Creating a Cybersecurity Culture Framework in Higher Education

Mafika Nkambule[1], Joey Jansen van Vuuren[1] and Louise Leenen[2]
[1]Tshwane University of Technology, Pretoria, South Africa
[2]University of the Western Cape and CAIR, Cape Town, South Africa

nkambulemw@tut.ac.za
Jansenvanvuurenjc@tut.ac.za
lleenen@uwc.ac.za

Abstract: This study provides a framework and strategy for the creation of a cybersecurity culture in higher education institutions. Cybersecurity is identified as very important in higher education institutions have to accept responsibility for protecting the institution's assets and personal information of staff and students. This study focuses on the challenges that higher education institutions confront in creating a cyber-secure environment, of which many relate to culture. Establishing a strong cybersecurity culture can be difficult due to variables such as the institution's size and the relatively short duration of student enrolment, which is three to four years on average. The paper includes a detailed roadmap for creating an appropriate cybersecurity culture in higher education institutions. It emphasises the critical role played by all parties concerned in achieving this goal, including administrators, academic staff, and students. As a result, higher education institutions can build a culture that prioritises cybersecurity and fosters safe behaviour among all participants while adhering to the principles presented in this paper.

Keywords: Cybersecurity, Culture, People, Processes, Technology, Phishing, Social engineering, Higher education

1. Introduction

When creating a cybersecurity program, there should be an overall focus on people, processes, and technology. Unfortunately, security professionals tend to focus mainly on processes and technology when addressing the prevailing cybersecurity challenges contributing to organisations' vulnerability to cyber-attacks. These attacks are primarily phishing attacks, accounting for over 90% of cybersecurity breaches across different organisations, leading to huge data breaches (Wong, Abuadbba, Almashor, & Kanhere, 2022). People are often directly responsible for 'allowing' these attacks to succeed in institutions of higher learning (McIlwraith, 2021). There are several reasons why cybercriminals target people; these reasons include a lack of knowledge and appreciation of what is essential to an organisation and the inability to identify phishing emails. Organisations will continue to suffer if an appropriate cyberculture is not in place. Students' relatively short enrolment periods complicate the establishment of a good cybersecurity culture. Students are, on average, enrolled for only three to four years, depending on their fields of study. Due to the large student numbers, the size of the institutions is another factor responsible for the complexity of developing and maintaining a conducive cybersecurity culture.

Due to the over-reliance on processes and technology, organisations have invested significantly in these two aspects to combat all cybersecurity challenges. Common countermeasures against cyber-attacks include the provision of proper anti-malware and antivirus software, access control, authentication, cryptography, and end-to-end network security. However, cybersecurity is more than network security, and more attention needs to be paid to non-technical aspects that affect cybersecurity (Breda, Barbosa, & Morais, 2017). Human operators are responsible for many cybersecurity vulnerabilities because they are highly susceptible to manipulation (Mouton, Nottingham, Leenen, & Venter, 2018). Mouton et al. (2018) emphasised that social engineering attacks target this vulnerability by using various manipulation techniques to elicit individuals to perform sensitive requests.

The main aim of this paper is to create a holistic framework required for creating a good cybersecurity culture framework for higher education. The authors performed a literature survey to investigate culture-based cyber-attacks. The proposed framework for creating a cybersecurity culture in higher education is based on a comprehensive literature survey and the extensive experience of two of the authors in this field. The main research question is: *What is the framework required for creating a holistic cybersecurity culture in higher education that addresses the vulnerabilities of people, processes, and technology and effectively combats prevailing challenges, particularly those related to social engineering and phishing attacks?* The primary outcome of this study is to propose a holistic framework for creating a strong cybersecurity culture in higher education.

Section 2 is an overview of the literature on the prevailing culture-based cybersecurity challenges. Section 3 introduces and discusses culture as the underpinning component of cybersecurity. In contrast, section 4

proposes a step-by-step guide for cultivating an appropriate cybersecurity culture in higher education. Section 5 lists critical roles requiring a cybersecurity culture in higher education. Section 6 considers data protection within higher education institutions, while section 7 discusses the necessary awareness activities to develop the cybersecurity culture.

