Barriers to Cyber Hygiene in Hybrid Work Environments: A Case Study of a Lesotho Development Parastatal

Lebohang Nkhabu, Machdel Matthee
Department of Informatics
University of Pretoria
Lynnwood road, Pretoria, South Africa
le.nkhabu@gmail.com, machdel.matthee@up.ac.za

Abstract. *This study's objective is to investigate the barriers to maintaining effective cyber hygiene in hybrid work environments, focusing on a case study within a development parastatal in Lesotho. The shift to hybrid work models, accelerated by the COVID-19 pandemic, has introduced new vulnerabilities in cybersecurity, particularly regarding remote work. Utilizing qualitative, research through interviews with IT specialists, managers, and end-users, the study identifies key barriers confirming themes found in literature affecting cyber hygiene in companies namely, user characteristics (such as awareness and attitude),environmental support (awareness and training, policies, leadership, ICT support) and environmental characteristics (organisational culture, poor infrastructure). It is shown that the developing country context of the parastatal exacerbate these barriers.*

Keywords: Cyber hygiene, hybrid work, cybersecurity, remote work, barriers, Lesotho parastatal

1 Introduction

With the rise of digital transformation, organisations worldwide have shifted towards hybrid work environments, blending in-office and remote work setups (Beno, 2021). The COVID-19 pandemic has significantly accelerated this trend bringing forth both opportunities and challenges in maintaining secure information systems (Huang & Yen, 2021). Among these challenges is the increasing importance of cyber hygiene, which refers to the practices and behaviours individuals and organisations adopt to protect themselves from cybersecurity threats (Vishwanath, et al., 2020). Cyber hygiene is also referred to as cybersecurity behaviour in this study.

Hybrid work environments, while offering flexibility, introduce various cybersecurity vulnerabilities, particularly in remote work contexts where organisational oversight and secure infrastructure are limited (Morris & Still, 2023). Emerging economies are progressively allocating resources towards leveraging web-enabled platforms and services (Lallie, et al., 2021). For developing countries such as Lesotho, where infrastructure and cybersecurity literacy may already be constrained, this shift presents significant risks (Mosola, Moeketsi, Sehobai, & Pule, 2019).

This research investigates the barriers to cyber hygiene in a hybrid work model within a Lesotho development parastatal. Using an inductive, qualitative approach, the study aims to explore how the factors impeding cyber hygiene in this specific context.

2 Background

The rapid transition to hybrid work arrangements during the COVID-19 pandemic has fundamentally altered the cybersecurity landscape for many organisations (Beno, 2021). As employees increasingly operate outside traditional office environments, new and more sophisticated cyber threats have emerged (Al-Mohannadi, et al., 2016). This shift has made cyber hygiene, a set of practices aimed at safeguarding information systems more crucial than ever. However, the hybrid work model brings with it a range of challenges, particularly for employees working remotely without the protective measures provided by corporate IT infrastructure. This necessitates a renewed focus on understanding and mitigating barriers to effective cybersecurity practices.

2.1 Cyber Hygiene and Its Role in Cybersecurity

As the pandemic spurred remote work, the need for robust cyber hygiene became clear. Research identifies cyber hygiene as essential for preventing breaches that compromise system confidentiality, integrity, and availability (Kalhoro, Rehman, Ponnusamy, & Shaikh, 2021). Cyber hygiene within remote settings emphasises secure configurations, device usage protocols, and safe internet practices, which are complicated by unsupervised environments and potentially insecure home networks (Droppa & Harakal, 2021).

2.2 Remote Work Challenges and Cyber Threats

Remote work environments inherently elevate cyber risk by relying on public and personal networks, which lack organisational controls. The dependence on personal devices and unmonitored networks has increased the attack surface, making devices susceptible to malware, phishing, and other cyber threats (Borkovic & Skovira, 2020). Moreover, as users perform sensitive activities like online banking and corporate transactions on potentially insecure networks, the likelihood of exposure to cyber-attacks grows (Kovacevic, Putnik, & Toskovic, 2020) .

2.3 Human and Organizational Factors in Cyber Hygiene

Human behaviour is a significant determinant in cyber hygiene practices, influenced by demographic factors, social norms, and cybersecurity awareness levels. Organisational structures and policies also play crucial roles in shaping employee adherence to cybersecurity protocols. Notably, organisations that actively involve management in cybersecurity initiatives experience better compliance and improved cyber hygiene behaviours among employees (Li, et al., 2019).

