How Working from Home has Affected the SA Industries: A Cybersecurity Culture Perspective

Avuya Shibambu
Council for Scientific and Industrial Research
Pretoria, South Africa
ashibambu@csir.co.za

Sophia Moganedi
University of Pretoria
Pretoria, South Africa
moganedis@yahoo.com

Abstract
The notion of working from home is not a new concept. However, it has become a buzzword amid the COVID19 pandemic. Some scholars were already engaging in the work-from-home concept a few years before the pandemic. However, contextualization of this concept from a South African perspective only became compelling during COVID19 times, when various industries had to shift their focus and adjust rapidly. This paper aims to investigate through, literature reviews, and to understand the cybersecurity challenges that emerged as a result of this adjustment. Moreover, interrogate South Africa's readiness and lessons learned from this significant shift.

Keywords: cybersecurity, awareness, working from home, South Africa, cyber-attacks, Covid19

1. Introduction

When the coronavirus hit Wuhan, China in 2019, the world was not ready for the changes that were to follow. An upper-respiratory disease was identified in Wuhan in late December 2019 when dozens of people were reported to have mysterious Pneumonia (World Health Organization, 2020). By the beginning of January 2020, the first death from the virus was reported. To date, millions of people around the globe have been affected and have died from COVID-19 (Statista, 2022). Strange, but necessary, measures had to be put in place to protect the public from this invisible killer. Social distancing – leaving at least 2 meters between people, hand sanitizing, wearing masks, limiting social gatherings, and lockdowns, were just some of these measures taken worldwide (Mendoza-Jiménez et al., 2021; UNICEF, 2021). Organizations quickly made decisions to either lay off their employees or get them to work from home (WFH) (Borkovich & Skovira, 2020; Posel et al., 2021). This came with a total shift in how people conduct their day-to-day work. A new challenge that came from remote working is employees finding themselves in a vulnerable position when it comes to cybersecurity.

COVID-19 had unexpected technological implications that forced employees to quickly adapt to this new change even though they were not fully equipped. The WFH culture meant that organizations had to make provisions for their employees to access work systems outside of their work premises. Virtual Private Networks (VPNs) were used more frequently, and measures of authentication were improved to make sure only authorized users gained access to sensitive systems and data. Although this is the case, some employees still found themselves in breach of security measures by falling victim to attacks such as spam, phishing, giving out sensitive information via social engineering tricks, and so forth (Borkovich & Skovira, 2020).

South Africa, particularly, was faced with several challenges when the lockdown was initiated as a strategy to minimize the spread of COVID19 amongst the people. Outside of the cybersecurity risks mentioned above, there were social implications as well. People found it hard to

follow the lockdown regulations as passed by the South African government and supporting departments, as a result, there was looting, breaking the curfew rules, and breaking the rules to not go to places of entertainment such as nightclubs (Business Tech, 2021). It took time for people to get used to the new normal and this led to the virus spreading like wildfire.

The lockdown was a necessary measure to prevent the COVID19 spread and the benefits of working from home were experienced by both employees and employers. For employers, WFH meant less operational costs such as water and electricity usage, more productive employees, motivated employees, less time taken away from work (sick leave, etc.), and so forth (Rachmawati et al., 2021; Tusl et al., 2020). Employees had a more balanced work-life relationship, were more motivated to work, spending less money commuting to and from work, and many more (Ipsen et al., 2021). Because there were few cars on the road, the environment also benefitted as there was less carbon emission (Rachmawati et al., 2021).

It was not long until hackers found an opportunity to disrupt organizations while their employees were exploring the notion of WFH. As mentioned earlier, businesses found new ways to conduct business and keep in contact with clients, stakeholders, and employees, and this included conducting meetings online. Zoom and Teams. These communication platforms were among the most used applications for both personal and business-related calls. In SA, there was a trend of Zoom calls being hacked. An incident is recorded where the SA parliament was holding a virtual meeting and hackers sent a flood of pornographic images to the video call as well as hurled racially and sexually abusive insults (eNCA, 2020).

