Towards an Ontology-Driven Approach for Contextualized Cybersecurity Awareness

Namosha Veerasamy, Zubeida Khan, Oyena Mahlasela, Mamello Mshali, Matshidiso Marengwa and Danielle Badenhorst
CSIR, Pretoria, South Africa

nveerasamy@csir.co.za
omahlasela@csir.co.za
mmtshali3@csir.co.za
mmarengwa@csir.co.za
dbadenhorst@csir.co.za

Abstract: Traditional training in the form of classrooms and on-site sessions require that participants are present at a specific time and place. Furthermore, traditional learning compels learners to follow a set schedule and does not provide any leeway for those that struggle to understand certain ideas or those that may want to progress faster. While some platforms have been developed to assist with cyber security awareness and digital literacy, they may not offer the benefit of contextualized learning. A "one-size fits all" strategy may not be the best in this rapidly evolving cyber landscape we live in. To assist in solving this problem, a research study was conducted on existing training techniques. This was used to propose an ontology-based solution for cybersecurity awareness that can be applied to certain sectors whereby contextualization is a critical need.

Keywords: Cybersecurity awareness, Cybersecurity, Learning management systems (LMS), Ontology

1. Introduction

The digital landscape continues to grow rapidly, offering many opportunities for participation and inclusion among users. In the current digital era, cybersecurity is a critical concern, and companies need to give priority to education and awareness campaigns to reduce the danger of cyberattacks (Taherdoost, 2024). Part of this strategy will entail building security values into the fabric of the organisation in order to tackle the human risk element.

In low- and middle-income countries (LMICs), individuals have increased access to devices alongside internet connectivity. According to Statistisa.com (2024) the top countries spending time on the Internet daily include: South Africa (9.21 hours), Brazil (9.12 hours), and Philippines (9.09 hours). However, this increased digital dependence may make these and other LMIC vulnerable to cybercrime. There have been several cyberattacks within South Africa including phishing scams, malware, and ransomware attacks (Dagada, 2024; IT Web, 2024). According to a report from Trend Micro, Brazil is the world's second most vulnerable country to cyberattacks (Mari, 2024). Across Southeast Asia, the Philippines has emerged as a key target for cybercriminals with a record high number of 163,279 financial-related phishing attempts on business devices in 2023 (Fintech News Philippines, 2024). These attacks exploit vulnerabilities in user behaviour and cybersecurity awareness and culture which leads to significant financial losses, and disruption to personal and professional lives.

To address this growing threat, various cybersecurity awareness platforms have emerged globally. These platforms offer training modules, simulations, and educational resources for assisting internet users with the knowledge and skills to protect themselves online. However, the implementation of cybersecurity awareness training platforms worldwide is highly variable, as it depends on specific cultural and institutional factors (Almusharraf, 2024)a critical challenge persists: many of these platforms are not well-suited for adaptability and scalability. This may stem from a lack of context and adaptation for certain critical issues. The researchers aim to tackle this problem by investigating the current cybersecurity awareness tools and platforms, which would reveal what is lacking. Thereafter, the lacking features are explained and further unpacked towards an improved cybersecurity awareness platform.

The remainder of the paper is structured as follows. Section 2 follows with the background for this study followed by Section 3, on the Ontological aspects and ontology-based solution is presented, and the authors conclude in Section 4.

2. Background

2.1 Research Approach

A cross-sectional archival research approach was followed in order to analyse existing literature on traditional security awareness techniques. A pragmatic stance was also used in order to look at existing concepts and ideas and look at they role they can play in the research field. The overall benefit of using a pragmatic approach is that is provides more practical solutions to real-word problems. This enabled the researchers to look at more useful and functional ideas to assist with the challenges identified.

The researchers explored traditional awareness techniques, learner management systems (LMSs), and existing cyber security awareness platforms. Thereafter, emerging technologies are presented, and the limitations of existing platforms are discussed.

