated from background knowledge of human factors and the recognition that cybersecurity challenges cannot be solved by focusing only on technological solutions. Therefore, this paper measures CSC in the context of e-health based on the recent shift in cybersecurity research from a purely technical approach to a sociocultural approach [21].

DOI: https://doi.org/10.54216/JCIM.170213
Received: April 10, 2025 Revised: June 23, 2025 Accepted: August 22, 2025

Recent studies have emphasized the importance of CSC for solving cybersecurity concerns [17, 21], and have concentrated specifically on concerns that arise from human issues [22]. Individuals and groups [21, 23] see CSC as an all-encompassing and comprehensive strategy that addresses challenges that hinder the acceptance of technological solutions to cybersecurity. Hence, research into CSC bridges the divide between the technical and sociocultural approaches by combining the components of both and adopting a perspective that considers both individual and organizational security culture aspects.

Multiple definitions of CSC exist, and existing definitions of CSC showed no consistency - there was no single globally defined and acceptable definition of the term in literature, as is also the case with cybersecurity definitions. However, many definitions are simply adapted or reworded versions of other authors' definitions [17, 20, 23]. This supports the claims of researcher that CSC is an emerging research area that lacks deeper study including its definition [16].

Definitions that were used to derive the definition above follow. By thoroughly examining the existing definitions of CSC suggested in [12, 19, 21] the following important elements were identified Management, human or human characteristic, context or environment, SETA (Security, Education, Training and Awareness).

CSC "… *can be defined as the intentional and unintentional manner in which cyberspace is utilized from an international, national, organizational or individual perspective in the context of the attitudes, assumptions, beliefs, values, and knowledge of the cyber user to promote or inhibit the safety, security, privacy, and civil liberties of individuals, organizations or governments.*" [12]

CSC "… *refers to the set of values, conventions, practices, knowledge, beliefs, and behaviors associated with information security. Therefore, its skeleton is being outlined by the working environment along with the technological infrastructure and security countermeasures that define it.*" [19]

The CSC *"refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest themselves in people's behavior with information technologies"* [21].

Hence, CSC focuses on the way employees act regarding cybersecurity with an intention to protect the organization's information assets or to achieve the desired level of cybersecurity, and the relationship between this behavior and their underlying knowledge, beliefs, perceptions, attitudes, assumptions, norms and values [21].

After identifying essential elements required this paper defines CSC as "*a measure (technological and non-technological) that is used as a performance tool by management (guided by policies and procedures) to change human characteristics and their sociocultural measures like attitudes, assumptions, beliefs, norms, knowledge, perceptions, skills, behaviors and practices to achieve cybersecurity at all levels of CSC in order to protect against intentional and unintentional cyber-harms using the available technology*."

c. Cybersecurity culture variables

Various theoretical frameworks were reviewed to obtain a holistic view of CSC and these included models that are not specifically related to CSC such as those that are frequently used in research on e-government and e-assessment.

This study ensured that detailed information was obtained about CSC variables by reviewing existing CSC frameworks [18, 19–21, 24]. Since the importance of human factors in CSC had been highlighted, the human factor domain (HFD) framework [24] was included. However, the study also drew from a study that had carried out thorough systematic literature reviews and a study that had mapped the CSC factors to the HFD framework. Context is considered very important in the development of CSC. None of the frameworks [18, 19–21, 24] have been developed for or implemented in public e-health institutions, or in the African context and this highlights the significance of the framework that was developed in this study. Furthermore, the review revealed that technology as a crucial variable (as noted in CSC definitions) failed to be considered by the existing CSC and HFD frameworks [18, 19–21, 24].

Table 1 compares constructs used in the theorical frameworks reviewed. Four key CSC variables were derived based on information gathered from the review of CSC definitions and theoretical frameworks as well as the HFD Framework. These are preparedness, responsibility, management and environment [18, 19–21, 24] . Note that the last column of Table 1 refers to five models, namely CSC Theoretical Framework for Assessing Organizational Readiness (CSC-FAOR), Security Culture model (SCM), Organizational Cybersecurity Culture (OCSC), Human Factor Domain (HFD) and the Strategy, Technology, Organization, People and Environment (STOPE).

DOI: https://doi.org/10.54216/JCIM.170213
Received: April 10, 2025 Revised: June 23, 2025 Accepted: August 22, 2025

It is evident from Table 1 that across the work of different researchers there is a lack of clarity concerning the names of the constructs; what the constructs mean and what they include as elements is not consistent. The lack of standardized definitions has the result that a variety of ways is used to measure constructs. For example, in CSC-FAOR and some other frameworks, the organizational factor has external and internal aspects that are identified and measured [19]. In contrast, in OCSC, an organizational factor (known as the organizational mechanism) was used to refer to the management responsibility in the organization, and various other external factors were treated as separate constructs arising from outside the organization [18]. No single factor or construct was defined or used consistently across the frameworks. There is no clear definition of research terms such as domain, dimension and level; hence, it is difficult to compare frameworks. Furthermore, Table 1 shows that technology has not been identified as a construct in any of the three existing theoretical frameworks that are intended for CSC (CSC-FAOR, SCM and OCSC) [18, 19–21, 24] . However, within the STOPE framework, which is widely used to handle challenges related to the use of digital technology [25], technology was regarded as a significant component [21]. Nevertheless, technology has been emphasized as a crucial element in some definitions of CSC [21].

Table 1: Theoretical Framework Comparison

Models						
	CSC-FAOR	**SCM**	**OCSC**	**HFD**	**STOPE**	**Final Model**
Constructs	Individual level	Individual tier	Beliefs, values and attitudes	Preparedness and responsibility	People	Preparedness and Responsibility *Organizational Culture*
	Organization-al level	External factor	External influences (external factors)	Environment (Internal factors)	Environment	External Environment *Non-Organizational Management*
		Internal Factors	Organization-al mechanisms	Management	Organization-al Strategy	Internal Organizational Management
		Technology			Technology	Technology
	Cyber-security culture	Human behavior	Behaviors	Human behavior		Cybersecurity culture

Note that, although the HFD framework includes the environment as part of an organization's dimension, this is rejected in this research as the environment is regarded as a non-organizational dimension.

The STOPE factors, other than technology, correspond largely with those in the new framework, namely preparedness and responsibility, management, and environment. Hence, preparedness and responsibility are represented as "P" (people) in the STOPE framework, management (as a variable) corresponds with strategy and organization in STOPE, while the environment (as a variable) is also represented environment in the STOPE framework. Technology can be considered as the fifth variable of CSC in this study.

d. The Relationship between Management and CSC

Management (sometimes referred to as "organization") is an influential internal factor of a CSC and reflects the decisions made at the organizational level [18, 22, 26]. Therefore, issues associated with management are the responsibility of the organization's leadership [18, 21, 24]. Organizational matters related to management include

DOI: https://doi.org/10.54216/JCIM.170213
Received: April 10, 2025 Revised: June 23, 2025 Accepted: August 22, 2025

cybersecurity policy, practices, security governance, organizational learning, assets, CSC leadership, and communication [18, 19, 24]. The significance of policy, procedures and guidelines is highlighted in many of the definitions of CSC [18, 22, 23].