2.4 Cyber Hygiene in Hybrid Work

The beginning of the COVID-19 pandemic has heightened the necessity to explore and analyse digital transformation (Kabanda & Chingoriwo, 2021). This exploration has exposed many organisations to new cybersecurity risks (Georgiadou, Mouzakitis, & Askounis, 2022). Studies indicate that cyberattacks, such as phishing, malware, and ransomware, have surged during the pandemic due to increased internet use by remote workers (Lallie, et al., 2021). Phishing attacks, for instance, increased significantly as attackers exploited users' reliance on email communications and their lack of awareness of cybersecurity threats when working from home (Georgiadou, Mouzakitis, & Askounis, 2022). Similarly, malware attacks such as ransomware affected critical sectors, including healthcare and education, with remote workers often lacking adequate security measures to protect sensitive data (Pranggono & Arabo, 2020).

Cyber hygiene is central to mitigating these threats, involving practices such as strong passwords, software updates, and multi-factor authentication (Cain, Edwards, & Still, 2018). However, hybrid work environments, particularly in developing regions, present additional challenges. Employees working from home or public spaces frequently connect to unsecured networks, increasing the risk of cyberattacks (Li, Xin, & Siponen, 2022). Without the protection of corporate IT infrastructures, these individuals become the first line of defence, requiring both technical skills and cybersecurity awareness to mitigate risks (Vishwanath, et al., 2020).

2.5 Barriers to Cyber Hygiene

Studies show that it has become increasingly essential to address the human aspects of cybersecurity, and this study aims to address those aspects as barriers in cybersecurity behaviour or simply, cyber hygiene (Li, et al., 2019). Barriers to cyber hygiene in hybrid work environments can be categorised into personal, environmental, and organizational factors.

2.5.1 Demographics

Research indicates that age, gender, and educational background significantly influence cybersecurity behaviours. Younger employees, while more comfortable with technology, may be less cautious about cybersecurity, often neglecting best practices such as password management and software updates (Whitty, Doodson, Creese, & Hodges, 2015). On the other hand, older employees, though generally more security-conscious, may lack the technical expertise to implement effective cybersecurity measures. Gender also plays a role, with studies suggesting that women may exhibit greater caution when sharing information online but also tend to lack confidence in their cybersecurity skills (Anwar, He, Ash, Yuan, & Li, 2017).

2.5.2 Cybersecurity Awareness

One of the primary barriers to cyber hygiene is the lack of adequate training and awareness programs, particularly in developing countries. Many organisations provide limited cybersecurity training, leaving employees unaware of the risks associated with remote work (Hadlington, 2017). Cybersecurity awareness needs to be tailored to specific roles and responsibilities, with ongoing training that addresses emerging threats (Ani, He, & Tiwari, 2019). However, in Lesotho and similar contexts, budgetary

constraints and limited access to professional development opportunities hinder the implementation of comprehensive cybersecurity programs.

2.5.3 Organisational Culture

The role of organisational culture in promoting cyber hygiene cannot be overstated. Organisations that actively promote cybersecurity through policies, regular audits, and leadership involvement tend to have employees with better cyber hygiene practices (Li, Xin, & Siponen, 2022). In contrast, organisations where cybersecurity is treated as the sole responsibility of the IT department often see lower engagement from employees in maintaining secure practices. Furthermore, inconsistent policy enforcement across departments exacerbates this issue, creating gaps in organisational security (Desolda, Ferro, Marrella, Catarci, & Costabile, 2022).

2.5.4 Environmental Factors

Remote workers often use public or home networks that lack the same level of security as office environments, making them more vulnerable to cyberattacks. Additionally, the absence of direct supervision leads to lax cybersecurity practices, such as failing to update software or using weak passwords. Family dynamics, such as shared use of devices or networks, further complicate cybersecurity efforts at home, especially when devices used for work are also accessed by other household members (Kalhoro, Rehman, Ponnusamy, & Shaikh, 2021).

2.6 Framework for understanding citizen's cybersecurity behavior

Li et al. (2022) places the factors discussed in section 2.5 in a framework to depict its interrelatedness in influencing citizens' cybersecurity behaviour. Li's Framework is shown in Fig. 1 below.