2. Background

The higher education landscape industry remains a popular target for cyberattacks, and in these institutions, the number of attacks is increasing. In a poll of 154 higher education institutions in the USA, more than 40% of the institutions reported that security tasks have become much more critical in the past year due to remote learning (SOPHOS, 2021). In 2020, the education sector experienced the highest number of ransomware attacks of all industries (tied with the retail sector), with the education sector having the third-highest rate of ransom payment (35%). SOPHOS indicated that, in 2021, 74% of ransomware attacks on higher education institutions were successful. Research institutions have faced even more threats, including intrusions by hackers organised and financed by foreign governments (Basinger, 2019). The average data breach cost in higher education in 2022 increased from $3.86M to $4.24M (Conte, 2022).

The COVID-19 pandemic caused a move from physical lectures to a largely online mode during this time, and most universities introduced remote learning (Baum, Bełdowski, & Dąbroś, 2022). This new learning approach resulted in university personnel and students relying heavily on technology for teaching, learning, and effectively working from home. Borkovich, Skovira, and Kohun (2021) indicated that working from home introduced several unintended consequences, including:

- New opportunities for cybercriminals as many staff members are not technically savvy and are unlikely to put in the necessary effort to secure their home networks.
- Cybercriminals have lots of time to create malware and phishing attacks and be innovative in how they attack, as they are also primarily working from home.
- There is an increase in the attack surface for cybercriminals (more individuals and institutions could be targeted as these institutions also now work online).

Higher education is among the most vulnerable sectors globally (Toptal, 2019). This is because they store both student and staff records and have interconnected systems where students and researchers collaborate and work. Research data can be very sensitive in nature.

It has become clear that cybercriminals have shifted their focus from technology to humans. Several research articles attribute this change in focus to the fact that it has increasingly become difficult to directly penetrate networks across organisations due to heightened attention to network security, including several products and IT controls implemented over the years (Breda et al., 2017; Mangan, 2021).

Cybersecurity attacks, ranging from phishing to tailgating to impersonation, which are mainly directed at people, keep on increasing year over year (Chaudhry, Chaudhry, & Rittenhouse, 2016); Mimecast (2022) confirms that 96% of companies have been a target for email-related phishing attempts and that email-based cyber threats continued to mutate, causing global havoc. This is also confirmed by Andriu (2023). According to Conte (2022), some of the reasons why cybercriminals succeed with their attacks within institutions of higher learning include:

- The number of legacy systems and processes still being used.
- Lack of appropriate specialists and engineers that can support systems security.
- The number of employees, academics, and students working online and remotely since the COVID-19 pandemic.
- Lack of cybersecurity awareness and culture within higher education leaves them more vulnerable to threats.
- Higher education institutions often struggle to prioritise cybersecurity, similar to the general public, where it is not always taken seriously. Personal cybersecurity practices are perceived as tedious and mundane, which leads many individuals to neglect basic precautions. Within higher education, outdated systems, poor processes, and a lack of cybersecurity awareness further amplify vulnerabilities, making these institutions attractive targets for cybercriminals. This lack of a pervasive cybersecurity culture leaves both individuals and institutions exposed to significant risks (Conte, 2022).

A study done in Ethiopian universities on the current status of cybersecurity in their institutions revealed a variety of difficulties ranging from old software and bad password management to a lack of encryption and insufficient access controls. The 2024 Vega vulnerability assessment reports 11,286 overall discoveries, while Nessus detected 1749 vulnerabilities across all of the institutions' websites. Based on these findings, the study recommends counteractive methods suited to the unique needs of each identified flaw (Eshetu, Mohammed, & Salau, 2024).

According to new research from Malwarebytes Threat Down analysts, 2023 was the "worst year on record" for education, with a 105% increase in known ransomware attacks targeting the global education sector and a 70% increase in ransomware targeting higher education specifically — with nearly half targeting academic institutions in the United States (ThreatDown, 2024).

A robust cybersecurity culture is essential for higher education institutions to safeguard their valuable assets and protect against cyber threats. Based on (Cheng & Wang, 2022), academia has a unique culture, which allows a considerable degree of openness and transparency not available in other industries and presents security vulnerabilities.