This is represented by the first hypothesis: ***H1****: Management has a relationship with a CSC in e-health.*

e. The Relationship between Preparedness, Responsibility and CSC

Several scholars have argued that in addition to other factors, employees' behaviors play a vital role in achieving CSC [18–20]. Preparedness and responsibility relate to employees; employees are any member of the organization that operates in the leadership, group, and individual layers of the organization [18–20]. These two factors, which form the foundations of an organization's culture, have a major impact on employees' behaviors regarding cybersecurity and are related to key underlying human and behavioral concepts including beliefs, values and attitudes. Employees' cybersecurity behaviors include both the official and the personal intentional behaviors of individuals at any of the three levels (organizational, team and individual level of the organization.

Various authors [18–20] have included competency to the individual human level elements, which highlights the knowledge construct that extends the information security model. In the proposed framework, preparedness includes both awareness and competence (AC) [18, 19, 24]. Associated concepts are knowledge, self-efficacy, training and openness to changing from old practice [18, 19, 24]. Responsibility includes the combination of attitudes and behaviors (AB) of employees and can be revealed by the amount of attention given to CSC, perceptions, acceptance, norms and participation in CSC activities. Responsibility also relates to the institutionalization of more tangible processes, such as monitoring and control, compliance, and rewards and punishment [18].

A central issue that emerges in definitions of CSC is the challenges posed by humans and human characteristics. Hence, these definitions highlight human qualities such as attitudes, beliefs, values, knowledge, behavior, practices, reputation, compliance, communication, skills, awareness, training, perceptions, norms and practices [22, 25, 27]. In response to this, preparedness and responsibility are identified as human qualities that must be in the CSC.

This leads to the second and third hypotheses:

H2*: Preparedness has a relationship with a CSC in e-health.*

H3*: Responsibility has a relationship with a CSC in e-health.*

f. The Relationship between Environment and CSC

In this study, environment refers only to the non-organizational or contextual characteristics of a CSC. In other words, the environment is regarded as an external issue that affects development and implementation of the CSC. The environmental factor is comprised of features that are outside the control of the organization and examples include legislation, legal principles and competition from peer institutions as well as cultural element of the society [18, 20, 21].

The environment is the foundation upon which the CSC can be built and used. A CSC environment can be classified as country/national level, organizational and individual level [12].

The fourth hypothesis reflects this: ***H4****: Environment has a relationship with a CSC in e-health.*

g. The Relationship between Technology and CSC

Technology is a crucial component of a CSC [21]. While CSC itself is typically regarded as a non-technical factor that cultivates security awareness and behavior [21], it is vital not to overlook the role of technology in the environment where a CSC is required. Technology facilitates employees' interactions with 21st century organizational assets including information, data, systems, people, highlighting its role in CSC. CSC is only meaningful when technology, people and their behaviors, and information are brought together and CSC influences cybersecurity awareness and business processes [21].

This leads to the final hypothesis: ***H5:*** *Technology has a relationship with a CSC in e-health.*

h. Theoretical framework

The review of existing CSC definitions and frameworks (including STOPE and HFD) allowed five CSC factors to emerge, namely preparedness, responsibility, technology, management and environment (see Subsections a to g above) [18, 20, 21]. Figure 2 depicts the CSC factors and their hypotheses.

DOI: https://doi.org/10.54216/JCIM.170213
Received: April 10, 2025 Revised: June 23, 2025 Accepted: August 22, 2025

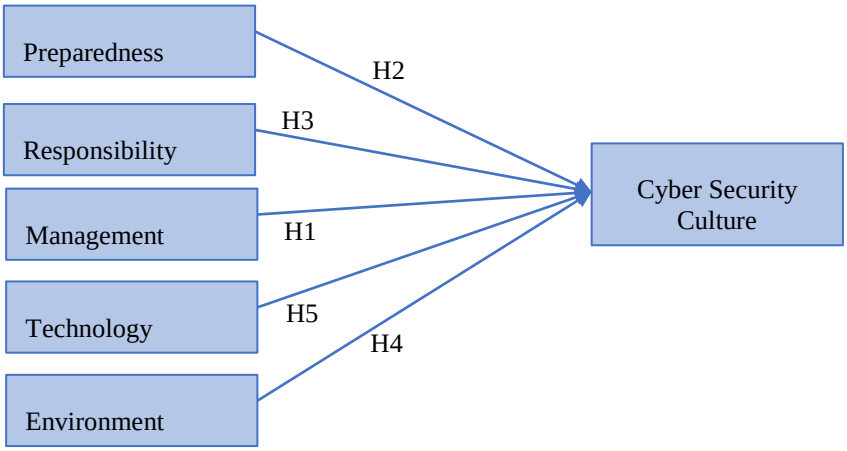

Figure 2. Theoretical framework (Source: Author)

Figure 2 shows the coordination between technical and sociocultural approaches to cybersecurity research, emphasizing significant human factors. The role of the preparedness, responsibility, management and environment, and technology factors in shaping CSC is emphasized. Ultimately, CSC aims to change human characteristics and behaviors to enhance cybersecurity at all levels (individual, team, organization and national).

Table 2 consolidate Table 1 and Figure 2 and shows how the research constructs are mapped to the hypotheses.

Table 2: Synthesized Table Mapping Constructs to Hypotheses

Construct	**Theoretical Basis**	**Description**	**Hypothesis**
Management	Model 1 (CSC-FAOR) - Model 5 (STOPE)	Refers to an internal CSC element. Management relates to actions and steps at the organisation that impact on CSC. It includes operation, policy, and procedure of organization cybersecurity.	**H1**: Management has a relationship with a CSC in e-health.
Preparedness and Responsibility	Model 1 (CSC-FAOR) - Model 5 (STOPE)	Relates to individual factors that deal with employee's traits and characteristics, which affect directly on their security behaviours. Ppreparedness and responsibility are internal CSC elements. Preparedness include employee's awareness and competency, and education on cybersecurity issues. Responsibility include human attitude and behavioral factors, like, the practices and personalities of employees of the organization in terms of cybersecurity.	**H2**: Preparedness has a relationship with a CSC in e-health. **H3**: Responsibility has a relationship with a CSC in e-health
Environment	Model 2 (SCM) - Model 5 (STOPE)	Refers to non-organisational characteristics that influenced CSC. In other words, the environment is regarded as external factors that affects development and implementation of the CSC. Example includes development of new technology and the appropriate law as well as competition from peer institutions and the cultural element of the society.	**H4**: Environment has a relationship with a CSC in e-health.

