sciendo

Land Forces Academy Review
Vol. XXVIII, No. 3(111), 2023

A PHENOMENOLOGICAL STUDY OF THE LIVED EXPERIENCES OF IT AND CYBERSECURITY PROFESSIONALS IN BOTSWANA: INVESTIGATING THE PERCEIVED LEADERSHIP EFFECT ON SUPPLY CHAIN CYBERSECURITY

Andreas VASSILAKOS
Capitol Technology University, Laurel, MD, USA
avassilakos@captechu.edu

Ronald MARTIN
Capitol Technology University, Laurel, MD, USA
rlmartin1@captechu.edu

ABSTRACT

This qualitative study aimed to investigate the experiences of cybersecurity professionals in the context of supply chain cybersecurity in a developing nation. Sixteen professionals from various industries in Botswana were interviewed. The study found that despite the critical role of cybersecurity as an organizational resource, it was still undervalued and underdeveloped, and leadership lacked comprehension of its importance. The participants expressed concerns about the increasing cybersecurity threats, lack of reporting, and technological inadequacies. The study recommends that organizations should develop a comprehensive cybersecurity strategy that includes policies, procedures, technical controls, vendor management, employee awareness and education, regular risk assessments, and incident response plans. The authors also proposed further research steps on supply chain cybersecurity for developing nations. The study contributes to the literature on supply chain cybersecurity in the context of developing nations and provides practical recommendations for organizations to enhance their cybersecurity measures.

KEYWORDS: Supply Chain Management, Information Systems, Information Technology, Information Assurance, Management, Cybersecurity Management, Developing Nations, Africa

1. Introduction

Cybersecurity is an issue of concern for governments, enterprises, and citizens at a global scale. The gravity of securing digital systems is particularly essential within the context of developing countries, as their efforts towards economic prosperity and growth can be disrupted by nefarious actors. This becomes a concerning matter when appropriate controls are not in place. According to Kshetri (2019), *"Cybersecurity is considered to be as a luxury, not a necessity in many African economies. Its importance has not yet been sufficiently appreciated or acknowledged in the continent"*. Interpol (2020) identified

DOI: 10.2478/raft-2023-0022
© 2023 Andreas Vassilakos et al. This work is licensed under the Creative Commons Attribution-Non Commercial-No Derivatives 3.0 License.

various factors that are responsible for the increasing cyber and cyber-enabled crime in Africa, including *"ignorance and mal-usage of ITC, neglect of updates' requirements for technical material, use of software without licenses and use of outdated technology"; "poverty, unemployment and a high number of jobless IT students"; "Lack of technical and infrastructural frameworks to combat cybercrimes"*; and *"Political instability and social problems"*.

Digital transformation is currently predominantly observed in developed countries; however, it is expected to expand worldwide as technological innovations become more cost-effective and obtainable (Reva, 2020). As a result, developing nations may experience an increase in cyber incidents. Currently, a significant proportion of African countries have not devoted sufficient resources to address both current and emerging cybersecurity issues (Reva, 2020). According to Kshetri (2019), *"organizations must increase investment in cybersecurity technologies, provide cybersecurity-related training to employees and appoint professionals such as CISOs"*.

Despite the increasing risks in the cyber realm, the necessary skills associated with protecting themselves have not yet been developed by Internet users (Kshetri, 2019). The lack of experience and lack of technological literacy has been an issue with populations in Africa, which combined with a low level of proficiency in English, can be problematic when defending against cyber threats (Kshetri, 2019).

According to Bada et al. (2018), *"several reports are depicting a bleak picture regarding the unprecedented increase of cybercrime in Africa"*. Following a study employing twelve focus groups across six African countries, Bada et al. (2018) discovered that no national awareness programs exist, ICT literacy remains low, and organizational leaders significantly underestimate the issue. Consequently, Bada et al. (2018) suggested that African nations establish a central authority to orchestrate existing ad-hoc awareness endeavors, focus on specific target groups such as subject matter experts, mobile-phone users, and executive board members, and seize the unique opportunity to integrate ICT literacy campaigns with cybersecurity principles, ultimately cultivating societal norms that endorse best practices.