The sections to follow will report on the impact working-from-home has had on organizations when it comes to their cybersecurity culture. Section 2 presents a discussion on cybersecurity threats that emerged as a result of the WFH model. Although this paper acknowledges that these cybersecurity threats were not new to organizations, their rapid occurrence compromised several organizations beyond their response capabilities. Section 3 interrogates South Africa's readiness to accept the notion of WFH and built the capability to handle these cybersecurity threats that impact different organizations. Section 4 draws guidance from all these sections to provide a well-known perspective yet not fully comprehended by several organizations that can be adopted as an initial effort to minimize the threats and impact. Section 5 provides a summary of the discussions presented in this paper.

2. Cybersecurity threats introduced by the WFH model

Human errors have predominantly contributed to global cybersecurity issues (Borkovich & Skovira, 2020). However, the WFH notion has exacerbated these issues as the cyber threat landscape enlarged due to remote working. Cyber attackers have seen an opportunity to exploit security weaknesses as employees establish remote connections to various organizational networks and information systems (Georgiadou et al., 2022). The Healthcare sector became a target during the pandemic and its network and systems compromise meant citizens' life and healthcare information were at high risk (Williams et al., 2020).

Common threats that have always been of great concern in many organizations and to various cybersecurity professionals were accelerated beyond the cybersecurity professionals' ability to quickly respond. Khan et al. (2020) conducted a study on the common but dangerous cyber threats which worsened during the pandemic. Their discussions elaborated on the top 10 threats and materialized attacks that compromised various organizations since the first hard level 5 lockdown, globally.

Malware and phishing techniques stemmed out to have been the most prevailing types of cyber-attacks during the pandemic. Phishing email subject lines and malware signatures had reference to COVID-19, which took advantage of the pandemic and social panic mode. Although phishing attacks are the commonly known techniques used to harvest sensitive information from users and contribute to 61% of cyber incidents, it remains the predominating technique during the pandemic (Naidoo, 2020).

Fake websites and links shared through social networking platforms to what was perceived to be informational platforms about the pandemic, precautious measures and vaccines have delivered malware into various organizational network

infrastructures. While in another study, Khan et al. (2020) assert that World Health Organization (WHO) as a trusted health organization had its website cloned and allegedly claimed to provide WHO-approved COVID-19 vaccine. As a result, numerous people have unknowingly disclosed their credit card information to perpetrators while trying to purchase the vaccine kit via this fake cloned website (Khan et al., 2020).

Online video conferencing platforms have enabled many organizations to continue their businesses during the early days of hard-level global lockdown. Zoom, Microsoft Teams, and Google Meet became the predominantly used video conferencing platforms (Gauthier & Husain, 2021; Khan et al., 2020). This significant increase in the use of these platforms was motivated by the variety of functions and features available to enable communication between organizations, clients, and employees (Singh & Awasthi, 2020). This meant that major and critical industries had to adopt those platforms to continue business operations, thus increasing the risk appetite (Khan et al., 2020).

As more organizations adopted these platforms, various vulnerabilities were discovered, which led to various countries banning the use of Zoom video conferencing due to insecure configurations which raised security concerns (Yadav, 2021). These concerns and the ban were a result of the security vulnerabilities that were exploited by cyber attackers (Singh & Awasthi, 2020). The exploitability of these vulnerabilities raised data privacy concerns, as these video conferencing platforms were penetrated by uninvited meeting attendees (Kagan et al., 2020).

3. South Africa's readiness to adopt the WFH model and deal with cybersecurity threats

Various scholars in different academic disciplines have interrogated South Africa's readiness to respond to cybersecurity challenges that emerge as the result of the significantly evolving Information and Communication Technology (ICT). These research focus and efforts aimed to trigger extensive debates in the South African government and its agencies. Thus far, little is known about the cybersecurity readiness state (Veerasamy et al., 2019). Although the cybersecurity issues and readiness from a South African perspective have been an ongoing debate and the readiness status remains unknown, the pandemic compelled the South African government and its agencies to rethink this readiness status and respond promptly. Furthermore, several South African government and locally based organizations failed to convey some level of adaptability, sustainability, and resilience in their cybersecurity units and structures.

In 2020 one of the largest private healthcare and hospitalization providers in South Africa had its admission and other business systems compromised. Although the organization claims that no systems hosting patient data were compromised, the fact remains that it had to operate with some of its affected systems being shut down to prevent the widespread of the attack. In 2021, the Department of Justice and Constitutional Development was hit with ransomware causing critical systems to be unavailable to internal and external stakeholders (Pieterse, 2021).