DOI: https://doi.org/10.54216/JCIM.170213
Received: April 10, 2025 Revised: June 23, 2025 Accepted: August 22, 2025

Technology	Model 2 (SCM) & Model 5 (STOPE)	Deals with relevant Internet and information technology issues related particularly to the use of technology. It is an intermediate theme because it is situated between internal and external themes. Examples are the increasing number of cyber-related threats, new and fast emerging technologies.	**H5**: Technology has a relationship with a CSC in e-health.

4. Methods

a. Study design

This study employed a survey, utilizing questionnaires as the primary data collection tool for both medical practitioners and administrative staff. The research approach was quantitative and encompassed various analytical methods including a frequency analysis, descriptive statistics, validity assessments, exploratory factor analysis, Cronbach's Alpha calculations, correlation analyses and regression analyses.

The six-section survey contained questions based on the five main factors of a CSC. Data collected covered participants' demographics and aspects evaluating preparedness, responsibility, technology, environment, and management factors using an agreement legend. The questions asked were related to the five CSC factors. Participant bias was lessened by framing some of the questions as either positive or negative but for analysis negative answers were converted to positive ones. No issues of skewness and kurtosis were observed, which indicated that the research data was distributed. Twelve participants were involved in a pilot run before the data collection took place to test the research instrument in a hospital setting similar to those that would eventually be used. Feedback from that study was used to improve the data collection instrument. Thereafter questionnaires were administered to 120 medical professionals and administrative staff members all of whom made use of internet-based IT systems to access important confidential information in two public hospitals. Convenience sampling was used to select the South African province where the study was conducted and judgment sampling was used to select the target population. Ninety-nine questionnaires were returned, giving a response rate of 82.5%. The relatively small sample size was because only a limited number of the targeted population met the stated criteria to be included.

b. Study site and participants

The study was conducted at two public hospitals facilities in the Mpumalanga province of South Africa. The province was selected given ease of contact with management and this facilitated study approval. The study population were medical professionals and administrative staff working at these sites.

c. Sample size

The sample size was calculated through statistical power analysis using G*power. With a statistical power of 0.95, an Alpha level of 0.05, and an effective size (F2) of 0.15, the sample size surpassed the required minimum threshold of 90 participants for this study. The selection of the Mpumalanga province for the study utilized convenience sampling, chosen for its ease of contact with authorities, which in turn resulted in a straightforward approval process by management. This sampling method is fast and has other practical benefits. On the other hand, the potential selection bias associated with this the method makes the research findings non-generalizable. The study was therefore conducted to acquire basic knowledge and recognizing that a more representative study should follow in other provinces.

Drawing a representative sample and testing hypotheses to ensure generalizability of the finding is one benefit of quantitative research approach. On the contrary small sample size affects generalizability of research finding as it can limit representation of target population. Notwithstanding the sample size is surpassed the minimum threshold according to the statistical power analysis G*power (making it acceptable for use in this study), it can still be argued as relatively small. The large number of, and size of South African provinces, made it challenging to include other provinces. Data was only collected from Mpumalanga province, where it was convenient for the researcher to access hospitals. This made the research sample size relatively small.

Mpumalanga Health Department is one of South Africa's Health Departments and contains similar hospital categories. However data from Mpumalanga alone may not accurately represent all provinces' health departments across broader of South Africa. There may be factors considered essential in other hospital that may not form part

DOI: https://doi.org/10.54216/JCIM.170213
Received: April 10, 2025 Revised: June 23, 2025 Accepted: August 22, 2025

of critical factors in another hospital context. Therefore, it can be difficult to generalize the findings of this research to larger South Africa healthcare sectors because of impacts emanating from healthcare individual differences

Once the province had been selected purposive sampling was employed, taking into account potential participants' skill levels. Instead of striving for representativeness, this study targeted individuals who could provide useful input as they had the necessary work experience, roles, and other qualities that were considered to be central to the topic of CSC and the context of e-health. The categorization of participants into medical professionals and administrative staff was deliberate and aimed to ensure a reasonably representative sample reflecting the context of the hospital and of South Africa. Nevertheless, the aim was to focus primarily on the expertise and particular knowledge of the participants.

d. Data analysis

The Statistical Package for Social Sciences (SPSS) version 28.0 was used for data analysis. Participant demographics were analyzed and depicted using frequency tables. The internal consistency of the component questions was assessed using Cronbach's Alpha, and a valid threshold value of 0.60 was considered. The mean and standard deviation of the components measured; together their individual items were summarized using descriptive statistics. The relationships between the components was measured using the Pearson correlation. exploratory factor analysis comprising the Kaiser-Meyer-Olkin (KMO) measure, communality, Total Variance Explained (TVE), and the Rotated Component Matrix (RCM) were used to test the validity of the research instrument. As explained in Section 3, five factors had been identified as part of the research design and were used in the exploratory factor analysis using eigenvalues. Multiple linear regression was used to evaluate the causality of those five independent variables (management, responsibility, technology, environment, and preparedness) toward the dependent variable cybersecurity.

Multiple linear regression was selected as the primary analytical technique due to its suitability for examining the relationship between multiple independent variables (such as awareness, training, policy, technology) and a single continuous dependent variable cybersecurity culture (CSC). Multiple linear regression is particularly appropriate for identifying the strength and significance of individual predictors while controlling for the influence of others, making it ideal for understanding the relative impact of various human and organizational factors on CSC. This method also allows for the testing of linear assumptions, multicollinearity diagnostics, and model fit indicators, which support robust inferential conclusions. Alternative models, such as logistic regression or structural equation modeling (SEM), were considered; however, the nature of the outcome variable and sample size (n=99) made Multiple linear regression a more practical and interpretable choice for this exploratory study.

The chosen measures for this study were deemed valid in the South African context through the application of exploratory factor analysis, which systematically eliminated questionnaire items (questions) inconsistent with the South African environment. Only those questions that demonstrated both validity and reliability were retained for further analysis. Moreover, the validation of constructs in this study was further confirmed through previous findings of. The measures themselves had previously been developed employing a systematic literature review.

R Square values range from 0 to 1 and indicates the extent of the model's contribution to the dependent variable. A value of 0.1 or greater is indicative of a meaningful contribution. This study utilized regression coefficients to quantify the amount of change in the dependent variable related to a one-unit alteration in the independent variable. Correlation (r) measures the association between two variables, with values ranging from -1 to 1. As the absolute value of r approaches 1, the correlation between the variables is understood to become stronger. The research instrument employed a Likert Scale with five points, where 1 signifies "strongly disagree" and 5 corresponds to "strongly agree."