3. Methodology

This paper used a literature review as the primary methodology to investigate the primary components and constituents of a framework for a cybersecurity culture in higher education combined with the extensive experience in cyberculture development of two of the authors. The literature review involves a comprehensive and structured approach to identify, analyse, and synthesise existing research and literature on cybersecurity culture in higher education institutions. Khalaf, Youssef, and El-Saadany (2017) introduce a structured approach for research areas such as risk management; Once the literature review is conducted and the relevant studies are identified, a rigorous analysis and synthesis of the findings must be performed. The analysis will examine the literature's key themes, concepts, and frameworks and identify gaps and areas for further exploration.

Significant research has been done in developing culture frameworks for cybersecurity. Goleš Babić (2020) focuses on the development of a framework to address human factors in cybersecurity through organisational culture. This study aims to enhance cybersecurity practices by emphasising the role of organisational culture in influencing employees' cybersecurity behaviour. In addition, the researcher offers insights into how organisations can leverage their culture to mitigate human-related cybersecurity risks and promote a secure work environment. Leenen and van Vuuren (2019) present a framework for developing a cybersecurity culture within military organisations. The article discusses the framework's components, including leadership commitment, policies and procedures, training and education, technological measures, and organisational support. It provides insights into cultivating a strong cybersecurity culture within military contexts to enhance cybersecurity resilience and readiness.

In their cybersecurity culture paper, Kortjan and Von Solms (2014) emphasise the importance of cyber security due to the increasing sophistication of cyber threats. Furthermore, they emphasise the need for individuals and organisations to be aware of the risks and adopt appropriate measures to protect themselves against cyberattacks. Khader, Karam, and Fares (2021) provide a comprehensive overview of the existing research on cybersecurity culture in higher education institutions. They emphasise cultivating a positive cybersecurity culture and highlight its key components: awareness, knowledge, attitudes, behaviours, and organisational support, and conclude by identifying gaps in the literature and calling for further research and practical strategies to promote cybersecurity culture in higher education. Georgiadou, Mouzakitis, Bounas, and Askounis (2022) emphasise the importance of developing a positive cybersecurity culture in higher education institutions. They examine the components of cybersecurity culture, including awareness, knowledge, attitudes, behaviours, and organisational support. In addition, they also explore the factors influencing its development, such as leadership commitment, policies, training programs, and curriculum integration.

A cybersecurity culture framework specific to the higher education environment will be developed based on the insights and knowledge gained from the literature review.

4. Cybersecurity Culture – A Core Component

Cybersecurity involves protecting a broad range of assets, particularly humans and organisations. Maintaining cybersecurity is no longer purely an IT function (Conte, 2022). Conte's research emphasises that maintaining cybersecurity is a collective responsibility involving all organisation members. They contend that individuals at

all levels should actively engage in cybersecurity practices and adopt a proactive mindset toward identifying and mitigating potential risks. Organisations need to foster a cybersecurity culture that permeates all aspects of their operations, promoting a shared sense of responsibility and commitment to cyber defence (Firmansyah, 2024). Cybersecurity culture has various definitions, but the following two are often used. ENISA defines cybersecurity culture as "…the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest themselves in people's behaviour with information technologies" (Agbo-ola, 2022). Veiga's definition is: "The intentional and unintentional manner in which cyberspace is utilised from an international, national, organisational or individual perspective in the context of attitudes, assumptions, beliefs, values and the knowledge of the cyber user" (Veiga, 2016).

Cybersecurity is more than awareness and information security frameworks; it is concerned with making cybersecurity an integral part of an employee's jobs, habits, and conduct (Von Solms & Van Niekerk, 2013). Gcaza and Von Solms (2017) confirm that cybersecurity culture is a primary measure to ensure cybersecurity in a nation or organisation. They also indicate that cybersecurity must have a collective focus throughout the institution, where everyone works together to recognise, prevent and stop attacks of all kinds. A cybersecurity culture ranges from essential things, such as using strong passwords, to more technical concepts, like understanding the signs of breaches. Students and staff need to be made aware of cybersecurity policies and processes and how they directly affect them - this can be communicated through orientation and ongoing communications from the administrators and their professors (Conte, 2022).

4.1 Components of Cybersecurity Culture

The first step in the development of the framework is to identify the different components of a cybersecurity culture. Figure 1 below depicts the generic components to consider in engendering a cybersecurity culture as identified by the authors.