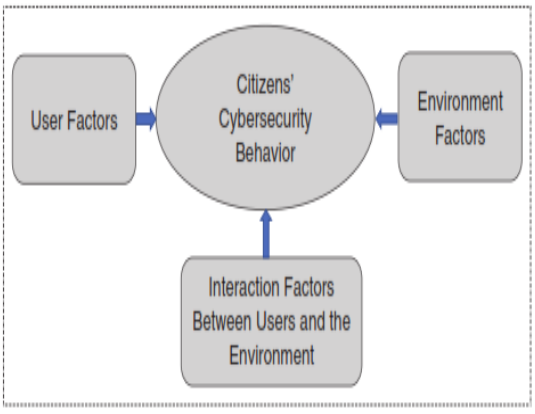

Figure 1. Li's Framework for understanding citizens' cybersecurity behaviour (Li et al., 2022)

Li's Framework identifies user factors like demographics, knowledge and cognitive skills, and environmental factors like activities, support, security, safety, policies, awareness training, sharing and connections, to investigate how they can impact cybersecurity behaviour of people.

Li et al. (2022) also highlights the environmental factors including the characteristics of the home environment, connected devices (IOT) and the shared usage of devices. The interaction between the environmental factors and user factors are guided by the following:

Safety Climate: In organisational contexts, a strong safety climate, shaped by management and peer attitudes, encourages compliance with security protocols. In contrast, home environments rely on the collective awareness and security practices of all family members, making it challenging to establish a cohesive safety climate.

Support Systems: Organisations typically provide robust IT support, training and clear policies to enhance cybersecurity. In contrast, home users often lack access to professional support and rely on informal networks or third-party services, which may not provide adequate protection.

Policies and Training: The presence of formal cybersecurity policies and awareness training in organisations contrasts sharply with the informal and often inconsistent approaches taken by home users. This disparity highlights the need for tailored educational initiatives aimed at improving cybersecurity behaviours amongst citizens.

The framework underscores several important implications for enhancing citizens' cybersecurity behaviour. Firstly, there is a need for comprehensive cybersecurity education that caters to diverse user demographics, addressing specific knowledge gaps and promoting awareness of potential threats. Secondly initiatives aimed at improving the security of home and public networks and devices are essential. This includes providing resources for users to understand how to secure their home environments effectively. Thirdly, developing community-based support systems that facilitate knowledge sharing and provide access to professional cybersecurity resources can help to mitigate risks for remote work users. Lastly policymakers should consider creating frameworks that promote cybersecurity awareness and support for citizens, recognising the unique challenges faced by home users compared to organisational employees.

Note that the focus of Li et. al is also on people working from home, but extends to people working remotely from the field and from public environments. Li et al. go further to break down the environmental factors that may affect behaviour into the characteristics associated with the home environment and the support provided by the work

environment. Fig. 2 below shows an illustration of this:

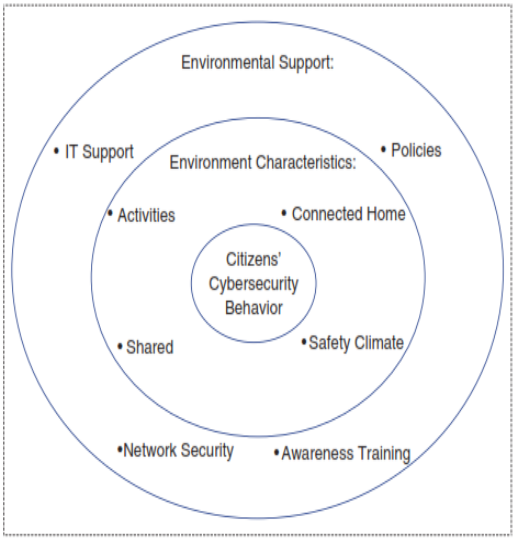

Figure 2. The Environmental Influences on Citizen's Cybersecurity behaviour (Li et al., 2022)

According to Li et al (2022), the environment is characterised by a diverse range of computer and internet-centric activities, such as online shopping, banking, communication, entertainment and education. This contrasts with the more work-focused activities in an organisational context.

Individuals may underestimate the security risks associated with the highly connected home environment. Remote work environments often have a shared environment where family members share internet connections and devices. While convenient, this can lead to privacy concerns and challenges in managing cybersecurity responsibilities.