5. Results

a. Demographical information

This data presented the demographic information of the 99 respondents (Table 3), focusing on age, gender, education level and job title. The age distribution showed that the largest group of respondents were between 21 to 30 years (32.3 %), followed by the 31 to 40 years (29.3 %), 41 to 50 years (20.2 %), 51 to 60 years (15.2 %) and 60+ years (3.0 %) categories. There were more females (56.6 %) than males (43.4 %), and most of the respondents hold a bachelor's degree (57.6 %), followed by doctoral degree holders (19.2 %), master's degree (MSc) holders (9.1 %), those with secondary education (8.1%) and those with vocational professional nursing training (6.1 %). Job titles were varied, with doctors representing the largest group (36.4 %), followed by administrative personnel (20.2 %), nurses (17.2 %), pharmacists (8.1 %), and others (18.2 %).

DOI: https://doi.org/10.54216/JCIM.170213
Received: April 10, 2025 Revised: June 23, 2025 Accepted: August 22, 2025

Table 3: Demographic Information

Variable	Category	Frequency	Percentage (%)
Age	21- 30	32	32.3
	31- 40	29	29.3
	41- 50	20	20.2
	51- 60	15	15.2
	60+	3	3.0
	Total	99	100.0
Gender	Male	43	43.4
	Female	56	56.6
	Total	99	100.0
Education	Secondary	8	8.1
	Vocational	6	6.1
	Degree	57	57.6
	MSc	9	9.1
	PhD	19	19.2
	Total	99	100.0
Job Title	Doctor	36	36.4
	Nurse	17	17.2
	Pharmacist	8	8.1
	Admin	20	20.2
	Other	18	18.2
	Total	99	100.0

In summary, the data indicated a diverse sample with a significant number of young adults, a slight female majority, predominantly bachelor's degree-educated individuals, and a range of job titles, with medical doctors being the most notable. This information is valuable for other demographic analyses and decision-making processes in fields such as healthcare and education.

b. Reliability

The Cronbach's Alpha values for the five dependent variables are presented in Table 4 and indicate internal consistency reliability. This means the research instrument did not have any problems related to the reliability of the questionnaire items used in this study. Awareness and competency (A&C) scored a high 0.900, suggesting

DOI: https://doi.org/10.54216/JCIM.170213
Received: April 10, 2025 Revised: June 23, 2025 Accepted: August 22, 2025

strong reliability. Responsibility (A&B) had a lower score of 0.627 and management of cybersecurity practices (MCP, also represented as M) achieved 0.816. Environment (E) scored 0.731 and Technology (T) had the lowest Cronbach's Alpha score of 0.607. CSC demonstrated strong reliability with a Cronbach's Alpha of 0.896.

Table 4: Cronbach's Alpha

Variables	**Cronbach's Alpha**
Preparedness (A&C)	0.900
Responsibility (A&B)	0.627
Management (M)	0.816
Environment (E)	0.731
Technology (TECH)	0.607
CSC	0.896

The constructs supported in this thesis were consistent with the constructs identified in the literature review.

c. Validity

The KMO measure of sampling adequacy was 0.761, indicating data suitability for factor analysis. Bartlett's test of sphericity yielded an approximate chi-square of 3301.716 with 1378 degrees of freedom and a p-value of 0.000, affirming that the variables are correlated and supporting factor analysis (see Table 5).

Table 5: Kaiser-Meyer-Olkin and Bartlett's Test

Measure		**Value**
Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy.		0.761
Bartlett's Test of Sphericity	Approx. Chi-Square	3301.716
	df	1378
	Sig.	0.000

d. Communalities

Table 6 shows the communalities, indicating the proportion of variance in groups of questionnaire items related to the five factors accounted for a Principal Component Analysis (PCA). For the preparedness, responsibility, technology, environment and management variables, communalities ranged from 0.651 to 0.846, indicating that these factors explained between 65.2% and 84.6% of the variance in the questionnaire items.

Table 6: Principal Component Analysis: Communalities and Extraction Ranges

Questions	**Initial**	**Extraction (Range)**
Q5_1 – Q5_15 Preparedness (A&C)	1.000	0.652 - 0.846
Q6_1– Q6_19 Responsibility (A&B)	1.000	0.651 - 0.802
Q7_1 – Q7_2 Technology (TECH)	1.000	0.664 - 0.759
Q8_1 – Q8_8 Environment (E)	1.000	0.664 - 0.759
Q9_1 – Q9_16 Management (M)	1.000	0.667 - 0.834

DOI: https://doi.org/10.54216/JCIM.170213
Received: April 10, 2025 Revised: June 23, 2025 Accepted: August 22, 2025

Factor Analysis Results are given in Table 7. The analysis aimed to reduce the data's dimensionality and identify underlying patterns. Five principal components were extracted, explaining a total variance of 75.642% (see Table 7). The eigenvalue for Component 1 (Preparedness) was 23.942 suggesting that it accounts for a large portion of the variance, which is 47.174%. Component 1 primarily loaded onto questions related to preparedness. Component 2 (Responsibility) primarily loaded onto questions related to responsibility. Components 1 and 2 together accounted for 64.221% of the total variance, demonstrating that these factors are the most important dimensions of the data. In summary, the PCA identified two dominant components related to preparedness and responsibility, explaining nearly half of the total variance. Additional components seem to represent additional dimensions within the data, probably technology, environmental concerns and management; however, further exploration is needed to fully understand their significance.

Table 7: Factor Analysis Results

Factors	**Questions**	**Rotated Component Metrix**	**Component Matrix**	**Total Variance Explained**	**Eigenvalue**
Preparedness (A&C)	Que 5_1	0.538	1	47.174%	23.942
	Que 5_2	0.646			
	Que 5_3	0.679			
	Que 5_4	0.431			
	Que 5_5	0.745			
	Que 5_6	0.593			
	Que 5_7	0.717			
	Que 5_8	0.519			
	Que 5_9	0.447			
	Que 5_10	0.479			
	Que 5_11	0.610			
	Que 5_12	0.702			
	Que 5_13	0.485			
	Que 5_14	0.672			
	Que 5_15	0.701			
Responsibility (A&B)	Que 6_1	0.556	2	17.047%	9.035
	Que 6_2	0.402			
	Que 6_3	0.519			
	Que 6_4	0.646			

DOI: https://doi.org/10.54216/JCIM.170213
Received: April 10, 2025 Revised: June 23, 2025 Accepted: August 22, 2025