2.2 Traditional Cybersecurity Awareness Techniques

Traditional security awareness techniques have been used for years to educate users on security threats and create awareness to protect them from cyber-attacks. Some of the traditional security awareness techniques included classroom training, which took the approach of instructor-led training, and users learned about security threats (Tschakert and Ngamsuriyaroj, 2019). The only form of engagement here is question-and-answer sessions, a quiz, or a test at the end of class. Other traditional techniques used posters as visual aids with easy-to-read texts and graphics to highlight some of the important security best practices (Nagyfejeo and Von Solms, 2020). Phishing simulations were also used to test users' knowledge of identifying phishing emails where simulated emails were sent to test users' actions (Rizzoni et al., 2022). Going forward, interactive training can put a spin on classroom-style training by combining instructor-led training lectures, group activities, workshops and role play scenarios.

However, traditional security awareness techniques have limitations in their application, such as focusing on remembering facts instead of developing the skills needed for application, i.e., to make secure decisions in the cyber environment (Abawajy, 2014). They are also insufficient to address the frequent threats that are evolving at a fast pace. Thus, traditional security awareness needs some improvements to accommodate frequent updates on the latest threats and effectively track the progress of security training. Furthermore, as organisational sizes grow it is imperative to offer forms of training that is sustainable, adaptable, and accessible to a wider audience. A wide variety of training methods exist. These include: e-learning, instructor-led learning, role-playing, simulations, videos, mobile learning, microlearning and adaptive learning. Online and virtual platforms present more reachable methods of training provision. A key development in online training are LMSs-this is discussed next.

2.3 Learner Management Systems

We now live in an interconnected world where the traditional concept of formal learning, taking place in a single physical location, is becoming increasingly less relevant (*Encyclopedia of Education and Information Technologies*, 2020).A LMS acts as a virtual campus, facilitating remote learning and thereby enabling students to engage with courses flexibly from any given location (Aldiab et al., 2019). It accommodates diverse needs, including disabled students through accessibility features. Using LMS for cybersecurity awareness enhances the educational experience by pooling learning tools and resources centrally, allowing access to various materials from one platform. The integration of media is another useful feature of LMS as it provides an avenue for learning in different formats (audio, visual, experiential, etc). User Management enables administrators to monitor profiles, assign access rights, track progress, and facilitate communication, ensuring the management of user data and personalised learning within an organisation.

A LMS offers many benefits for training and education. It saves time by centralising schedules, registrations, and documents, and streamlining coordination (S. H. Alshammari et al., 2018; Zheng et al., 2018). Additionally, it provides flexibility, enabling training anytime and anywhere without the need for physical facilities or trainers. Content delivery is consistent across all learners, ensuring uniformity of information. Personalisation is facilitated through tailored learning paths and adaptive content delivery, enhancing effectiveness (H. Alshammari et al., 2018). It is cost-effective, which reduces the expenses associated with traditional training methods like venue rentals and travel. Tools are also embedded to support both asynchronous and synchronous communication, enabling collaboration and community within courses (Kasim and Khalid, 2016).

2.4 Existing Cybersecurity Awareness Platforms

Due to the complexity and constant evolution of security, technological defenses alone are rarely adequate to protect these individuals from online threats (Taherdoost, 2024). The dynamic nature of cyber threats demands that employee security awareness be approached proactively, rather than reactively. Conventional security training techniques are static and not engaging enough to hold learners' attention. However, there are modern training programs that provide workers with the knowledge and abilities they need to defend against cyberattacks. This review examines several popular contemporary security training program platforms, evaluating their features and impact. In recent years, these cybersecurity awareness platforms have become increasingly crucial for organisations aiming to mitigate the risks associated with cyber threats (Greenlaw and Mufeti, 2022). Among the prominent platforms in this domain are KnowBe4 and Mimecast, which both offer comprehensive solutions to enhance cybersecurity awareness. Another tool on the market is TitanHQ. An overview of the features and functionalities of each awareness platform is as follows:

- KnowBe4: This platform is recognized as one of the leading cybersecurity awareness training platforms and equips organisations alike with the tools required to educate and train employees on the recognition and mitigation of cyber threats (KnowBe4, 2024). This is performed using features such as interactive training modules, simulated phishing attacks, real-time reporting and analytics and engaging modules which cover various cybersecurity topics (KnowBe4, 2024).
- Mimecast: This is another prominent cybersecurity awareness platform that focuses on threat intelligence and email security (Mimecast, 2024). This is achieved through the platform's provision of advanced email security solutions which comprise of protection against phishing attacks, malware, and ransomware, email attachment and URL analysis (Mimecast, 2024).
- TitanHQ- user-friendly UI that provides security awareness training with gamification, intelligent reporting, and cyber knowledge assessments for compliance best practices (Titan HQ, 2024).