Figure 1: Core Components of a Cybersecurity Culture

These core components include:

- **Raising risk awareness:** The first step is to ensure that no one is left behind and that there is proper cybersecurity awareness among all university stakeholders, including staff and students (Takács & Pogátsnik, 2024). A properly configured cybersecurity awareness programme should include the following (Terranova, 2021) :
- *Assembling a security awareness team: The recommendation is to have a cross-functional team from all business and academic areas. This team will be responsible for designing and developing the cybersecurity awareness programme.*
- *Determining roles for security awareness: This activity ensures that a specific programme is designed for particular employees based on their job functions. The main objective is for an institution to have a training catalogue, ensuring everyone gets the proper training at the right time. Doing so will ensure proper compliance with the industry standard and security of the university.*
- *Identifying levels of responsibility: This activity ensures that specialised training is also designed for specialised groups ranging from management of the different institutional areas, including ICT specialists.*

- *Establishing minimum security awareness for different stakeholders: Cybersecurity awareness programmes can vary from essential to specialised levels. Establishing a minimum level expected from all employees and students is always suitable for the culture and security of the higher education institution.*
- **Adopting policies and measures:** One of the critical activities in driving staff and student behaviour is to design policies that are fit for purpose and ensure that all affected stakeholders sign them as part of their annual agreements to confirm that they have read and understood them.
- **Promoting corporation and information sharing:** Information sharing is crucial for protecting critical infrastructure, according to the Cybersecurity and Infrastructure Agency (CISA, 2020). Higher education institutions can benefit from sharing critical information. For example, if one South African university spots a cyberattack, a threat intelligence platform should inform all other South African universities about this attack. This will enable these universities to tighten their controls in response to this new attack and share resources to help each other fight this new attack. However, in their cybersecurity framework, Microsoft warns that information sharing in cybersecurity should be done in a manner that does not erode privacy or adversely impact freedom (Microsoft, 2014). They further mention that sharing cybersecurity data can introduce several privacy concerns, including:
- *What type of information is shared?*
- *To what extent can it be linked to individuals or organisations?*
- *Who is the information shared with?*
- *How is the information shared and used?*

Proper consultation with all stakeholders, including privacy organisations, is fundamental to successfully implementing an information-sharing programme.

- **Be cognisant of ethical issues:** Ethical issues in cybersecurity include, but are not limited to, managing confidential and personally identifiable information (Fenech, Richards, & Formosa, 2024). Macnish and Van der Ham (2020) argue that structures in the university should be flexible for identifying ethical issues during cybersecurity programmes. Macnish et al. further indicate that, at times, cybersecurity researchers need to act like hackers in order to test the validity of their assumptions and hypotheses. For example, a researcher may send a phishing message to research subjects without seeking prior consent, as that could jeopardise the objective of the research itself.

5. HE Cybersecurity Cultivation Framework

5.1 Cybersecurity Culture Roles for Higher Education

The identification of roles is another necessary process to implement the cybersecurity culture plan. The figure below depicts five groups critical to ensuring a successful cybersecurity culture implementation.