In addition to cyberattacks that affected various sectors, the Education sector struggled to adjust to the changes that required ICT to be integrated into education systems to ensure continuous learning and maintenance of good education standards. This is to illustrate that the current state of ICT is not well put in place to enable adaptability during stressors. Consequently, exposing a gap in the concept of security and the ability to respond to cyber threats.

Cyber-attacks have always been considered an IT problem, thus making other non-IT-related departments within the organization pay no attention to these issues, especially social-engineering attacks. From a South African context, the notion of working from home raises many security and privacy concerns which were not carefully considered during the hard levels of the lockdown. The WFH notion introduced unpredicted cyber risks to organizational sensitive data, hence the numerous attacks.

Working from home only means a limited number of security settings and policies get to be applicable and functional, especially on users' machines. Apart from the security settings, home networks do not guarantee trusted and reliable connections especially when users need to connect back to organizational networks.

According to Chigada and Madzinga (2020), the threat landscape expands, even more, when users use their devices to connect to the organizational network and systems. This is because the majority of home network devices are poorly configured and fail to ensure secure and reliable connections (Abukari & Bankas, 2020).

Having an unmanaged personal device connecting through an untrusted and unreliable network can expose sensitive information and introduce network vulnerabilities (Abukari & Bankas, 2020). Although Abukari and Bankas (2020) recognize VPN as a technical measure that can be used to mitigate network connection security and related concern, it is not adequate to guarantee secure and reliable connections. This is because a VPN connection must be established by the user when they wish to access the organizational systems. However, the user can still perform other tasks without establishing the VPN connection. Nothing prevents the user from visiting malicious websites and responding to phishing attacks when they are not connected to the organizational network. Therefore, this study argues that mitigation techniques are beyond technical measures that can be deployed by an organization.

Although cyber-attacks and cybercrimes are global issues, South Africa's cybersecurity readiness is still unclear if not non-existence. Thus, questioning the capacity of various organizations within the South African borders to fully adopt and embrace the concept of working from home amid the cyber-attacks emerging as a result of human error and social engineering.

4. Creating a Cybersecurity Culture through Awareness

Cybersecurity awareness training is not a new concept in the broader spectrum of cybersecurity. This concept has been a major focus in various research debates and business discussions that looks to approach and minimize the cyberattacks and incidents resulting from human error and social engineering techniques. Pieterse (2021), Abukari and Bankas (2020) are of the view that cybersecurity awareness training and awareness programs are essential in organizations as an approach to minimizing cyber-related attacks and shifting towards building security-focused cyberculture.

South African organizations should put people at the center of their cybersecurity programs and strategies' discussions and planning. For many decades, anti-virus solutions have been accepted as the first line of defense in cyber-attack-related matters. However, the notion was changed when many organizations encountered threats and compromises as a result of human error and social engineering techniques. Thus, introducing the concept of cybersecurity awareness training and education.

This paper assumes that, as much as organizations are willing to invest money in their security tools, at least some greater effort must be dedicated to empowering users from a cybersecurity perspective. Security tools are as effective and efficient as the users. The South African Banking Risk Information Centre (SABRIC) has highlighted that the cyber-attacks that compromise South African organizations have caused them to lose at least 157 million dollars, which is close to three billion in rands, annually (Kshetri, 2019). This means that organizations will need to assess their cybersecurity strategies and prioritize employee awareness and training. However, to ensure that these security awareness training initiatives are successful, the approaches should consider the relevance of the information being shared with employees and also make sure that employees understand how they are to respond to cyber-attacks especially social engineering attacks (Bada et al., 2014). Kritzinger and Von Solms (2010) recommend the consideration of practical aspects and challenges relating to the implementation of the WFH model from a security awareness perspective. Their recommendation outlines some important areas which include the social impact on the employees that must be carefully considered and understood by organizations and also employees working from home. This area is mostly focused on the behavior of the employees changing and becoming more conscious (Abawajy, 2014). In addition, the understanding of cultural factors and how they influence an intended behavior must be considered when designing and implementing security awareness training and content.