These platforms play a vital role in helping organisations strengthen defences against cyber threats, and to protect their sensitive data and maintain a secure digital environment. Despite this, there are some limitations with such platforms' ability to cater to certain users' needs. Some shortcomings are brought to light by the literature on cybersecurity awareness platforms in the country of South Africa. These include a lack of contextualisation for the South African landscape (Nagyfejeo and Von Solms, 2020; Vanderkooi et al., 2023) and methods that lack engagement (Devar and Hattingh, 2020; Henning et al., 2017). These limitations could also be applicable to other countries in that there is a strong requirement for training to meet the needs of various types of users.

2.5 Emerging Technologies for Cybersecurity Awareness

Organizations may drastically lower the risk of cyberattacks and safeguard their sensitive data and systems by adopting an organized approach to cybersecurity awareness(Taherdoost, 2024). Key to building cybersecurity awareness is adapting to emerging technologies to provide for more current techniques. Due to growth, popularity and widespread use of emerging technologies, this topic is explored next in order to indicate the role they can play in the enhancement of cybersecurity awareness. Three critical areas were identified and and reviewed at a high level.

- **Artificial Intelligence (AI):** AI can be used to personalize learning experiences by creating content for an individual user needs and learning styles (T. Gasiba et al., 2020; T. E. Gasiba et al., 2020). While these techniques have been explored as a solution, there is still a contextual background missing from some use-cases (Sewak et al., 2023). AI can be harnessed to create customised training models based on their role, threat profiles, skills or experience. While pre-defined content may cover standardised and basic security topics, AI content can be adaptive and tailored to specific knowledge gaps. AI could also be used to build simulations that help to emulate the real world. Furthermore, AI can play a significant role in the monitoring, reporting, and tracking of users' progress.
- **Ontologies:** Ontologies are a branch of AI, with many use-cases. Importantly, for cybersecurity awareness, it can be used for organising and structuring knowledge in cybersecurity awareness programs (Sewak et al., 2023; Syed et al., 2016). By defining relationships between concepts, ontologies enable the development of more comprehensive and interconnected training materials. Ontologies can help to structure the content for various topics cybersecurity which can be helpful to manage and organise the content, especially for training purposes. Furthermore, ontologies can be used for various other purposes like pre-training models for prediction tasks, fine-tuning models to answer domain-

specific questions and, thereafter, even making domain knowledge more explicit in Virtual Reality-based training. Overall, ontologies provide a means of structuring, capturing and connecting data.

- **Virtual Reality (VR) and Augmented Reality (AR):** VR and AR can be implemented to create engaging learning environments and simulations (Alqahtani and Kavakli-Thorne, 2020; Wagner and Alharhi, 2024). Learners can experience the consequences of different cybersecurity practices in a safe and controlled environment. The use of VR simulations provides a realistic format through which users can engage and interact with potential vulnerabilities, attack scenarios and response mechanisms.

2.6 Limitations of Existing Cybersecurity Awareness Platforms

To gain a deeper understanding of the limitations of existing cybersecurity awareness platforms context, we consulted existing literature, and we note the findings here. Firstly, because a majority of current platforms are being developed with a global audience in mind, contextualisation is frequently absent from them (Scholtz et al., 2020; Vassilakos and Martin, 2023). This stance then disregards the unique requirements of users, including their limited access to the internet, their variety of spoken languages, and other socioeconomic considerations (as in the South African context) (Vanderkooi et al., 2023). This problem could also be applicable to various parts of the world where various languages are spoken and also the country faces various socioeconomic challenges. The challenge of the digital divide in which certain demographical and regional groups have unequal access to modern technology can be further confounded by issues such as the use divide in which there are differences in the level of skills possessed. Due to the lack of access and availability some people in developing countries may not have the necessary skills to use technology safely and security. It is thus critical to provide for personalised content in order to try and bridge the digital skills divide and educate the public on best practices in an adaptable and updated environment.

Secondly, a majority of cybersecurity awareness platforms overlook the need for the general public to understand their digital rights and duties in favour of primarily targeting business users to fulfil compliance requirements (Nagyfejeo and Von Solms, 2020). Thirdly, users may not be properly engaged by the typical training methods used by current platforms; however, micro-learning, gamification, and storytelling are examples of contemporary learning strategies that have demonstrated potential to improve engagement and retention of information in this regard (Devar and Hattingh, 2020; Henning et al., 2017).