Organisations can implement comprehensive security plans with significant investments in resources. However, such professional IT support is generally absent in remote work environments, with users relying on third-party cybersecurity services or informal support from social relationships.

Organisational networks are typically more secure compared to home networks, which may have inadequate security measures and configurations. Organisations provide formal cybersecurity awareness training to employees, while home users may only have access to informal training from various sources, such as mass media or social relationships. Organisational environments have relatively complete cybersecurity policies, while home environments often lack clear and comprehensive policies.

The framework emphasises that the characteristics of the home environment, such as diverse activities, connected devices, shared usage and lack of a strong safety climate, combined with limited environmental support in terms of IT assistance, network security, awareness training and policies, create a more challenging landscape for citizens to maintain effective cybersecurity behaviours compared to organisational settings (Li et al, 2022)

3 Methodology

The study employs a qualitative research design within an interpretivist approach, focusing on a single case study of a development parastatal in Lesotho. This is a bi-national organisation established to implement and manage a major water resources development project between Lesotho and South Africa. It has an employment number of around 600 employees. Its primary responsibilities include harnessing water resources for mutual benefit and generating hydroelectric power for domestic use. The project involves the construction and maintenance of dams, tunnels, and associated infrastructure to transfer water from the highlands to South Africa, while also ensuring energy security for Lesotho. It also plays a significant role in environmental management, resettlement planning, and community development in areas affected by the project. In addition, it ensures compliance with legal and environmental obligations, promotes sustainable resource use, and collaborates with various stakeholders to ensure the project's long-term success and minimal ecological impact (LHDA, 2024).

The first author collected data through semi-structured interviews with 13 participants from the organisation, including IT specialists, managers, and end-users from various departments (see Table 1). Purposeful sampling was used to ensure the inclusion of a variety of roles. Job descriptions relate to water quality operation and management, reservoir operation and management, environment management to name but a few. The interviews were conducted between September 2023 and July 2024 using MS Teams. Recordings were downloaded and transcribed. The interviews were conducted in English but the interviewer and interviewee sometimes reverted to Sesotho, the native language to improve correct interpretation.

Table 1. Participant Personal Information

Level	Male	Female	Age bracket
Junior	3	0	33-38
Senior	6	0	38-50
Manager	1	3	48-55

The interviews were designed to gather insights into the participants' experiences with cybersecurity practices during remote work. The interview questions were grouped and designed according to

the framework of Li et al (2022). Organizational documents, such as information security policies, were also analysed to triangulate the data and ensure reliability (Cain, Edwards, & Still, 2018).

Thematic analysis was used to process the interview transcripts, guided by the themes from the framework of Li et al (2022). Environmental (organizational) support, organizational and environmental characteristics, and personal characteristics such as attitudes toward cyber hygiene (Parsons, McCormac, & Butavicius, 2013) were used as broad themes. The analysis aimed to identify barriers and challenges that impede effective cybersecurity practices in hybrid working environments in a developing context. The identified themes are discussed in Section 4.

4 Findings

The findings are presented according to the themes and sub-themes discussed below.

4.1 Environmental support

4.1.1 User awareness and training

This theme emerged from discussions about whether the organisation provided cybersecurity awareness, training, or knowledge to its employees. The awareness initiatives appeared to focus on general cybersecurity practices rather than practical guidance for remote or hybrid work scenarios. Participants generally lacked familiarity with the term cyber hygiene, although many could infer its meaning. A manager noted:

"If you're saying cyber hygiene probably you are saying you are doing the good practices with your computers or with your personal devices."

A junior participant replied:

"I can maybe take it from the term hygiene as in cleanliness. Maybe how we can protect ourselves from someone hacking into the system through us"

As a country with evolving ICT infrastructure and varied digital literacy levels across sectors, formal training on nuanced cybersecurity topics is still emerging.

The participants awareness of cybercrime in general was also explored. Few participants mentioned attacks on local companies such as the Central Bank of Lesotho, the Lesotho National High Court. Others mentioned personal cyber-attacks such as phishing and hacking of WhatsApp. One participant mentioned an attack launched against the case study organisational which fortunately failed.