Study Background

Botswana was selected as the country of focus by the authors. As a result of successful regulatory reform, Botswana's progressive telecom market has stimulated competition, contributing to elevated mobile penetration rates, the implementation of cutting-edge broadband technologies, and decreased connectivity expenses, all while depending on satellites and adjacent nations for international bandwidth (Central Intelligence Agency, 2023). According to the Ministry of Transport and Communications of the Republic of Botswana, *"the community is well connected with mobile network covering more than 90% of the population. Internet usage is increasing throughout the country with many people using the mobile services to access the Internet, more especially the social media; the country's mobile broadband subscription was 1 409,274 as of Dec 2016"*. Sarefo, Dawson, and Banyathang (2023) examined cybersecurity threats and strategies in Botswana by conducting a survey with participants from ten sectors. They suggested that organizations in Botswana must prioritize cybersecurity by recruiting talent and implementing multi-layered defense strategies (Sarefo et al., 2023). Also, they suggested the national CIRT has to address potential threats and provide support for less-resourced entities (Sarefo et al., 2023).

At the supply chain front, cybersecurity is becoming an increasingly important topic for organizations at a global

level. Supply chain managers should be attentive when it comes to the cybersecurity threats against their domain of responsibility. In order to achieve cyber-resilience, it is imperative to conduct a thorough evaluation of the susceptibilities present in their technological infrastructure, their vital business assets, the interconnectedness of various components and procedures, and the requisite personnel expertise towards effective supply chain management (Boyes, 2015). A holistic security strategy is needed; solely relying on technical countermeasures may prove insufficient due to the broad spectrum of potential risks and vulnerabilities (Boyes, 2015).

Kabanda et al. (2018) investigated South African small and medium enterprises to comprehend their perception of cybersecurity and the determinants that shape their strategies. The results reveal that the understanding of cybersecurity among small and medium enterprises is restricted by internal organizational factors; budgetary constraints, management support, and prevailing attitudes (Kabanda et al., 2018). The authors identified this as a gap, specifically because both South Africa and Botswana belong in the Southern African Development Community (SADC, 2023), and focused this study on the perceived effect of leadership in combating cybersecurity threats focused on the supply chain within Botswana. The authors chose to follow a holistic approach, and not be restricted to the size or type of organization.

2. Methodology

2.1. Research Design

For this study, the authors chose qualitative phenomenology as the utilized methodology. According to Creswell & Creswell (2018), it is *"a design of inquiry coming from philosophy and psychology in which the researcher describes the lived experiences of individuals about a phenomenon as described by participants"*.

The findings of the study can help organizations in Botswana improve their posture when protecting against supply chain cybersecurity threats. According to Symantec (2016), Botswana ranked as the eight most attacked country in the continent with 3% percentage within African and a count of 37,880.

2.2. Data Gathering

The experience of professionals in Botswana was collected through interviews utilizing the Zoom video conferencing platform. The interviews were semi-structured, allowing the participants to elaborate more freely when they wished. All participating respondents were asked the same set of questions, which included the same central question and thirteen sub-questions. The questions were crafted to allow the respondents to discuss how they felt about the researched phenomenon while also allowing them to provide information for a more holistic picture of the context. The semi-structured approach allowed participants who could not complete the interview successfully due to infrastructure or network connectivity constraints to provide their responses in a future time through a written piece.

2.3. Research Population

The research population was limited to professionals within Botswana. Participants had to be subject matter experts, academics, professionals, or government leaders or officials with jobs related to cybersecurity, Information Technology, logistics, supply chain management, or any appropriate field. Participants had to hold at least a Bachelor's degree, preferably in a field related to the study. A demographic survey was conducted to confirm that interested participants fit the study criteria, and gathered data on gender, age, extended home region, country of residence, highest degree or level of education, years of work

experience, job title, and any relevant certifications. All respondents had to be at least 18 years old or older.

The research population consisted of sixteen professionals satisfying the selection criteria imposed by the authors. There were no benefits for being included, no compensation was offered or provided, and the participation was strictly voluntary. All participants were recruited utilizing the professional social media platform LinkedIn.