Lectures, whether face-to-face or online, in an LMS, may lead to a lack of engagement and retention as users become passive and have fewer opportunities for interaction. More active involvement may help users to retain information and feel better engaged. Furthermore, only having theoretical training may leave participants with knowledge that is not relatable or practically applied. The need for more adaptable training can provide users with actionable instances of applications. The concept of Self-regulated learning includes strategies that learners use to get the information they need and adjust their cognitive aspects (Ehsanpur and Razavi, 2020).

Employing organised classification inside already-existing platforms is one suggested remedy, which entails using user demographics and local priorities to organise material, to increase relevance and efficacy (Mongadi et al., 2022). Furthermore, awareness platforms may better connect with their intended audience by including context-specific modules, such as cyber hygiene tips pertaining to the internet usage trends and other culturally appropriate uses (Kappas et al., 2019; Mongadi et al., 2022). The incorporation of personalised learning paths in ontologies offers the potential for adaptive content to bridge individual knowledge gaps.

3. An Ontology-Driven Approach

3.1 Ontological Considerations

Gruber (1993) describes an ontology as an “explicit specification of a conceptualization”. What is meant here in simpler terms is that an ontology is a structured way to represent a domain of discourse such that it is machine processable. It provides a formal representation of knowledge using classes, subclasses, properties, and instances, as building blocks for a domain, such as the cybersecurity awareness domain.

Ontological methodologies consider various aspects like the conceptualisation of the topic, the level of detail of ideas, implementation into an ontology, model evaluation, instantiation of the ontology with examples and future maintenance requirements (updates and addition of features). Ontology reuse is also a key aspect in that it can substantially aid the process and minimise efforts. Ontology design is an evolving process that can be supported by domain experts to provide valuable inputs. In the context of this study, cyber security professionals can provide insights into the topics and areas of expertise that is needed to be incorporated into the cybersecurity awareness training ontology.

A hybrid approach can be employed for ontology development, combining both top-down and bottom-up approaches. For the top-down approach, existing cybersecurity awareness ontologies and knowledge bases can be scanned to identify concepts and relationships. To contextualise this, data collected from local articles and reports can be used to further populate the ontology with specific content. For representation, the ontology will be represented using the Web Ontology Language (OWL) as it is a W3C standard (Semantic Web Standards, 2012).

Ontology-based approaches facilitate structured categorization and knowledge representation of cybersecurity awareness concepts, enhancing understanding and accessibility of these concepts. Domain experts can provide key inputs into the design of the ontology. Our approach involves inputs from literature to guide the development of an ontology.

3.2 Addressing Limitations

The study revealed that while existing platforms contain cybersecurity content and can facilitate learning, there is a need for more contextualised solutions for certain markets. Based on the initial research from Section 3.5, we identified three primary shortcomings of current cybersecurity awareness platforms. We describe these here and in Fig. 1 alongside how an ontology can assist with these shortcomings.

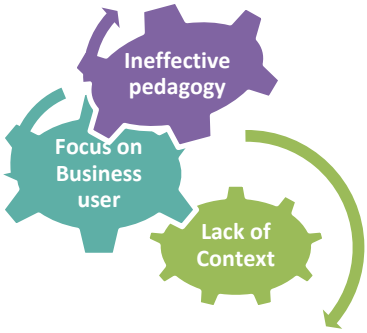

Figure 1*:* Thematic themes identified for limitations within existing platforms

- Lack of context: Existing cybersecurity awareness platforms may lack context-specific content tailored to the specific landscape. The proposed hybrid approach, including bottom-up development, includes the consideration of local articles and policies to complete the knowledge base. Furthermore, an ontology's hierarchy can be used to classify digital literacy levels. This can assist in identifying specific knowledge gaps which can then be targeted with contextualised material for targeted learning. Users could also become hypervigilant (continuous heightened state of assessing potential threats). Therefore, it is imperative to contextualise the information with relevant examples and scenarios so that users are trained to identify potential threat signals and not become overwhelmed with the sheer volume of false indicators.
- Strong focus on business needs only: Here, too, the bottom-up approach will be used to include citizen information concerning a user's rights and responsibilities from human-centred documents rather than only focusing on specific regulations. Users need awareness of their own vulnerabilities to foremost curb risky practices. Thereafter, good practices can also become instilled and applied in the business environment based on habitual behaviour and sound routines.
- Ineffective pedagogy (teaching practices): While ontology cannot solve this in its entirety, it can assist to some degree. The ontology can be integrated with existing LLMs. The LLMs could use ontological knowledge to provide intelligent feedback, recommend learning resources, and assess learner performance.