It appeared that formal knowledge and training were inconsistent across the organisation. For example, a junior participant could not recall receiving any dedicated cyber hygiene training, while others described existing training as overly technical and inaccessible. Another junior participant suggested that the organisation should have a weekly bulletin that provides information on cyber threats and new trends on the cyber threat landscape, to inform every one of them and suggest how they can protect themselves. The interview process itself prompted reflection, as a senior participant noted:

"I realized that there might be practices I can improve after the type of questions I had to answer."

In Lesotho's parastatal sector, which combines technical project delivery with public service obligations, such gaps highlight how cybersecurity awareness must be tailored to a non-uniform workforce. This includes technical field officers, administrative staff, and community-facing personnel, each requiring context-sensitive guidance rather than generic instruction.

4.1.2 Policies

In many Lesotho parastatals, policy development and resource allocation are often reactive, driven by broader national mandates and constrained by budgetary limitations. The organization has an information security policy and most of the participants are aware that it exists, but don't seem to have read it. Some participants did not know that the policy exists, because they said that they normally do not bother to read policies placed on SharePoint. While some staff acknowledged receiving VPNs or work-issued modems, policy clarity was lacking. One manager highlighted the urgency of the pandemic-driven shift to remote work:

"There was no time for anyone to write policies."

This reflects a common reality in Lesotho's government-linked institutions, where digital transformation initiatives are often fast-tracked without accompanying governance frameworks. A senior participant also indicated uncertainty around policy applicability to remote contexts.

It appears that policies exist but staff are generally not aware of it. The following organizational documents were considered: the Information Security Policy, the ICT Acceptable Use Policy, the ICT Asset Management Policy and a Disaster Recovery Plan. The documents touch on password management, device sharing, home and public assets, and the use of personal mobile devices. Clear guidelines are given.

4.1.3 Leadership

Leadership influence emerged as a key enabler. A manager stated:

"Leadership by example and role modelling helped shape responsible behaviour."

This illustrates how in Lesotho's parastatal structure, where hierarchical leadership is strong and often culturally respected, behavioral change can be achieved more effectively through visible senior example rather than formal enforcement mechanisms. Trust and informal mentoring thus play critical roles in shaping secure behaviors.

4.1.4 Infrastructure and IT support

In Lesotho, where many homes lack enterprise-grade internet and power fluctuations are common, technical limitations are significant.

Participants cited issues such as weak Wi-Fi security, outdated equipment, and unsecured smart devices. A concerned was expressed:

"The TV connects to the Internet… they can access it."

This reflects a growing issue in Lesotho's urban households, where the adoption of smart technology often outpaces user awareness about cybersecurity risks. Furthermore, a manager said:

"I am not even sure if we are allowed to use our personal emails for work, I just do it when necessary."

In the parastatal setting, where work often involves cross-border communication, public sector documentation, and sensitive infrastructure data, this ambiguity can expose the organization to significant risk. This also points to a systemic challenge: the coexistence of modern digital demands with legacy policies and limited ICT support capacity in developing nations like Lesotho.

4.2 Environmental characteristics

4.2.1 Connected home and shared public spaces

This theme covers employees' experiences working remotely versus in the office, and how their environment shapes their cybersecurity behaviours. In Lesotho, where infrastructure and connectivity differ drastically between urban and rural areas, remote work often occurs in settings not originally designed for professional tasks.

Participants described common challenges such as domestic distractions, device sharing, and use of insecure networks: "*You are provided with a USB modem for connection which you share with your family"*. A junior participant, who had a more controlled home setup, shared:

"I currently live alone… no one is allowed to come to my home while I work."

Conversely, a senior participant admitted to leaving devices unattended, while another demonstrated awareness by saying:

"I never forget the shortcut Windows logo L to lock my computer."

Such variability is typical in Lesotho's hybrid workforce, where staff may alternate between working from central headquarters, rural project sites, or home environments lacking stable power or connectivity. The disparity in conditions underscores a key issue that parastatal employees must manage cybersecurity responsibilities without consistent infrastructure or supervisory support, making personal habits a critical line of defence.

4.3 User characteristics

4.3.1 Perceptions and Attitudes Towards Cyber Hygiene

This theme investigates how employees perceive cybersecurity risks and their attitudes towards mitigating them

Many employees showed greater trust in the protections offered by office networks:

"There are firewalls, there are proxies... at home, you are not okay."