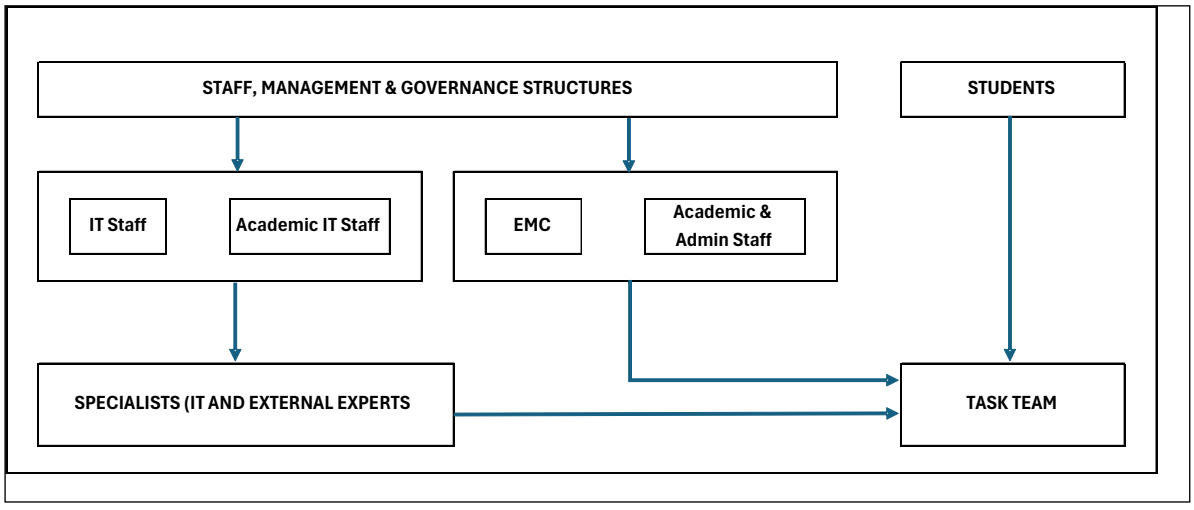

Figure 3: Critical groups in a cybersecurity culture

The diagram illustrates the collaboration between key groups at a higher education institution, to address cybersecurity. Below are the critical roles of each group:

- **University Staff, Management, and Governance Structures:** This overarching group provides strategic direction, policy formulation, and operational support for cybersecurity through:
- ***ICT Support Services (IT Staff):*** *Focused on supporting technologies, identifying threats, implementing controls, and ensuring technical solutions are in place.*
- ***Other Academic and Administrative Staff:*** *Promotes cybersecurity awareness, ensures policy adherence, and supports secure day-to-day operations.*
- ***Executive Management Committee (EMC):*** *Develops the cybersecurity risk management strategy, enforces measures, and allocates resources.*
- ***Other Governance Structures:*** *Ensures compliance with institutional and national cybersecurity standards.*
- **Students:** Students are key stakeholders who can identify threats, report issues, and promote a culture of cybersecurity through awareness training and peer influence, with student leaders playing a significant role.
- **Specialists (IT and External Experts):** This team includes external experts (vendors and Academic experts from the university and other institutions) who bring advanced expertise to identify and mitigate sophisticated threats, install technical controls, and support staff and students.
- **Core Cybersecurity Task Team:** This unified team includes members from ICT Support Services, administrative staff, management, specialists, and students, ensuring cohesive efforts to implement strategies, enhance awareness, and respond effectively to cyber incidents.

5.2 Implementation of the Cybersecurity Culture in HE

The best practices for cybersecurity cultivation involve training and education, management, using suitable systems, and consistently continuing the conversation around cybersecurity. A cybersecurity culture aims to normalise these topics and fields so that they become second nature to everyone in education. However, to get to that point, each educational institution must take the proper steps for integration and training (Cybint, 2021b). *In addition, universities need:*

- Commitment from management.
- More secure processes.
- Educate university staff and students on policies, procedures and awareness strategies (Conte, 2022).

Figure 2 below depicts six recommendations to be adopted and implemented as part of engendering cybersecurity culture in higher education.