3. Results and Discussions

The study explores the lived experiences of IT and Cybersecurity professionals of developing nations with a focus on the African region. This study specifically focuses on the perceived effect of leadership in combating cybersecurity threats against the logistics within Botswana. The study focuses on the supply chain subfield of logistics. The researchers tried to capture the essence of the experience in an appropriate manner as phenomenological tradition dictates. The researchers were compelled to explore the topic due to the COVID-19 pandemic causing an emergence of supply chain cybersecurity threats.

3.1. Pre-Interview Questionnaire

As part of this study, sixteen participants shared their experience to gain deeper insights into the perceived effect of leadership on supply chain cybersecurity. Before participating, a demographic questionnaire was completed (See Table no. 1). The demographic data were confirmed during the beginning of each interview.

Table no. 1

Participant (N#)	Gender	Age	Highest Degree/Level of Education	Years of Work Experience
1	Male	30-45	Ph.D. or higher	10
2	Male	30-45	Master's Degree	6
3	Male	18-30	Bachelor's Degree	3
4	Male	30-45	Ph.D. or higher	7
5	Male	30-45	Bachelor's Degree	6
6	Male	18-30	Bachelor's Degree	5
7	Male	18-30	Bachelor's Degree	5
8	Female	30-45	Bachelor's Degree	5
9	Male	18-30	Bachelor's Degree	2
10	Female	18-30	Bachelor's Degree	2
11	Male	30-45	Master's Degree	15
12	Female	30-45	Master's Degree	11
13	Male	30-45	Bachelor's Degree	21
14	Male	45+	Master's Degree	25
15	Female	18-30	Bachelor's Degree	6
16	Male	30-45	Master's Degree	15

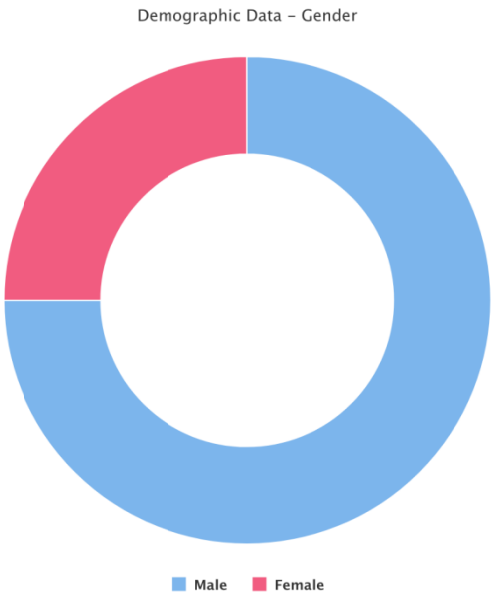


Figure no. 1: *Study Demographic Data – Participants gender ratio*
(Source: Authors, 2023)

The participants included twelve males and four females (See Figure no. 1). Six participants were in the 18-30 age group, nine participants were in the 30-45 age group, and one participant was in the 45+ age group (see Figure no. 2).

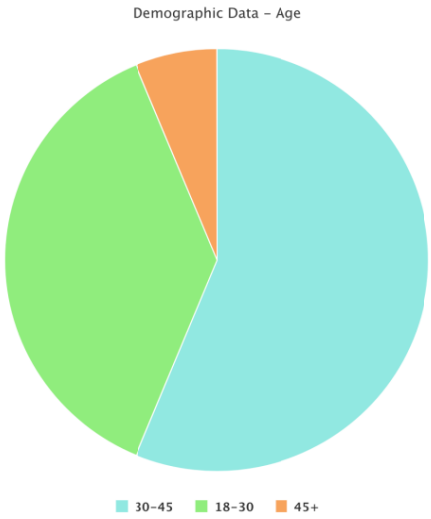


Figure no. 2: *Study Demographic Data – Participants age groups*
(Source: Authors, 2023)

Nine participants had a Bachelor's degree, five participants had a Master's degree, and two participants had a Ph.D. degree or higher (see Figure no. 3). The average years of work experience was nine, with a range of twenty three where the smallest was two and the largest was twenty five. The median of the years of work experience was six.