Various organizations have taken the initiative to integrate cybersecurity awareness into their technical security tools. These tools enable organizations to not only create cybersecurity awareness training and sharing of content but create a practical sphere of assessing the risk

appetite from the users' perspective through phishing simulations. These simulations give the security teams within the organization an overall view of the awareness level of the users by how they respond to these simulations which simulate real attacks. Moreover, these tools can automate training and phishing simulations to ensure that awareness training and sharing of content are done throughout the year and across various business units.

Although these security awareness and training platforms are beneficial to many organizations, they have not been easily adoptable in the South African context due to the default content embedded in these platforms. Some organizations have found it challenging to conduct security awareness programs using these European content-generated platforms as they do not apply to the South African context and culture. Thus, rendering these platforms not effective. However, these platforms have advanced to enable additions and modifications of security awareness content, which will allow South African content to be contextualized to fit the cultural setup and match the employee's cognitive characteristics (Bada et al., 2014).

The full realization of these security and awareness training platforms can enable South African organizations to create a cybersecurity culture even outside the borders of office premises. This study believes that the traditional methods of having cyber awareness posters and banners on office walls are no longer effective due to working from home. Therefore, these online platforms enable the organization to reach employees regardless of location. Also, these platforms enable the awareness level amongst employees to increase because the training and awareness strategies are becoming interactive (Abawajy, 2014).

Cybersecurity awareness training and programs can be successful if some effort and consideration are put into their development and implementation. For achieving successful security awareness training and programs in South Africa, this paper proposes taking guidance from Bada et al., (2014). The following considerations would benefit South African organizations when developing and implementing security awareness training and programs:

- Communication: Organizations need to understand how security awareness training and programs will be communicated to the employees.
- Context and relevance: Employees are likely to remember content that is relevant to their day-to-day functional duties. This is where the content must be specific and relevant to provide the employee with information on how the element of security relates to them and how they can change their behavior while not affecting their performance.
- Humor: A sense of humor has a way of getting people to share information when they find something funny but informative.
- Language: different units within an organization use different business languages to communicate. Consequently, employees will easily remember a language they understand. Consideration of the language will enable the employees to be interactive and easily understand the message conveyed through the awareness training

5. Conclusion

This study took a look at how COVID19 started and brought about a new way of working through the WFH model. Benefits were highlighted, ranging from those experienced by the employer, employee, and the environment at large. New cybersecurity threats were also introduced by the pandemic and SA was given a closer look in light of this. It is the assumption of this study that SA is not ready to fully adopt the WFH concept from a cybersecurity readiness perspective. However, adopting the security-focused cyberculture as discussed by Pieterse (2021) can enable various organizations to build towards being cyber resilient while embracing the WFH model. Also, organizations should be prepared to put more effort into their cybersecurity awareness and training programs because this is a continuous process that keeps up to date with advancing social engineering and cyber-attack techniques.

References

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

33(3), 237–248. https://doi.org/10.1080/0144929X.2012.708787

Abukari, A. M., & Bankas, E. K. (2020). Some cyber security hygienic protocols for teleworkers in Covid-19 pandemic period and beyond. *International Journal of Scientific and Engineering Research (IJSER)*, *11*(4), 1401–1407.

Bada, M., Sasse, A., & Bada, M., Sasse, A., Nurse, J. (2014). Cyber Security Awareness Campaigns: Why They Fail to Change Behavior. *International Conference on Cyber Security for Sustainable Society*, 38.

Borkovich, D. J., & Skovira, R. J. (2020). Working From Home: Cybersecurity in the Age of Covid-19. *Issues In Information Systems*, *September*. https://doi.org/10.48009/4_iis_2020_234-246

Business Tech. (2021). *Over 400,000 people have been arrested for breaking South Africa's Covid-19 rules*. https://businesstech.co.za/news/lifestyle/481707/over-400000-people-have-been-arrested-for-breaking-south-africas-covid-19-rules/

Chigada, J., & Madzinga, R. (2020). Cyberattacks and threats during COVID-19 : A systematic literature review Coronavirus Disease-2019. *South African Journal of Information Management*, 1–11.

eNCA. (2020, May 7). *Parliamentary virtual meeting hacked with porn images*. https://www.enca.com/news/parliamentary-virtual-meeting-hacked

Gauthier, N. H., & Husain, M. I. (2021). Dynamic Security Analysis of Zoom, Google Meet and Microsoft Teams BT - Silicon Valley Cybersecurity Conference. In Y. Park, D. Jadav, & T. Austin (Eds.), *Silicon Valley Cybersecurity Conference* (pp. 3–24). Springer International Publishing.