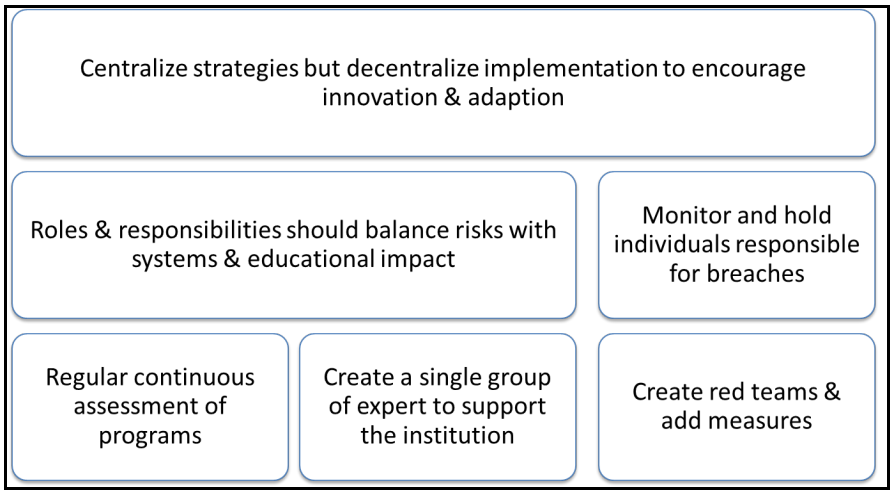

Figure 2: Recommendations for Cybersecurity culture

- **Strategies:** Obtain uniformity and implementation of standards. It is essential to ensure that the design of institutional components like strategy, enterprise architecture and policies is managed centrally. The implementation of all these elements should happen at a local level. Therefore, the implementation should be decentralised to encourage adaptation and innovation.
- **Roles & Responsibilities:** A clear definition of roles and responsibilities helps bring staff members on board and ensure everyone knows their roles in fighting cybercrime within the institution.

- **Responsibility:** Consequence management will ensure everyone complies with and protects the institution. The nature of the consequences will be detailed as part of cybersecurity policy development. In addition, everyone will be encouraged to play an active role in combating cybersecurity in the institution.
- **Continuous assessment:** All programmes should be evaluated regularly to improve performance.
- **Success measures:** If you cannot measure it, you cannot improve. Identifying clear success measures will be very crucial in ensuring that there is measurable improvement in the organisation.

5.3 Steps for Implementation of Cybersecurity Culture

Table 3 below introduces a framework to be used when cultivating cybersecurity culture om Higher Education Institutions – the framework addresses the *practical* steps to be taken to develop a cyberculture. This table has been adapted from research by (Leenen, Jansen van Vuuren, & Jansen van Vuuren, 2020).

Table 3: Steps for Implementation of cybersecurity culture

Preparation Phase	Design Phase	Execution Phase
a: Cybersecurity strategies and policies must be in place. Strategies must include the cyber-safe use of technology, data security, privacy, and include a cybersecurity risk management program	*1*: Set up the core Core cybersecurity task team: task team	*i*: Run awareness and educational campaigns
b: Cyber security team (specialists) must be well-trained and certified	*2*: Define main goals, success criteria and target groups	*ii*: Run cybersecurity exercises
c: Understand current culture and processes and access the risks	*3*: Identify ICT and other supporting divisions	*iii*: Measure the success of the exercises
d: Set up an initial baseline, i.e., the current behaviour	*4*: Identify roles and responsibilities	*iv:* Adjust over time: *Return to Step 6* *It is critical to adjust over time due to changes in technology*
e: Run a pilot activity and measure the impact	*5*: Design cybersecurity communication strategies, awareness programs and exercises with metrics	
f: Get buy-in from executive management	*6*: Review and update the program	

Phase I - Preparation

- **Strategy and policies:** Cybersecurity strategies and policies must be in place, including cyber-safe technology use and privacy. It must also include a detailed risk management programme.
- **Certified teams:** These are part of the specialist teams identified above. They need to be identified and undergo an advanced cybersecurity training programme.
- **Culture, processes, and risks:** It is also essential to ensure that the current organisational culture and processes are well understood and adequately assessed.
- **Baseline:** Assessing how staff and students react to cybersecurity attacks such as phishing is essential before designing and implementing the programme. This will help to measure and understand any improvement through additional training and awareness.
- **Pilot:** Once you have done the initial assessment and established the baseline, it will be essential to put your new plan to the test. Running a pilot and measuring the results will reveal the plan's impact across the institution.
- **Management buy-in:** The results of the pilot will be an excellent artefact for measurements and getting management's buy-in. Once you have management buy-in, you are ready for phase II of the plan.

Phase II - Design

- **Core cybersecurity task team:** During this phase, it will be required that a core cybersecurity team is established. This team will consist of members from across the institution and will be responsible for defining the goals and success criteria of the cybersecurity programme. Team members need to be chosen from admin, academic and maintenance staff and include students.

- **Goals and success criteria:** This stage deals with defining the primary goal, establishing the success criteria, and identifying the target groups. The target groups must include admin, academic and maintenance staff and various student groups such as science or law students, etc.
- **ICT Support & other business units:** Identification of crucial ICT service members is necessary to allocate the actual responsibilities as part of the programme. Also, make sure that they are given the appropriate level of training. Consideration must be given to include representatives from all the IT support staff, not just members from the ICT support department. Technical staff from academic departments, research groups, computer lab managers, etc. must all be included.
- **Design communication strategies:** During this phase, the actual communication and awareness strategies are designed by the core team, incorporating all the elements mentioned above. Messaging should be developed for the different target groups.
- **Review and update:** This will be a living document which will be reviewed and updated as the programme is rolled out.