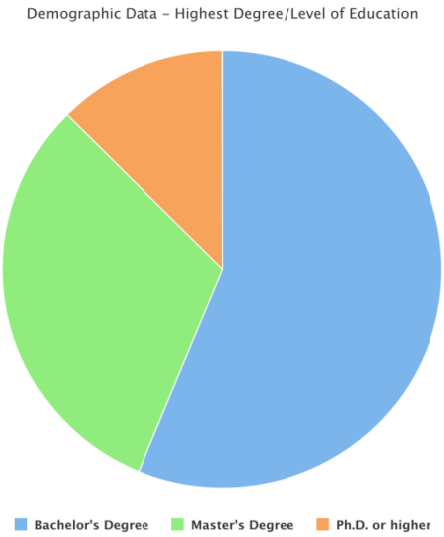


Figure no. 3: *Study Demographic Data – Participants level of education*
(Source: Authors, 2023)

3.2. Research Questions

After diving into the relevant literature and following extensive consultations with subject matter experts, the researchers developed the following questionnaire to investigate the research question. The questions were dynamic in nature. The questions were finalized after further literature was examined and the pilot study phase was conducted. The central question and consequent sub-questions were a result of reviewing relevant literature and feedback during consultations with subject matter experts.

Table no. 2

Central Question
How do cybersecurity professionals describe the effects of leadership on the cybersecurity posture of organizations in regards to threats against logistics with an emphasis on supply chain?

Table no. 3

Sub-Questions	
1	How would you describe cybersecurity as an organizational resource?
2.1	How do you perceive the increasing cybersecurity threats at a local scale?
2.2	How do you perceive the increasing cybersecurity threats at a global scale?
3	What role do you feel management and leadership plays in effective cybersecurity? If you feel it doesn't play a role, please explain why. If it doesn't play a role, what would be the issue?
4	Who do you feel is responsible in an organizational setting for the increasing rate of observed cybersecurity threats?
5	How important do you feel is the protection of supply chain and logistics?
6	What measures would you say could improve cybersecurity in supply chain and logistics?
7	In what ways do you collaborate with your organization's supply chain / logistics team?
8	How would you describe the stance of your organization's management and leadership on the importance of securing against threats on the supply chain and logistics?
9	Who's responsible for logistics and specifically supply chain accountability in your organization?
10	Would you feel that the reliability of the internet has an effect on the security of supply chain? If yes, in what way?
11	Would you feel that the reliability of the electrical grid has an effect on the security of supply chain? If yes, in what way?
12	Would you feel that the reliability of infrastructure in general has an effect on the security of supply chain? If yes, in what way?
13	Is there a government regulation or policy that serves as your guideline? What is the government regulation or policy that you follow?

3.3. Experiencing Cybersecurity Leadership at an Organizational Setting (Questions 1-4)

Participants provided insightful responses when asked how they would describe cybersecurity as an organizational resource. A great majority of the participants recognize cybersecurity as an integral part of their organization. This critical asset was brought to the center stage due to the COVID-19-induced digital transformation. Despite its importance as an organizational resource, it was expressed that cybersecurity is *"severely undervalued"* and still in its early developmental stages. It was also stated by some of the participants that their leadership does not comprehend the importance of cybersecurity. Combined with the small number of certified and skilled professionals, it could be deemed a vulnerability to come. A participant expressed the moving statement, *"As a professional, I fear the day that will be a significant event"*.

At a local scale, when asked about how they perceive the increasing cybersecurity threats, the participants expressed that it is still "uncharted waters" due to the public not understanding it as a concept, not taking it seriously, and living under pretenses that they are safe. A participant expressed that the public can be trusting while navigating cyberspace and fall victim easily. Concern was expressed because of an observed lack of reporting of cyber attacks. Some participants said it is hard to notice cybersecurity incidents within their country due to insufficient information. Some participants expressed their country's honest efforts to make advances but the importance of further capabilities development.