The following sections propose an ontology-based approach for assisting with the issue that existing platforms may not be adequate for the certain user groups.

3.3 Ontology Design

Ontologies have already been designed and considered for the cybersecurity domain where they represent knowledge about cybersecurity concepts, threats, in a hierarchy (Martins et al., 2020; Syed et al., 2016). These ontologies are used in various decision-support systems. While existing cybersecurity ontologies have been used to structure the domain, they have not been traditionally applied to cybersecurity awareness training. Existing

ontologies can form the basis for the ontology compilation. By re-using existing cybersecurity ontologies, one can translate that structured knowledge into a format that is accessible and engaging for a broader audience.

3.4 Towards Ontology Implementation

For the case of cybersecurity awareness training, ontologies can be used in a processed way shown in Fig 2 and explained here. A fundamental ontology for cybersecurity can form the underlying foundation. This ontology formally defines key concepts for threats, best practices, and their interrelationships in the cybersecurity awareness domain. Software technologies and applications need to be developed to use the machine-processable terms in the ontology to create assessments to measure learners and select relevant blocks/ sub-domains for learning (for instance, a focus on delving into common cyber threats like phishing or cyber bullying). Scenarios and simulations are then created based on this to generate an experience of learning.

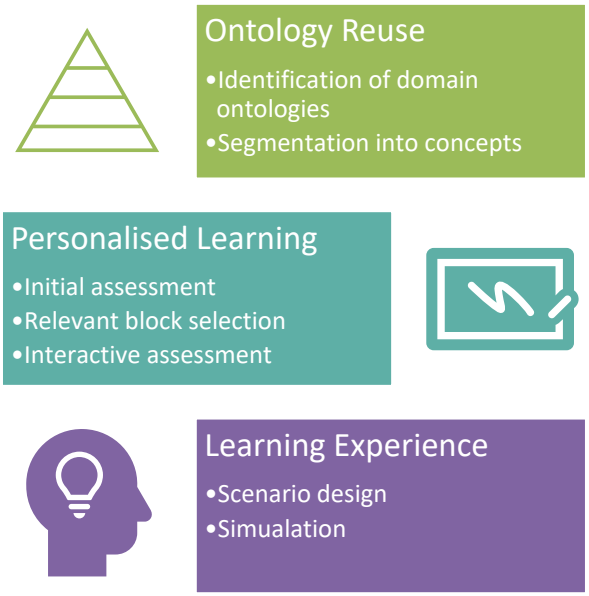

Figure 2*:* Ontology-based approach for cybersecurity awareness

The implementation process is summarised below:

- Ontology reuse and adapt: Existing cybersecurity ontologies are investigated and selected for relevance. Ontologies terms are also extracted from relevant documentation. Using existing ontologies provides an efficient method to compile the foundational outline. It can then to further elaborated and tailored to specifications of each topic area. If needed, cybersecurity awareness concepts are broken down into smaller segments. For instance, the concept of phishing would be broken down into the following components: techniques, impact, motivation, and prevention.
- Personalised learning: Based on a user's initial pre-assessment, the system could provide certain blocks to focus on and generate personalised content and assessments for this user. For instance, the user could be shown a few phishing examples to identify valid emails and phishing examples. Thereafter based on the examples that the student did not identify correctly, the relevant content can be selected and tailored. Assessments can be interactive with further practical examples and training content to solidify key areas (indicators of threats, warning signs, common pitfalls etc).
- Scenarios: Each user thereafter has a personalized learning experience. Thanks to the relationships between concepts in the ontology, training blocks can be designed around real-world scenarios. Users can practice identifying threats and see the consequences of choices in a safe, simulated environment. For the phishing scenario, the student can also be given the opportunity to look at different phishing trademark features, typical senders, and examples. The simulation and display of various phishing examples can help the student identify major pitfalls, as well as clues of the emails being phishing.