Phase III - Execution

- **Run campaigns:** This is the final stage of the programme, where the programme is rolled out to all identified target groups.
- **Run cybersecurity exercises:** Exercises designed explicitly for cybersecurity will be rolled out to everyone participating in the programme.
- **Measure:** Once the campaign is completed, including the exercises, it will be essential to measure the programme's impact or success on the overall cybersecurity posture of the university and rerun the campaigns continuously.
- **Adjust:** The programme should be designed to learn from the live campaigns and allow for parameter adjustment. Therefore, the core team should be able to adjust some parameters and rerun the campaigns. Once done, returning to the design phase and updating the original plan will be essential.

6. Conclusion

Cybersecurity culture has become central to combating socially engineered cyberattacks, specifically on humans. This is mainly due to the increasing difficulty for cybercriminals to attack the technology infrastructure, as organisations have invested considerable amounts in building all physical network security controls. However, there still needs to be a gap to be bridged in ensuring that human controls are equally implemented and robust. Therefore, cultivating a cybersecurity culture in higher education institutions is crucial to establishing a reliable human firewall and cybersecurity defence mechanism that keeps social engineering incidents to a bare minimum, if not eliminated.

A cybersecurity culture in higher education will take time to implement and for everyone to adopt. There will be a huge learning curve for staff and students. However, so long as proper awareness and timely communication are done, the university can remain safe, no matter how distant education becomes (Cybint, 2021a, 2021b). This paper considers fundamental elements for cultivating a cybersecurity culture for higher education institutions. This proposed framework seeks to cultivate a cybersecurity culture in higher education institutions and can now be tested and refined.

References

Agbo-ola, A. (2022). Motivating Cybersecurity Awareness within an Organisation: An explorative study from an awareness practitioner's perspective. In.

Andriu, A.-V. (2023). Adaptive phishing detection: Harnessing the power of Artificial Intelligence for enhanced email security. *Romanian Cyber Secur. J, 5*(1), 3-9.

Basinger, J. (2019). A Campus Culture of Cybersecurity. *The Chronical of Higher Education*. Retrieved from https://library.educause.edu/-/media/files/library/2019/3/checulturecybersecurity.pdf

Baum, I., Bełdowski, J., & Dąbroś, Ł. (2022). Remote Teaching and Remote Exams Due to COVID-19: Some Evidence from Teaching Law and Economics. In *Law and Economics of the Coronavirus Crisis* (pp. 237-247): Springer.

Borkovich, D. J., Skovira, R. J., & Kohun, F. (2021). Virtual social distancing: A digital ethnography of online learning. *Issues in Information Systems, 22*(4).

Breda, F., Barbosa, H., & Morais, T. (2017). Social engineering and cyber security. *International Technology, Education and Development Conference, 3*(3), 106-108.

Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016). Phishing attacks and defenses. *International journal of security and its applications, 10*(1), 247-256.

Cheng, E. C., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. *Information, 13*(4), 192.

CISA. (2020). Information Sharing and Awareness. Retrieved from https://www.cisa.gov/information-sharing-and-awareness

Conte, J. (2022). Cybersecurity and Higher Ed: Creating a Culture that Values Cybersecurity. October 19, 2022. Retrieved from https://collegiseducation.com/news/cybersecurity/cybersecurity-and-higher-ed-creating-a-culture-that-values-cybersecurity/

Cybint. (2021a). *How to Build a Cybersecurity Culture in Education*. Retrieved from https://www.cybintsolutions.com/how-to-build-a-cybersecurity-culture-in-education/

Cybint. (2021b, January 12, 2021). How to Build a Cybersecurity Culture in Education. Retrieved from https://www.cybintsolutions.com/how-to-build-a-cybersecurity-culture-in-education/

Eshetu, A. Y., Mohammed, E. A., & Salau, A. O. (2024). Cybersecurity vulnerabilities and solutions in Ethiopian university websites. *Journal of Big Data, 11*(1), 118.