This belief is grounded in the reality that most homes in Lesotho lack even basic cybersecurity measures, such as network segmentation or up-to-date firewalls. Similarly, a junior participant stated:

"I believe when the organisation gives us the modems, there's some kind of security features."

Such attitudes reflect the broader dependency on institutional protection, common in countries like Lesotho, where individual cyber responsibility is underdeveloped, and access to training or IT support at home is rare. This reliance reinforces a reactive mindset, and employees trust the system when inside the office but feel vulnerable and unsupported outside of it.

Some participants even expressed resignation towards cyber threats, suggesting a lack of empowerment. This indicates the need for a cultural shift within Lesotho's public sector institutions from viewing cybersecurity as a technical issue to seeing it as a shared responsibility requiring both system-level support and individual agency.

5 Discussion

The findings highlight the complex interplay between individual behaviours, organisational structures, and environmental factors that contribute to poor cyber hygiene in hybrid work environments (Droppa & Harakal, 2021).

The findings of this study align with literature and constructs defined by the framework suggested by Li et al (2022): This study confirmed that younger employees were generally more proficient in adopting secure digital practices. In addition, although training exists, participants complained that it is overly technical and inaccessible. Policy implementation is inconsistent and users are

concerned about cyber safety when working from public places or home.

The hybrid work model presents unique cybersecurity challenges, particularly in remote settings where employees are less likely to follow organisational policies. This is consistent with the study by Manzil & Naik (2022). The use of unsecured Wi-Fi networks, shared devices, and weak authentication methods were frequently cited as vulnerabilities as is the case in the investigation by Cross & Gillett (2020).

This study confirmed that organisational culture plays a significant role in shaping cybersecurity behaviours. In environments where management actively promoted and enforced cybersecurity protocols, employees were more likely to adopt good cyber hygiene practices similar to the study by Mosola et al. (2019). Conversely, organisations with less emphasis on cybersecurity training and support saw higher incidences of poor security practices.

The uniqueness of this study lies in the role the context plays in exacerbating the barriers to cyber hygiene. Lesotho is a developing country with unstable electricity supply and poor infrastructure in general. This leads to workers working form different locations depending on the availability of infrastructure, access and electricity. The abdication of responsibility of cyber hygiene to leaders can be ascribed to cultural respect for leaders. In addition, cyber hygiene training in this context is complicated by the parastatal organisation context of non-uniform workers. This context is underexplored in existing literature, which often focuses on developed nations with advanced technological infrastructures.

This study highlights unique cybersecurity vulnerabilities outside controlled office environments. These include unsecured networks, environmental privacy concerns, and socio-cultural barriers.

6 Conclusion

This study provides important insights into the barriers that impede effective cyber hygiene in hybrid work environments, particularly within the context of a Lesotho development parastatal. The findings underscore the need for organisations to adopt a holistic approach to cybersecurity, addressing not only technological factors but also organisational culture and individual behaviours.

To improve cyber hygiene in hybrid work, organizations in developing countries must invest in comprehensive cybersecurity training programs, not only create but enforce strict security policies, and provide adequate technological support for remote workers. From the interviews it appears that good cyber hygiene starts with good leadership and mentorship. By fostering a culture of cybersecurity awareness through effective leadership, organizations can better protect themselves from the growing threat of cyber-attacks in the digital age.

References

Al-Mohannadi, H., Mirza, Q., Namanya, A., Awan, I., Cullen, A., & Disso, J. (2016). Cyber-Attack Modeling Analysis Techniques: An Overview. *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)* (pp. 69-76). Vienna: IEEE. doi:10.1109/W-FiCloud.2016.29

Ani, U. P., He, H., & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology, 21*(1), 2-35. doi:10.1108/JSIT-02-2018-0028

Anwar, M., He, W., Ash, I., Yuan, X., & Li, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*, 37-43. doi:10.1016/j.chb.2016.12.040

Bandura, A. (1986). *Social foundations of thought and action : a social cognitive theory.* New Jersey: Prentice Hall.