Overall, in the ontology setup various interactive elements like tests, scenarios, training modules and assessments will be setup in order to provide content and testing for cybersecurity topics. The use of contextualised and engaging content can help with retention, progression and self-paced learning. During the training development using ontologies, experts will be used to develop and build the materials. Reviews and usability tests can also form part of the process.

4. Conclusion

Internet usage continues to grow, and a concerning gap exists between the rising cyber threats and the level of awareness among citizens. While there are many cybersecurity awareness platforms, most of them cannot be easily tailored to the cybersecurity threat landscape in specific situations. To solve this, the authors performed a literature review on cybersecurity training, and the initial study revealed challenges and opportunities like the lack of contexualised content and the content being too strongly geared for business use only. Furthermore, many technologies like AI, VR and ontologies offer promising areas of exploration. Using the findings, an ontological-based approach was presented as a solution for the inadequacy of existing cybersecurity awareness platforms. The ontology-based approach can assist by contextualizing cybersecurity awareness content for specific users, taking into consideration the digital divide and context specific influences. The ontological implementation provides for the ability to reuse and adapt segments. It also affords the opportunities for scenario development with a personalised learning experience, all of which are aimed at stronger awareness principles retention.

Further research can entail the evaluation of the effectiveness of this approach through the implementation and assessment of the proposed ontological model.

References

Abawajy, J., 2014. User preference of cyber security awareness delivery methods. Behaviour and Information Technology 33.

Aldiab, A., Chowdhury, H., Kootsookos, A., Alam, F., Allhibi, H., 2019. Utilization of Learning Management Systems (LMSs) in higher education system: A case review for Saudi Arabia. In: Energy Procedia.

Almusharraf, A.I., 2024. An Investigation of University Students' Perceptions of Learning Management Systems: Insights for Enhancing Usability and Engagement. Sustainability 16.

Alqahtani, H., Kavakli-Thorne, M., 2020. Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR). Information (Switzerland) 11.

Alshammari, H., Bin, M., Ali, B., 2018. LMS, CMS AND LCMS: The Confusion Among Them Information Technology and Indigenous Language Preservation A Case Study In The Malaya Cham Languages In Vietnam View Project.

Alshammari, S.H., Ali, M.B., Rosli, M.S., 2018. LMS, CMS and LCMS: The Confusion Among Them. Science International 30, 455–459.

Dagada, R., 2024. The Advancement of 4IR Technologies and Increasing Cyberattacks in South Africa. Southern African Journal of Security.

Devar, T., Hattingh, M., 2020. Gamification in Healthcare: Motivating South Africans to Exercise. In: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics).

Ehsanpur, S., Razavi, M.R., 2020. A Comparative analysis of learning, retention, learning and study strategies in the traditional and M-learning systems. Revue Europeenne de Psychologie Appliquee 70.

Encyclopedia of Education and Information Technologies, 2020. , Encyclopedia of Education and Information Technologies.

Fintech News Phillipines, 2024. Philippines Recorded Highest Numbers for Phishing Attacks [WWW Document]. URL https://fintechnews.ph/64749/fintech/philippines-recorded-highest-numbers-for-phishing-attacks/ (accessed 11.18.24).

Gasiba, T., Lechner, U., Pinto-Albuquerque, M., Porwal, A., 2020. Cybersecurity Awareness Platform with Virtual Coach and Automated Challenge Assessment. In: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics).

Gasiba, T.E., Lechner, U., Pinto-Albuquerque, M., 2020. Sifu - a cybersecurity awareness platform with challenge assessment and intelligent coach. Cybersecurity 3.

Greenlaw, R., Mufeti, K., 2022. Reducing Cyber Crime in Africa through Education. In: 2022 IEEE IFEES World Engineering Education Forum - Global Engineering Deans Council, WEEF-GEDC 2022 - Conference Proceedings.

Gruber, T.R., 1993. A translation approach to portable ontology specifications. Knowledge Acquisition 5.

Henning, M., Hagedorn-Hansen, D., von Leipzig, K.H., 2017. Metacognitive learning: Skills development through gamification at the stellenbosch learning factory as a case study. South African Journal of Industrial Engineering 28.