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. https://doi.org/10.1057/s41284-021-00286-2

Ipsen, C., van Veldhoven, M., Kirchner, K., & Hansen, J. P. (2021). Six key advantages and disadvantages of working from home in europe during covid-19. *International Journal of Environmental Research and Public Health*, *18*(4), 1–19. https://doi.org/10.3390/ijerph18041826

Kagan, D., Alpert, G. F., & Fire, M. (2020). Zooming Into Video Conferencing Privacy and Security Threats. *ArXiv*, 1–22.

Khan, N. A., Brohi, S. N., & Zaman, N. (2020). Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. *TechRxiv Powered by IEEE*, *May*, 1–6.

Kritzinger, E., & Von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers and Security*, *29*(8), 840–847. https://doi.org/10.1016/j.cose.2010.08.001

Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), 77–81. https://doi.org/10.1080/1097198X.2019.1603527

Mendoza-Jiménez, M. J., Hannemann, T. V., & Atzendorf, J. (2021). Behavioral Risk Factors and Adherence to Preventive Measures: Evidence From the Early Stages of the COVID-19 Pandemic. *Frontiers in Public Health*, *9*(June), 1–14. https://doi.org/10.3389/fpubh.2021.674597

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, *29*(3), 306–321. https://doi.org/10.1080/0960085X.2020.1771222

Pieterse, H. (2021). The Cyber Threat Landscape in South Africa: A 10-Year Review. *The African Journal of Information and Communication*, *28*(28), 1–21. https://doi.org/10.23962/10539/32213

Posel, D., Oyenubi, A., & Kollamparambil, U. (2021). Job loss and mental health during the COVID- 19 lockdown: Evidence from South Africa. *PLoS ONE*, *16*(3 March), 1–15. https://doi.org/10.1371/journal.pone.0249352

Rachmawati, R., Choirunnisa, U., Pambagyo, Z. A., Syarafina, Y. A., & Ghiffari, R. A. (2021). Work from home and the use of ict during the covid-19 pandemic in indonesia and its impact on cities in the future. *Sustainability (Switzerland)*, *13*(12), 1–17. https://doi.org/10.3390/su13126760

Singh, R., & Awasthi, S. (2020). Updated Comparative Analysis on Video Conferencing Platforms- Zoom, Google Meet, Microsoft Teams, WebEx Teams and GoToMeetings. *Easy Chair: The World for Scientist*, 1–9.

Statista. (2022). *Number of novel coronavirus (COVID-19) deaths worldwide as of August 5, 2022, by country*. https://www.statista.com/statistics/1093256/novel-coronavirus-2019ncov-deaths-worldwide-by-country/

Tusl, M., Kerksieck, P., Brauchli, R., & Bauer, G. F. (2020). Perceived impact of the COVID-19 crisis on work and private life and its association with mental well-being and self-rated health in German and Swiss employees: a cross-sectional study. *To Be Submitted*, 1–21.

UNICEF. (2021). *UNICEF GLOBAL COVID-19 Final Report* (Issue 23 February 2021). http://libdcms.nida.ac.th/thesis6/2010/b166706.pdf

Veerasamy, N., Mashiane, T., & Pillay, K. (2019). Contextualising cybersecurity readiness in South Africa. *14th International Conference on Cyber Warfare and Security, ICCWS 2019*, 467–475.

Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity risks in a pandemic. *Journal of Medical Internet Research*, *22*(9), 7–10. https://doi.org/10.2196/23692

World Health Organization. (2020). *Archived: WHO Timeline - COVID-19*. https://www.who.int/news/item/27-04-2020-who-timeline---covid-19

Yadav, R. (2021). Cyber Security Threats During Covid-19 Pandemic. *International Transaction Journal of Engineering*, *12*(3), 1–7. https://doi.org/10.14456/ITJEMAST.2021.59