On a global scale, every participant expressed the gravity of the increasing cybersecurity threats. As a participant stated, it is dynamic, and cyberspace is the new battlefield. Despite this being of concern to some participants, they explained that the status of their country as a "developing" one and technological ignorance is alarming regarding cybersecurity threats. A participant felt "scared' after the start of the COVID-19 pandemic due to the increase of attacks in cyberspace.

The role of management and leadership was supported by many participants, as well as the position of authority in effective cybersecurity. Some participants said that their leadership does not prioritize cybersecurity and insist on not allocating sufficient funds. Leadership and management is the group of people that the employees look up to and become an example, according to a participant; everything comes from a top-down perspective, and leadership plays a significant role. On who is responsible in an organizational setting for the increasing rate of observed cybersecurity threats, participant responses included that IT professionals are responsible, and that everybody should play a role regardless of their position. Some participants felt that the IT section or department should be overlooking cybersecurity or, in some cases, the IT Director. Another participant explained that untrained employees are responsible, especially the ones who are not "tech-savvy," including members of their leadership. A participant stated that pining that down to one person is challenging. However, it is a perfect storm of directors, the organization, and the combination.

3.4. Experiencing Supply Chain Cybersecurity as a Practitioner (Questions 5-9)

The vast majority of the participants agreed that supply chain cybersecurity is of great importance, and it is an organizational resource needed to be protected. A participant expressed that it is becoming increasingly important due to everything becoming digital and that cyber espionage will concern organizations.

Some of the measures the research participants suggested for improved cybersecurity in supply chain and logistics included regular audits and service level agreements. Others felt that regulatory requirements would help. A participant indicated that the implementation of processes will contribute towards this goal. Another participant insisted that continuous penetration testing and assessments and establishing an incident response plan and benchmarks will be helpful. An additional suggestion was the application of proper change management. A common thread among different participants' suggestions was training and education and cultivating a culture that promotes that. A participant explained that continuous awareness and training would combat the chances of insider threats.

Most participants described that their organizations have no dedicated supply chain teams. In the case where participants collaborate with a dedicated supply chain team, they provide awareness and educational tips on how to secure the cybersecurity of the supply chain. Other teams were described as interacting due to the legalities of procurement.

Participants were divided on the stance of their organization's management and leadership on the importance of securing against threats to the supply chain and logistics. Some participants explained that their leadership values cybersecurity and that they understand that protecting their customers' data also protects the organization's reputation. In a participant's case, their leadership prioritizes this matter. A participant expressed that even if they discuss this matter with their leadership, they will not take it seriously, and no effect will be observed. Another participant said, "Non existent!" about their organization's management and leadership stance on the matter.

Many participants expressed that they are not aware or unsure about who is responsible in their organizations for logistics and supply chain accountability. In some cases, the procurement or finance department is responsible, including under the leadership of a procurement manager or the Chief Financial Officer. In other cases, the person responsible was explained to be the supply and logistics manager.

3.5. Effect of Internet, Electrical Grid, and Infrastructure Reliability on Supply Chain Cybersecurity (Questions 10-12)

The participants' responses were mixed when they were asked about the effect of the internet, electrical grid, and infrastructure reliability on supply chain cybersecurity. Many of them enthusiastically expressed that the impact of the three factors on supply chain cybersecurity is immense and expressed their concerns about the potential of these attack vectors. The participants shared that the combination of power outages, frail infrastructure, and technological inadequacies is causing a vulnerability in supply chain cybersecurity.

Some participants expressed that normally the country is not in danger due to operations relying on manual processes. A participant used the word "technophobia" as the reason behind the lack of motivation when it comes to shifting to digital systems. COVID-19 was a major driving factor towards digital transformation, as many companies were forced to a teleworking environment; that is when the reliability issues exposed vulnerabilities as they pertained to supply chain cybersecurity, according to some participants.