Fenech, J., Richards, D., & Formosa, P. (2024). Ethical principles shaping values-based cybersecurity decision-making. *computers & security, 140*, 103795.

Firmansyah, B. (2024). Cybersecurity Fundamentals. In *Challenges in Large Language Model Development and AI Ethics* (pp. 280-320): IGI Global.

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

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems, 62*(3), 452-462.

Goleš Babić, M. (2020). *Organizational Culture Framework for Mitigating Human Factors in Cybersecurity.* University of Zagreb Faculty of Economics and Business Department of Informatics,

Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity Awareness Framework for Academia. *Information, 12*(10), 417.

Khalaf, M., Youssef, A., & El-Saadany, E. (2017). *Detection of false data injection in automatic generation control systems using Kalman filter.* Paper presented at the 2017 IEEE Electrical Power and Energy Conference (EPEC).

Leenen, L., Jansen van Vuuren, J., & Jansen van Vuuren, A.-M. (2020). *Cybersecurity and cybercrime combatting culture for african police services.* Paper presented at the IFIP International Conference on Human Choice and Computers.

Leenen, L., & van Vuuren, J. J. (2019). *Framework for the cultivation of a military cybersecurity culture.* Paper presented at the 14th International Conference on Cyber Warfare and Security (ICCWS 2019).

Macnish, K., & Van der Ham, J. (2020). Ethics in cybersecurity research and practice. *Technology in society, 63*, 101382.

Mangan, K. (2021). Cyberattacks Are Spiking. Colleges Are Fighting Back. Retrieved from https://www.chronicle.com/article/cyberattacks-are-spiking-colleges-are-fighting-back

McIlwraith, A. (2021). *Information security and employee behaviour: How to reduce risk through employee education, training and awareness* (2nd Edition ed.): Routledge.

Microsoft. (2014). A framework for cybersecurity information sharing and risk reduction. Retrieved from https://download.microsoft.com/download/8/0/1/801358EC-2A0A-4675-A2E7-96C2E7B93E73/Framework_for_Cybersecurity_Info_Sharing.pdf

Mimecast. (2022). *Phishing Update: This Pervasive Risk Just Keeps Growing*. Retrieved from https://www.mimecast.com/blog/phishing-update-this-pervasive-risk-just-keeps-growing/

Mouton, F., Nottingham, A., Leenen, L., & Venter, H. (2018). Finite state machine for the social engineering attack detection model: SEADM. *SAIEE Africa Research Journal, 109*(2), 133-148.

SOPHOS. (2021). The State of Ransomware in Education 2021. *A Sophos Whitepaper.* July 2021. Retrieved from https://assets.sophos.com/X24WTUEQ/at/g523b3nmgcfk5r5hc5sns6q/sophos-state-of-ransomware-in-education-2021-wp.pdf

Takács, J. M., & Pogátsnik, M. (2024). A Comprehensive Study on Cybersecurity Awareness: Adaptation and Validation of a Questionnaire in Hungarian Higher Technical Education. *Acta Polytechnica Hungarica, 21*(10).

Terranova. (2021). How To Build a Strong Security Awareness Program in 2021. Retrieved from https://terranovasecurity.com/how-to-build-a-strong-security-awareness-program-in-2021/

ThreatDown. (2024). *State of Malware 2024*. Retrieved from https://www.threatdown.com/wp-content/uploads/2024/08/ThreatDown-State-of-Malware-2024.pdf

Toptal. (2019). Cybersecurity in Higher Education: Problems and Solutions. Retrieved from https://www.toptal.com/insights/innovation/cybersecurity-in-higher-education

Veiga, A. D. (2016). A Cybersecurity Culture Research Philosophy and Approach to Develop a Valid and Reliable Measuring Instrument. Retrieved from https://www.researchgate.net/figure/Cyber-security-culture-research-philosophy-and-approach_fig3_306407687

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

Wong, A., Abuadbba, A., Almashor, M., & Kanhere, S. (2022). PhishClone: Measuring the Efficacy of Cloning Evasion Attacks. Retrieved from https://arxiv.org/abs/2209.01582