Beno, M. (2021, May). Analysis of Three Potential Savings in E-Working Expenditure. *Frontiers in Sociology, 6*. doi:10.3389/fsoc.2021.675530

Borkovic, D. J., & Skovira, R. J. (2020). Working from home: Cybersecurity in the age of Covid-19. *Issues in Information Systems, 21*(4), 234-246. doi:10.48009/4_iis_2020_234-246

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. (ScienceDirect, Ed.) *Journal of Information Security and Applications*. doi:10.1016/j.jisa.2018.08.002

Cross, C., & Gillett, R. (2020). Exploiting trust for financial gain: an overview of business email compromise (BEC) fraud. *Journal of Financial Crime, 27*(3), 871-884. doi:10.1108/JFC-02-2020-0026

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2022). Human Factors in Phishing Attacks: A Systematic Literature Review. *ACM Computing Surveys, 54*(8), 1-35. doi:10.1145/3469886

Droppa, M., & Harakal, M. (2021). Analysis of Cybersecurity in the Real Environment. *2021 Communication and Information Technologies (KIT)* (pp. 1-7). Vysoke Tatry, Slovakia: IEEE. doi:10.1109/KIT52904.2021.9583748

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal, 35*(2), 486-505. doi:10.1057/s41284-021-00286-2

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7). doi:10.1016/j.heliyon.2017.e00346

Huang, M., & Yen, B. P. (2021). Driving Forces for Digital Transformation – Case Studies of Q-Commerce. *International Conference on Electronic Business (ICEB). 21*, pp. 117-128. Nanjing, China: Association for Information Systems.

Kabanda, G., & Chingoriwo, T. (2021). A Cybersecurity Culture Framework for Grassroots Levels in Zimbabwe. *Oriental Journal of Computer Science and Technology, 14*(1-2-3), 17-34.

Kalhoro, S., Rehman, M., Ponnusamy, V., & Shaikh, F. B. (2021). Extracting Key Factors of Cyber Hygiene Behaviour Among Software Engineers: A Systematic Literature Review. *IEEE Access, 9*, 99339-99363. doi:10.1109/ACCESS.2021.3097144

Kovacevic, A., Putnik, N., & Toskovic, O. (2020). Factors Related to Cyber Security Behavior. *IEEE Access, 8*, 125140-125148. doi:10.1109/ACCESS.2020.3007867

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security, 105*, 192248.

LHDA. (2024). *LinkedIn LHDA Page*. Retrieved from LinkedIn: https://www.linkedin.com/company/lesotho-highlands-development-authority-lhda/mycompany/

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45*, 13.24. doi:10.1016/j.ijinfomgt.2018.10.017

Li, Y., & Siponen, M. (2011). A Call For Research On Home Users' Information. *Pacific Asia Conference on Information Systems. 112*. AIS Electronic Library. Retrieved from http://aisel.aisnet.org/pacis2011/112

Li, Y., Xin, T., & Siponen, M. (2022). Citizens' cybersecurity behavior: Some major challenges. *IEEE Security & Privacy, 20*(1), 54-61. doi:10.1109/msec.2021.3117371

Manzil, H., & Naik, M. (2022). COVID-Themed Android Malware Analysis and Detection Framework Based on Permissions. *2022 International Conference for Advancement in Technology, ICONAT 2022*. Goa, India: IEEE Xplore. doi:10.1109/ICONAT53423.2022.9726024

Morris, T. W., & Still, J. D. (2023). Cybersecurity Hygiene: Blending Home and Work Computing. In W. Patterson, *New Perspectives in Behavioural Cybersecurity: Human Behavior and Decision-Making Models* (pp. 107-119). Boca Raton: CRC Press. doi:10.1201/9781003415060

Mosola, N. N., Moeketsi, K. F., Sehobai, R., & Pule, N. (2019). Cybersecurity Protection Structures: The Case of Lesotho. *International Journal of Computer and Information Engineering*, 158-163. Retrieved from https://publications.waset.org/10010176/pdf

Parsons, K., McCormac, A., & Butavicius, M. (2013). The Development of the Human Aspects of Information Security Questionnaire (HAIS-Q). *Proceedings of the 24th Australasian Conference on Information Systems* (pp. 1-11). Melbourne Australia: ACIS 2013: Information systems: transforming the future.

Pranggono, B., & Arabo, A. (2020). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters, 4*(2). doi:10.1002/itl2.247

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, 113160. doi:10.1016/j.dss.2019.113160

Whitty, M. T., Doodson, J., Creese, S., & Hodges, D. (2015). Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords. *Cyberpsychology, Behavior, and Social Networking, 18*(1), 1-7.