Factors	Questions	Rotated Component Metrix	Component Matrix	Total Variance Explained	Eigenvalue
	Que 6_5	0.517			
	Que 6_6	0.486			
	Que 6_7	0.614			
	Que 6_8	0.604			
	Que 6_10	0.660			
	Que 6_12	0.602			
	Que 6_13	0.542			
	Que 6_14	0.720			
	Que 6_15	0.669			
	Que 6_16	0.424			
	Que 6_17	0.397			
	Que 6_19	0.406			
Technology (TECH)	Que 7_1	0.633	3	2.116%	1.122%
	Que 7_2	0.475			
Environment (E)	Que 8_1	0.614	4	1.955%	1.036
	Que 8_2	0.444			
	Que 8_3	0.443			
	Que 8_4	0.488			
Management (M)	Que 9_1	0.616	5	7.350%	3.895
	Que 9_2	0.701			
	Que 9_3	0.571			
	Que 9_4	0.410			
	Que 9_5	0.591			
	Que 9_6	0.368			
	Que 9_7	0.738			

DOI: https://doi.org/10.54216/JCIM.170213
Received: April 10, 2025 Revised: June 23, 2025 Accepted: August 22, 2025

Factors	Questions	Rotated Component Metrix	Component Matrix	Total Variance Explained	Eigenvalue
	Que 9_8	0.667			
	Que 9_9	0.563			
	Que 9_10	0.487			
	Que 9_11	0.629			
	Que 9_12	0.731			
	Que 9_13	0.473			
	Que 9_14	0.660			
	Que 9_15	0.651			
	Que 9_16	0.441			

e. Descriptive analysis

In the dataset with 99 observations for 6 constructs, key statistics revealed insights into each construct's characteristics (see Table 8). Awareness and competency (the characteristics of preparedness) ranged from 1.00 to 4.13, with a mean of 2.4963 and a standard deviation of 0.78282. Attitude and behaviors (the characteristics of responsibility) ranged from 1.56 to 4.06, with a mean of 2.7898 and a standard deviation of 0.44351. Cybersecurity Practices (related to Management) ranged from 1.50 to 3.81, with a mean of 2.5739 and a standard deviation of 0.56845. Environment (E) spanned from 1.00 to 5.00, with a mean of 2.7374 and a standard deviation of 0.75628. Technology ranged from 1.00 to 5.00, with a mean of 2.6667 and a standard deviation of 0.93405. Lastly, CSC ranged from 1.50 to 3.56, with a mean of 2.6221 and a standard deviation of 0.45953. These statistics provide a clear overview of how data are distributed and focus for each construct. The Technology construct's frequent importance in the models presented earlier served as the basis for its inclusion. Two essential variables that represent access to and familiarity with cybersecurity-related technology in healthcare settings were used to measure the construct, albeit, due to the exploratory nature of the study and contextual limitations.

Table 8: Descriptive Statistics for Constructs

Constructs	N	Minimum	Maximum	Mean	Std. Deviation
Preparedness (A&C)	99	1.00	4.13	2.4963	0.78282
Responsibility (A&B)	99	1.56	4.06	2.7898	0.44351
Management (M)	99	1.50	3.81	2.5739	0.56845
Environment (E)	99	1.00	5.00	2.7374	0.75628
Technology (TECH)	99	1.00	5.00	2.6667	0.93405
CSC	99	1.50	3.56	2.6221	0.45953

DOI: https://doi.org/10.54216/JCIM.170213
Received: April 10, 2025 Revised: June 23, 2025 Accepted: August 22, 2025

f. Correlation

Table 9 presents a correlation matrix with Pearson correlation coefficients for six variables: A&C, A&B, M, E, Tech, and CSC. The matrix contains correlations, significance levels, and sample sizes (N) for each pairwise combination of variables. Notably, A&C is significantly correlated with A&B ($r = 0.563$, $p < 0.01$), and both variables show significant correlations with M (A&C: $r = 0.570$, A&B: $r = 0.574$, $p < 0.01$). E shows weak correlations with other variables, while Tech and CSC exhibit strong correlations. CSC, in particular, is highly correlated with A&C ($r = 0.850$, $p < 0.01$), A&B ($r = 0.815$, $p < 0.01$), and M ($r = 0.817$, $p < 0.01$); and moderately correlated with Tech ($r = 0.253$, $p < 0.01$). These findings suggest relationships and dependencies among the variables, with CSC showing particularly strong associations with other factors in the study.

Table 9: Correlation of the Constructs

		A&C	**A&B**	**M**	**E**	**TECH**	**CSC**
A&C	Pearson Correlation	1					
	Sig. (2-tailed)						
	N	99					
A&B	Pearson Correlation	.563**	1				
	Sig. (2-tailed)	.000					
	N	99	99				
M	Pearson Correlation	.570**	.574**	1			
	Sig. (2-tailed)	.000	.000				
	N	99	99	99			
E	Pearson Correlation	.009	.150	.012	1		
	Sig. (2-tailed)	.332	.019	.339			
	N	99	99	99	99		
TECH	Pearson Correlation	.039	.208*	.034	.742**	1	
	Sig. (2-tailed)	.698	.016	.505	.000		
	N	99	99	99	99	99	
CSC	Pearson Correlation	.850**	.815**	.817**	.242**	.253*	1
	Sig. (2-tailed)	.000	.000	.000	.004	.046	
	N	99	99	99	99	99	99

DOI: https://doi.org/10.54216/JCIM.170213
Received: April 10, 2025 Revised: June 23, 2025 Accepted: August 22, 2025

g. CSC as dependent variable and environment, management, technology, responsibility, and preparedness as predictors

The regression model exhibits a moderate fit (R = 0.695) with an R-squared of 0.482 (see Table 10). This means that the variance explained in this study for all factors influencing CSC was 48.2% which is a good research contribution. The model's F-statistic is 26.100, signifying a significant overall fit ($p < 0.01$). The Durbin-Watson statistic is 2.116, suggesting no significant autocorrelation. The predictors are environment, management, responsibility, technology, and preparedness. The data in this research has 95% confidence interval. This means there is 95% chance of predicting the results of multiple regression in this study.

Table 10: Model Summary

Model	R	R Square	Change Statistics					Durbin-Watson
			R Square Change	F Change	df1	df2	Sig. F Change	
1	.695[a]	.482	.482	26.100	3	84	.000	2.116
a. Predictors: (Constant), Environment, Management, Technology, Responsibility, Preparedness								
b. Dependent Variable: Cybersecurity culture								

The analysis of variance (ANOVA) for the model reveals significant results ($F = 26.100$, $p < 0.01$) (see Table 11). The regression model (with predictor's environment, management, responsibility, technology and preparedness) accounts for a substantial portion of the variance in the dependent variable CSC. The regression component has a sum of squares of 24.545 with 3 degrees of freedom, while the residual component has a sum of squares of 26.332 with 84 degrees of freedom. Overall, the model explains a significant portion of the variability in CSC.