IT Web, 2024. SA businesses: dangerously unprepared for cyber-attacks [WWW Document]. URL https://www.itweb.co.za/article/sa-businesses-dangerously-unprepared-for-cyber-attacks/dgp45qaBEP1vX9l8 (accessed 4.30.24).

Kappas, T., Bournaris, T., Economou, E., Moulogianni, C., 2019. A Systematic Review on Collective Awareness Platforms. In: Communications in Computer and Information Science.

Kasim, N.N.M., Khalid, F., 2016. Choosing the right learning management system (LMS) for the higher education institution context: A systematic review. International Journal of Emerging Technologies in Learning 11.

KnowBe4, 2024. KnowBe4 Security Awareness Training [WWW Document]. URL https://www.knowbe4.com/security-awareness-training (accessed 4.10.24).

Mari, A., 2024. Brazil Is The World's Second Most Vulnerable Country To Cyberattacks [WWW Document]. Forbes. URL https://www.forbes.com/sites/angelicamarideoliveira/2023/09/27/brazil-is-the-worlds-second-most-vulnerable-country-to-cyberattacks/ (accessed 11.18.24).

Martins, B.F., Serrano, L., Reyes, J.F., Panach, J.I., Pastor, O., Rochwerger, B., 2020. Conceptual Characterization of Cybersecurity Ontologies. In: Lecture Notes in Business Information Processing.

Mimecast, 2024. Mimecast Email Security [WWW Document]. URL https://www.mimecast.com/products/email-security (accessed 4.10.24).

Mongadi, J.T., Biljon, J. Van, Merwe, R. Van Der, 2022. Persuasive technology and user experience design guidelines to motivate users for autonomous learning on a digital learning platform in the context of a corporate environment in South Africa. In: 2022 Conference on Information Communications Technology and Society, ICTAS 2022 - Proceedings.

Nagyfejeo, E., Von Solms, B., 2020. Why Do National Cybersecurity Awareness Programmes Often Fail? International Journal of Information Security and Cybercrime 9.

Rizzoni, F., Magalini, S., Casaroli, A., Mari, P., Dixon, M., Coventry, L., 2022. Phishing simulation exercise in a large hospital: A case study. Digit Health 8.

Scholtz, D., Kritzinger, E., Botha, A., 2020. Cyber safety awareness framework for south african schools to enhance cyber safety awareness. In: Advances in Intelligent Systems and Computing.

Semantic Web Standards, 2012. Web Ontology Language (OWL) [WWW Document]. URL https://www.w3.org/OWL (accessed 7.11.24).

Sewak, M., Emani, V., Naresh, A., 2023. CRUSH: Cybersecurity Research using Universal LLMs and Semantic Hypernetworks. In: CEUR Workshop Proceedings.

Syed, Z., Pädia, A., Finin, T., Mathews, L., Joshi, A., 2016. UCO: A Unified Cybersecurity Ontology. In: AAAI Workshop - Technical Report.

Taherdoost, H., 2024. A Critical Review on Cybersecurity Awareness Frameworks and Training Models. In: Procedia Computer Science. Elsevier B.V., pp. 1649–1663.

Titan HQ, 2024. Titan HQ [WWW Document]. URL https://www.titanhq.com (accessed 11.18.24).

Tschakert, K.F., Ngamsuriyaroj, S., 2019. Effectiveness of and user preferences for security awareness training methodologies. Heliyon 5.

Vanderkooi, D., Sangari, M.S., Mashatan, A., 2023. Raising Cybersecurity Awareness Through Electronic Word of Mouth: A Data-Driven Assessment. In: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics).

Vassilakos, A., Martin, R., 2023. Understanding the Challenge of Cybersecurity in Africa: A Holistic Analysis of Southern African Development Community (SADC) and Foundation for Future Research. HOLISTICA – Journal of Business and Public Administration 14.

Wagner, P., Alharhi, D., 2024. Leveraging VR/AR/MR/XR Technologies to Improve Cybersecurity Education, Training, and Operations. Journal of Cybersecurity Education Research and Practice.

Zheng, Y., Wang, J., Doll, W., Deng, X., Williams, M., 2018. The impact of organisational support, technical support, and self-efficacy on faculty perceived benefits of using learning management system. Behaviour and Information Technology 37.