3.6. Observations and Insight on Policy (Question 13)

The overwhelming majority of participants expressed concern about the insufficiencies of policy at both a national and organizational level. Some participants explained that their organizations rely on internal controls as a source of policy and do not follow a framework from a governmental authority. Despite the presence of national frameworks at the time of the data collection, some participants expressed a lack of awareness on this matter. Some participants shared that their organizations choose to develop their own policies instead of using a well-established or centralized one. A participant stated that the country's cybersecurity regulations are not yet fully adapted and not enforced. Some participants felt that regulations have been politically motivated and not serving the public's interest.

It should be noted that according to the Ministry of Transport and Communications of the Republic of Botswana (n.d.), the following are legislations and policies that are related to cybersecurity issues: Cybercrime and Computer Related Crimes Act No. 22 of 2007; Communications Regulatory Authority Act No. 19 of 2012; Electronic Communications and Transactions Act No. 14 of 2014; Electronic Records (Evidence) Act No. 13 of 2014; and the National Information and Communications Technology Policy commonly called Maitlamo.

4. Recommendations

After conducting the interviews and analyzing the information the respondents shared, the authors intended to compile some recommendations in the study context. Even though maintaining an organization's confidentiality, integrity, and availability against supply chain cybersecurity threats in the context of a developing nation can be challenging due to limited resources, lack of funding, lacking infrastructure, and insufficient awareness, the threats must be addressed.

Organizations should develop a comprehensive cybersecurity strategy that prepares policies, procedures, and technical controls. The cybersecurity strategy should address any identified risk an organization might face and align with standards such as ISO 27001 and NIST Special Publication 8570. In the context of supply chain cybersecurity, organizations should develop a strategy for vendor management that includes risk assessments of vendors and suppliers and policies that vendors and suppliers have to follow to conduct business with the organization.

It should be a priority for organizations to provide employee awareness and education on cybersecurity and further training on supply chain threats. As new threats appear, organizations should update their curriculum, especially when high-profile cases of supply chain breaches happen. That allows employees to learn from discrepancies other organizations failed to address.

Organizations should conduct regular risk assessments to identify potential threats to the supply chain. This includes risks associated with third parties, supplies, and any other external stakeholders interacting within the same supply chain. On the same goal, organizations should develop a robust incident response plan to deal with breaches effectively and conduct regular audits that target supply chain vulnerabilities. Organizations should have a comprehensive disaster recovery and business continuity plan if a supply chain incident disrupts business operations. Organizations should keep their systems up-to-date to avoid cyber threats and invest in technological assets that allow more robust encryption, intrusion detection, and threat intelligence.

Finally, it is recommended that organizations embrace collaboration and information sharing with other organizations in the industry or government to share lessons learned, best practices, and information on supply chain cybersecurity. This can help with preparedness against future threats.

Future research steps

Following the analysis of the study, the authors identified an overlap with the Mission Framework by Dawson (2017). The Mission Framework comprises education, technology, and policy (See Figure no. 4). The authors aim to augment the Mission Framework, and propose a new one specially tailored to supply chain cybersecurity in the context of developing nations. Therefore, further research has to be conducted to design and validate a framework focused on developing nations. To support this plan, the authors intend to produce a comprehensive literature review following the methodology by Webster and Watson (2002).

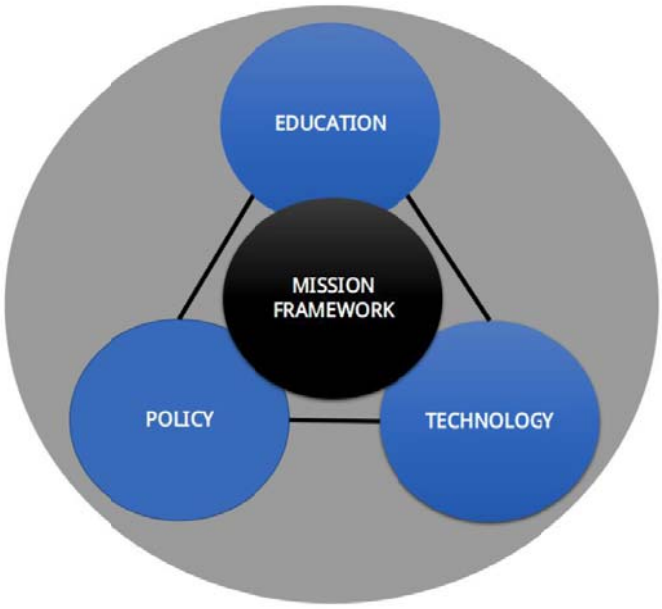


Figure no. 4: *Dawson's Mission Framework*
(Source: Dawson, 2017)