Table 11: ANOVA

ANOVA						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	24.545	3	8.182	26.100	.000b
	Residual	26.332	84	.313		
	Total	50.877	87			

The regression model examined the relationship between five predictor variables (preparedness, environment, management, technology and responsibility) and the dependent variable, CSC (see Table 12). The standardized coefficients indicate the strength and direction of these relationships. Environment had the highest impact with a beta of 0.500, followed by preparedness (0.482), responsibility (0.359), technology (0.321), and management (0.281). All of the predictor variables were statistically significant ($p < 0.001$), suggesting they contribute to CSC. Collinearity statistics show no severe multicollinearity issues. In summary, the study found that preparedness and environment had the most significant influence on CSC.

DOI: https://doi.org/10.54216/JCIM.170213
Received: April 10, 2025 Revised: June 23, 2025 Accepted: August 22, 2025

Table 12: Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.222	.383		.2456	.001
	Preparedness	.467	.148	.482	4.634	.000
	Environment	.695	.150	.500	4.634	.000
	Management	.340	.123	.281	2.766	.000
	Responsibility	.366	.096	.359	2.695	.000
	Technology	.331	.091	.321		.000

In summary, the results given in Section 5 provide an overview of the demographic information, reliability, validity, descriptive statistics, correlations, and regression analysis for the dataset of 99 individuals. The sample was diverse, with a significant proportion of young adults, predominantly female, holding bachelor's degrees and working in various job titles. Reliability analysis showed strong internal consistency for most constructs. Factor analysis revealed two dominant components related to preparedness and responsibility. Correlation analysis indicated significant relationships between variables, with CSC strongly associated with other factors. The regression model demonstrated that preparedness and environment have the most significant influence on CSC.

6. Discussion of the results

Regarding the first hypothesis: ***H1****: Management has a relationship with a CSC in e-health.*

The results suggest that the management factors have a positive effect on CSC factors for e-health, which was significant. This result means that practices related to management contributed significantly to the establishment of a strong positive cybersecurity culture in the context of e-health. The Beta value of 0.281 (see Table 12) showed moderate positive association which implies that more positive actions by management of the institutions in terms of cybersecurity practices (such as having a cybersecurity policy, leadership involvement, guidelines, a well-known cybersecurity department or team) will have a strong influence on CSC. The p−value for this factor was less than 0.05 and this means that H1 was supported and that the management factor has a relationship with CSC. This finding concurs with the findings of several other researchers [46, 56, 58, 65, 66] and is in line with the findings related to the South African e-health context discussed in this paper.

However, management had the lowest beta value contributing to CSC. Points that came out strongly from the responses regarding the management of e-health were that there was little or no support available from sources that that existed in the health institutions studied such as a cybersecurity department, team or section to handle cyber-related issues. In addition, limited support and participation was reported as coming from top management regarding cyber issues. What was also concerning was that participants lack knowledge of their hospital's cybersecurity policies and guidelines. This finding contrasts with that from studies conducted elsewhere (for example, at Liberty Mutual) where the institution has invested resources to create CSC and created leadership position for CSC [18]. This type of proactive management encourages other management activities like the creation of incentives (rewards and punishments), performance evaluations, appropriate cybersecurity training, and multiple communications channels. Therefore, for a better CSC in e-health there is need for strong management engagement.

Regarding the second hypothesis: ***H2****: Preparedness has a relationship with a CSC in e-health.*

Preparedness factors have a positive effect on CSC factors for e-health that was significant (see Table 12). The Beta value (0.482) indicates a moderate to strong relationship between preparedness factors as independent variable and CSC as dependent variable. Preparedness was the second-highest beta value contributing to CSC in this study. This implied that as preparedness increased CSC also increased. From the information given by the

DOI: https://doi.org/10.54216/JCIM.170213
Received: April 10, 2025 Revised: June 23, 2025 Accepted: August 22, 2025

medical and administrative staff in Mpumalanga, the hospitals were not well prepared for CSC. The finding showed that if the hospitals became more prepared in terms of cybersecurity awareness, education, and training, there would be a better CSC in those institutions. The results concur with the findings of several researchers [18, 19, 24]. The H2, which indicated that preparedness has a relationship with CSC, was validated by the p−value which was less than 0.05. However, based on the finding, it appears that the Mpumalanga public health institutions were not prepared to handle cybersecurity because little attention was given to cybersecurity issues. Therefore, number of actions should be increased or be brought more strongly to the attention of end users for these hospitals to be considered organizations that take cybersecurity seriously. Factors related to preparedness, including staff members' knowledge, awareness and training, and proper communication of the security policy were also found to be inadequate in the security culture assessment conducted [20]. The absence of preparedness factors can make it hard to develop and maintain CSC [21].

Regarding the third hypothesis: ***H3****: Responsibility has a relationship with a CSC in e-health.*

Responsibility factors have a positive significant effect on CSC factors for e-health. The Beta value (0.359) shows that the responsibility factor has moderate impact on affecting the changes in CSC (see Table 12). This indicate that when independent variable (that is, responsibility) increased, the dependent variable (CSC) also does. The finding suggests that the CSC of the hospitals where this study took place would improve if there were behavior that is more responsible and better attitudes towards cybersecurity by employees. The results were in line with the findings of the researchers referred to in the literature review [18, 20, 24]. Responsibility factors like attitude towards sharing of security passwords and personal belief regarding training and communication of security policy need to be improved in order to achieve security culture. Hypothesis H3 was validated with a p−value less than 0.05. Responsibility was the third-highest beta value contributing to CSC according to the finding in this research.

The results from hypothesis H5 follow. ***H5:*** *Technology has a relationship with a CSC in e-health.*

It was found that technology factors have a positive effect on CSC factors for e-health and this relationship was significant (Beta = 0.321; p − value < 0.05) (see Table 12). This suggests that an improvement regarding technological factors is likely to lead to a positive CSC. This result supports the findings of several researchers [26]. Technology was the fourth highest beta value contributing to CSC.

The hypothesis H4 states: ***H4****: Environment has a relationship with a CSC in e-health.*

Environment factors also have a positive effect on CSC factors for e-health and this relationship was found to be significant (Beta = 0.500; p − value < 0.05) (see Table 12). This result suggests that an increase in environmental factors can lead to a positive security culture. This conclusion has previously been supported by several researchers working in different contexts and types of organization [18, 20, 21, 24] and is also in line with the findings of the South African e-health context. It is important to note that in the findings reported here the environment was found to be the most dominant factor affecting CSC; it was the highest beta value contributing to CSC.

In summary, CSC in this study contributed 48.2% as an R Squared value for the factors management, technology, preparedness, responsibility, and environment.

7. Contribution

a. Theoretical contribution

The objectives of this study were (1) to gain insights into the factors influencing CSC in e-health institutions in South Africa, (2) to understand the dominating factors that influence the CSC. This study achieved this by performing multiple linear regression evaluation. The outcome of the evaluation addressed the first objective by showing that the five independent variables, namely preparedness, responsibility, management, technology and environment, collectively accounted for a noteworthy 48.2% contribution to CSC. For the second objective, the finding indicated that environment is the dominating factor influencing CSC. This was followed by preparedness and responsibility. Technology and management were the least influential factors according to this research. This underscores the relevance of these contributions within the context of South Africa's health sector, which is in a particular national and organizational environment. It is noteworthy that, based on the literature review conducted on CSC, no prior study has empirically assessed similar independent variables using a multiple regression approach.

Previous studies have predominantly employed thematic analysis of constructs or themes [46, 47, 64]. One paper was found which referred to empirical analysis, focusing on correlation, descriptive analysis, and thematic analysis, but did not extend to testing the causality between dependent and independent variables. The multiple

DOI: https://doi.org/10.54216/JCIM.170213
Received: April 10, 2025 Revised: June 23, 2025 Accepted: August 22, 2025

linear regression evaluation of this study also addressed research gaps by identifying factors that can be considered for the contextual framework development for CSC in a public e-health institution.

b. Practical implications

The findings in this study provide practical guidance for top decision makers regarding the core factors for cultivating and improving CSC, and how these can be strengthened by those concerned with ICT, security and cybersecurity in the public health sector in South Africa. The findings indicate that health institutions should pay attention to management, environment, preparedness and responsibility factors. These include considerations regarding size and location of the institution, training, education, awareness of cybersecurity threats, beliefs and norms, policy, and regulations when cultivating or improving CSC. Hence, the institutions should devise holistic action sets like the ones outlined below to ensure a culture of cybersecurity.

Establish a cybersecurity policy.

The policy should be expanded to explain how the various sections of the policy affect members of staff and how they can increase their cybersecurity knowledge.

Plan to update of the policy regularly to accommodate the rapid change in IT and cyber threats.

Make cybersecurity guidelines easily available.

Establish a feasible and effective way (in terms of when, where, how and how often) to provide current and relevant cybersecurity training and education to members of staff.

Create diverse communication channels (emails, posters and notices) for circulating cybersecurity information including policy.

Create constant awareness of cybersecurity threats among employee to help them build and retain knowledge.

8. Conclusion

In this study, an empirical evaluation of the factors that affect CSC was performed in Mpumalanga province in South Africa to gain a basic understanding of critical factors. The results showed management, technology, environment, responsibility and preparedness contributed 48.2% as variance explained. The dominating factor was the environment, followed by preparedness, responsibility, technology and management. Therefore, this study concludes that attention must particularly be paid to environmental factors, as this is a vital factor in the South African public health context.

The analysis undertaken supports the evidence-based interventions and strategies proposed to strengthen CSC, thereby ensuring the protection of sensitive health information and the compliance with security standards. The findings of this study illustrate the significance of management, technology, environment, responsibility and preparedness as factors in the establishment of CSC in South African healthcare institutions to ensure maximum protection of health data. The findings provide healthcare institutions' top management with a comprehensive overview of CSC and indicate which changes are required that affect employees. This enables data-driven decision making to improve targeted interventions and strengthen cybersecurity practices in healthcare institutions.

To strengthen cybersecurity culture and resilience within public e-health institutions, the following recommendations should be implemented:

Establish and Expand Cybersecurity Policy

Develop a comprehensive cybersecurity policy that clearly defines its sections and relevance to staff roles. Include practical examples and guidance to help employees understand how they can contribute to cybersecurity and enhance their knowledge.

Implement a Policy Update Framework

Create a structured plan for regularly reviewing and updating the cybersecurity policy to reflect evolving IT landscapes and emerging cyber threats. This should include timelines, responsible parties, and mechanisms for stakeholder input.

Ensure Accessibility of Cybersecurity Guidelines

Make cybersecurity guidelines easily accessible to all staff through centralized digital platforms and printed materials. These should be written in plain language and tailored to different departments.

DOI: https://doi.org/10.54216/JCIM.170213
Received: April 10, 2025 Revised: June 23, 2025 Accepted: August 22, 2025

Establish a Dedicated Cybersecurity Function

Create a cybersecurity department, team or make external services easily contactable that champion cybersecurity related issues like initiatives, responding to incidents, and ensuring compliance with regulations. The national or provincial cybersecurity security team needs to work regularly with health institutions to understand the specific laws and regulations that influence cybersecurity in health and to develop ways to address these specific requirements to ensure a culture of cybersecurity.

Standardize Cybersecurity Training and Education

Define the optimal frequency, format, and delivery methods for cybersecurity training. Use a mix of in-person workshops, e-learning modules, and scenario-based exercises to ensure relevance and engagement.

Diversify Communication Channels

Use multiple communication methods—emails, posters, intranet notices, and staff meetings—to disseminate cybersecurity updates, policy changes, and threat alerts. Ensure messages are consistent and easy to understand.

Promote Continuous Cybersecurity Awareness

Institute ongoing cybersecurity awareness campaigns and capacity-building workshops across staff members Use real-world examples, gamified learning, and regular quizzes to reinforce knowledge and encourage proactive behavior.

Regular cybersecurity awareness campaigns and for all staff levels, not just IT personnel

Compare Cybersecurity practices

Public e-health institutions must constantly compare their cybersecurity practices with those of their private counterparts to ensure that they maintain a good reputation.

9. Limitation

The limitations of this study are:

1. This study was conducted in only one province and a small purposive sampling due to the criteria for participation that were considered necessary.

2. The use of convenience sampling used to select the province where the research was conducted can negatively affect the accurate representation of the broader research population, which can also affect the generalization of research findings to other groups beyond the studied group.

The research context was public e-health institutions. Therefore, the interpretation of the findings should be in the context of the public e-health institution.

Based on the knowledge gained from this research, the researchers propose that future research continue the current empirical evaluation but involve more health institutions in other provinces. Future research may also focus on CSC in private e-health institutions to examine the relationships between the two forms of health institutions. This can help provide a more comprehensive view of South African health institutions regarding factors that affect the establishment of CSC. Future research can also explore different sectors within the healthcare industry, using different methodological approaches or as a way to examine the impact of specific interventions to improve CSC.

Funding: “This research received no external funding”

Conflicts of Interest: “The authors declare no conflict of interest.”

Author Contributions: E.N.M is a PhD student who composed the paper. J.M, as the main supervisor went through the paper and gave constructive feedback. B.C is the co-supervisor who also went through the paper and gave feedback. J.M and B.C contributions were used to improve the paper for submission.