During the early stages of the study, the authors identified the work of Ghadge, Weiß, Caldwell, and Wilding (2019) where a *"supply chain cyber security system"* was proposed as a *"unifying conceptual model"* (see Figure no. 5). The authors aim to utilize the proposed system by Ghadge et al. as a compass while developing a new proposed one focused on supply chain cybersecurity in the context of developing nations.

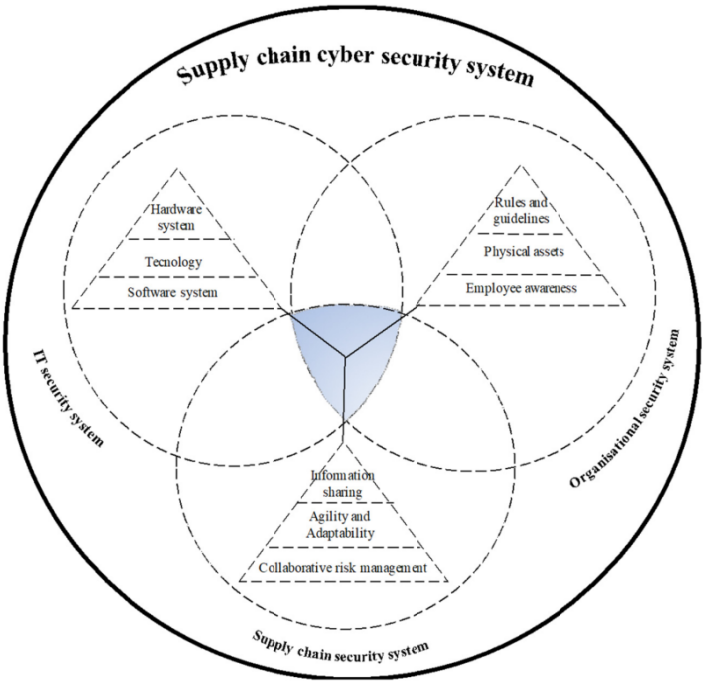


Figure no. 5: *Supply chain cyber security system*
(Source: Ghadge et al., 2019)

The authors intend to continue studies of the same focus with countries of different regions within Africa and countries of other continents. The authors aim to conduct a comparative analysis of the findings of their future studies. The study within this paper was strictly qualitative. However, moving forward, the authors aim to incorporate a hybrid approach and include quantitative data as well.

5. Limitations

The study exhibited certain limitations. First, the study was focused on Botswana, hence the restricted scope to the experiences of professionals living within the geographical boundaries of the country. Second, the research sample size, which contained sixteen participants, is too small to generalize data outcomes. Third, the data collection was limited to the instruments allowed during the COVID-19 pandemic and access to electricity and network connectivity.

6. Reliability & Validity

To assure reliability and validity, the authors chose the following procedures, as described by Katarzyna Peoples and originally by Creswell and Poth (2017). The chosen procedures were peer review and explanation of researcher bias. Peer review was employed by *"meeting with a neutral colleague who asks questions about the methods, results of the study, and any other emerging conclusions in an effort to create accountability and honesty"* (Peoples, 2021). The meetings took place during the

first phases and design of the study and during the conclusion. Explanation of researcher bias was employed by tracking any personal biases during all stages of the research through journaling.

7. Consent

As per the University standards, all participants provided written consent before participating in the study. The written permission was collected and preserved by the authors. The authors comprehensively explained the study details to the participants, and follow-up questions were welcome and answered accordingly. The participants were informed they had the right to withdraw from participating at any time. Also, the participants were informed that they had the right to refuse to answer any questions they might not feel comfortable with. The authors informed the participants that their information, name, or any data that could lead them to be identified would never be used unless their explicit permission is granted. The participants agreed to have their interviews electronically recorded and that only the authors and them could access the video recording. Before finalizing the consent portion of the study, the authors briefly reiterated the conditions to confirm and finalize the participation of the study population.

8. Ethical Approval

All participants provided consent by filling an appropriate form. The form was completed before the interview was conducted. The form was a requirement before participating in the study. No vulnerable people participated in the study. Also, no risks were associated with taking part in the research. The corresponding author received appropriate training on ethics by the Collaborative Institutional Training Initiative (CITI Program) in January 2021, which is valid until February 2026.

9. Conclusion

In this study, professionals were interviewed to explore their experiences and perceptions on the impact of leadership on supply chain cybersecurity in Botswana. The findings highlighted the importance of protecting supply chain cybersecurity and the need for comprehensive strategies to mitigate potential risks. However, the study identified various challenges, including limited resources, insufficient funding, inadequate infrastructure, and lack of awareness. Based on the study's findings, the authors recommended that organizations develop policies, conduct regular risk assessments, provide employee education on cybersecurity and supply chain threats, and keep their systems updated. Additionally, information sharing with other organizations and government entities was suggested to better prepare for future threats. The study had limitations such as a small sample size, a focus on Botswana, and limited data collection instruments due to the COVID-19 pandemic. Future research could focus on developing a new framework to address supply chain cybersecurity in developing nations, with a hybrid approach using quantitative data. Despite the study's limitations, the study provides valuable insights into professionals' experiences and perceptions and practical guidance for organizations to improve their cybersecurity strategies.

Conflict of Interest Statement

The research item does not represent the views of the U.S. Government, Department of State, or any other U.S. Government agency. The views and work presented within this item strictly represent the authors' academic work.

REFERENCES

Bada, M., Solms, B.V., & Agrafiotis, I. (2018). *Reviewing National Cybersecurity Awareness in Africa: An Empirical Study*, 6.

Boyes, H. (2015). Cybersecurity and Cyber-Resilient Supply Chains. *Technology Innovation Management Review*.

Central Intelligence Agency. (2023). Botswana. In *The World Factbook*. Available at: https://www.cia.gov/the-world-factbook/countries/botswana/

Creswell, J.W., & Creswell, J.D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th Edition). SAGE.

Dawson, M. (2017). *Hyper-connectivity: intricacies of national and international cyber securities.* Doctoral thesis, London Metropolitan University.

Ghadge, A., Weiß, M., Caldwell, N.D., & Wilding, R. (2019). Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal*, *Vol. 25, Issue 2*, 223-240. Available at: https://doi.org/10.1108/SCM-10-2018-0357

International Organization for Standardization. (2023). *Iso/iec 27001 standard – information security management systems*. ISO. Available at: https://www.iso.org/standard/27001

INTERPOL. (2020). *Online African organized crime from surface to dark web*.

Joint Task Force. (2020). *Security and privacy controls for information systems and organizations* (NIST Special Publication (SP) 800-53 Rev. 5). National Institute of Standards and Technology. Available at: https://doi.org/10.6028/NIST.SP.800-53r5

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, *Vol. 28, Issue 3,* 269-282. Available at: https://doi.org/10.1080/10919392.2018.1484598

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

Ministry of Transport and Communications. (n.d.). *National Cybersecurity Strategy*. Republic of Botswana.

Peoples, K. (2021). *How to write a phenomenological dissertation: A step-by-step guide*. 1st Edition, SAGE Publications, Inc.

Reva, D. (2020). *Maritime cyber security: Getting Africa ready*. Institute of Security Studies.

Sarefo, S., Dawson, M., & Banyatsang, M. (2023). An exploratory analysis of the cybersecurity threat landscape for Botswana. *Procedia Computer Science, Vol. 219*, 1012-1022. Available at: https://doi.org/10.1016/j.procs.2023.01.379

Southern African Development Community. (2023). Available at: https://www.sadc.int/

Webster, J., & Watson, R.T. (2002). *Analyzing the Past to Prepare for the Future: Writing a Literature Review*. MIS Quarterly (26, 2), xiii-xxiii.