DOI: https://doi.org/10.54216/JCIM.170213
Received: April 10, 2025 Revised: June 23, 2025 Accepted: August 22, 2025

References

[1] Department of Health, "The National Health Care Facilities Baseline Audit National Summary Report," National Department of Health, Republic of South Africa, 2012. [Online]. Available: https://www.hst.org.za/publications/HST%20Publications/NHFA_webready_0.pdf. Accessed: Nov. 13, 2024.

[2] South African National Department of Health, "eHealth Strategy South Africa 2012-2016," South African National Department of Health, 2012.

[3] D. R. Petretto et al., "Telemedicine, e-Health, and Digital Health Equity: A Scoping Review," Clin. Pract. Epidemiol. Ment. Health, vol. 20, no. 1, pp. 1–21, 2024, doi: 10.2174/0117450179279732231211110248.

[4] W. J. Triplett, "Cybersecurity Vulnerabilities in Healthcare: A Threat to Patient Security,"Cybersecurity Innovative Technol. J., vol. 2, no. 1, pp. 15–25, 2024, doi: 10.53889/citj.v2i1.333.

[5] N. Hassan, N. Maarop, Z. Ismail, and W. Abidin, "Information security culture in a health informatics environment: A qualitative approach," in Proc. 2017 Int. Conf. Res. Innovation Inf. Syst. (ICRIIS), 2017, pp. 1–6, doi: 10.1109/ICRIIS.2017.8002450.

[6] ITRC, "2018 End-of-Year Data Breach Report," 2019. [Online]. Available: https://www.idtheftcenter.org/wpcontent/uploads/2019/02/ITRC–2018-End-of-YearAftermath–FINAL–V2–combinedWEB.pdf. Accessed: Jun. 23, 2020.

[7] Ponemon Institute LLC, "Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data," 2016.

[8] R. Roohparvar, "5 Industries That Top the Hit List of Cyber Criminals in 2017," Infoguard Cyber Security, 2017. [Online]. Available: http://www.infoguardsecurity.com/5-industries-tophit-list-cyber-criminals-2017. Accessed: Jul. 02, 2019.

[9] C. M. Mejía-Granda, J. L. Fernández-Alemán, J. M. Carrillo-de-Gea, and J. A. García-Berná, "Security vulnerabilities in healthcare: an analysis of medical devices and software," Med. Biol. Eng. Comput., vol. 62, no. 1, pp. 257–273, 2024, doi: 10.1007/s11517-023-02912-0.

[10] D. Schatz, R. Bashroush, and J. Wall, "Towards a More Representative Definition of Cyber Security," J. Digit. Forensics, Secur. Law, vol. 12, no. 2, p. 8, 2017, doi: 10.15394/jdfsl.2017.1476.

[11] E. Luijif, K. Besseling, and P. De Grassf, "Nineteen National Cyber Security Strategies," Int. J. Crit. Infrastruct., vol. 9, no. 1-2, pp. 3–31, 2013.

[12] Da Veiga, "A Cybersecurity Culture Research Philosophy and Approach to Develop a Valid and Reliable Measuring Instrument," in Proc. 2016 SAI Comput. Conf., 2016, pp. 1006–1015, doi: 10.1109/SAI.2016.7556102.

[13] Aksoy, "Building a Cyber Security Culture for Resilient Organizations Against Cyber Attacks," İşletme Ekonomi ve Yönetim Araştırmaları Dergisi, vol. 7, no. 1, pp. 96–110, 2024, doi: 10.33416/baybem.1374001.

[14] Van 't Wout, "Develop and Maintain a Cybersecurity Organizational Culture," in Proc. 14th Int. Conf. Cyber Warfare Secur., 2019, pp. 457–466.

[15] K. Thomson, R. Von Solms, and L. Louw, "Cultivating an Organizational Information Security Culture," Comput. Fraud Secur., vol. 2006, no. 10, pp. 7–11, 2006, doi: 10.1016/S1361-3723(06)70430-4.

[16] N. Gcaza, R. Von Solms, M. Grobler, and J. van Vuuren, "A General Morphological Analysis: Delineating a Cybersecurity Culture," Inf. Comput. Secur., vol. 25, no. 3, pp. 259–278, 2017, doi: 10.1108/ICS-12-2015-0046.

[17] Corradini, Building a Cybersecurity Culture in Organizations. Berlin/Heidelberg, Germany: Springer, 2020, pp. 63–86.

[18] Huang and K. Pearlson, "For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture," in Proc. 52nd Hawaii Int. Conf. Syst. Sci., 2019, pp. 6398–6407.

DOI: https://doi.org/10.54216/JCIM.170213
Received: April 10, 2025 Revised: June 23, 2025 Accepted: August 22, 2025

[19] Georgiadou, S. Mouzakitis, K. Bounas, and D. Askounis, "A Cyber-Security Culture Framework for Assessing Organization Readiness," J. Comput. Inf. Syst., vol. 62, no. 4, pp. 706–716, 2020, doi: 10.1080/08874417.2020.1845583.

[20] Da Veiga, Cybersecurity Education for Awareness and Compliance. IGI Global, 2019, pp. 72–100.

[21] European Union Agency for Network and Information Security (ENISA), "Cyber Security Culture in Organizations," 2017.

[22] M. Ioannou, E. Stavrou, and M. Bada, "Cybersecurity Culture in Computer Security Incident Response Teams: Investigating Difficulties in Communication and Coordination," in Proc. 2019 Int. Conf. Cyber Secur. Protection Digit. Serv., 2019, pp. 1–4, doi: 10.1109/CyberSecPODS.2019.8885240.

[23] M. Alshaikh, "Developing Cybersecurity Culture to Influence Employee Behavior: A Practice Perspective," Comput. Secur., vol. 98, 2020, doi: 10.1016/j.cose.2020.102003.

[24] Alhogail and A. Mirza, "A Comprehensive Human Factor Framework for Information Security in Organizations," J. Theor. Appl. Inf. Technol., vol. 78, no. 2, pp. 201–211, 2015.

[25] S. H. Bakry, "Development of Security Policies for Private Networks," Int. J. Netw. Manag., vol. 13, no. 5, pp. 567–575, 2003.

[26] Uchendu, J. R. C. Nurse, M. Bada, and S. Furnell, "Developing a Cyber Security Culture: Current Practices and Future Needs," Comput. Secur., vol. 109, 2021, doi: 10.1016/j.cose.2021.102387.

[27] E. Pavlova, "Enhancing the Organizational Culture Related to Cyber Security During the University Digital Transformation," Inf. Secur., vol. 46, no. 2, pp. 239–249, 2020, doi: 10.11610/isij.4617.

DOI: https://doi.org/10.54216/JCIM.170213
Received: April 10, 2025 Revised: June 23, 2025 Accepted: August 22, 2025