EPiC Series in Computing

Volume 85, 2022, Pages 1–14

Proceedings of 43rd Conference of the South African Institute of Computer Scientists and Information Technologists

EPiC Computing

Towards an African cybersecurity community of practice

Rutendo Chibanda and Salah Kabanda
Information Systems Department
University of Cape Town, Cape Town
chbrut002@myuct.ac.za, salah.kabanda@uct.ac.za

Abstract

In recent years cybersecurity challenges and concerns have become a common theme for discussion by both the government and private sector. These challenges are partly brought on by the continued use of and dependence on information technology, such as the internet, wireless networks and the development and use of smart devices. Additionally, the Covid-19 pandemic has also led to the increase in internet use as it altered the way in which people live and work through forcing businesses and even schools to move to remote working. All these events have made cybersecurity challenges and concerns spiral and more so in Africa where cybercrime continues to rise and be a constant threat. This study proposes a cybersecurity community of practice as a strategy to address African contextual cybersecurity challenges. This qualitative enquiry, based on organizations on the African continent, identifies key characteristics and objectives of an African cybersecurity CoP. These findings provide practical implications for CoP African members and a steppingstone on what to consider prior to implementing an African CoP for addressing cybersecurity challenges and concerns.

Keywords

Cybersecurity Challenges, Cyber threats, and Cybersecurity Community of Practice

1. Introduction

The number of internet users worldwide in 2019, was 3.97 billion up from 3.74 billion in the previous year (Johnson, 2021; Oforji et al., 2017). This increase in internet use could be due to, an ease of access to computers, modernisation of countries around the globe as well as, a rise in the utilisation of smartphones (Johnson, 2021). There are various benefits associated with the increased use of the internet such as, the ability to communicate over geographical locations especially in these difficult times of the Covid-19 pandemic, easier access to information and better storage of vast amounts of data through cloud computing (Schatz et al., 2010). Researchers have associated this increased internet use during the pandemic with lower depression level scores and thus, a better quality of life in middle aged and older people as communication may counter isolation or loneliness (Wallinheimo & Evans, 2021).

However, the increased use of the internet has also led to an increase in cybersecurity challenges as there is the threat of attackers, intruders, spammers, and hackers within these environments (Namasudra et al., 2020). Cybersecurity refers to the protection of internet connected systems from cyberattacks (Srinivas et al., 2019). This increase in cybersecurity challenges is due to, cyber criminals having found an opportunity to compromise the databases and confidential data of both small and large enterprises in developing and developed countries (Tao et al., 2019). In recent years cybersecurity has risen due to the continued use and dependence on computer systems, the internet, wireless networks such as, WIFI or Bluetooth and the development and use of smart devices as a part of the Internet of Things (IoT) (Oforji et al., 2017). Africa has been recorded as one of the regions with the fastest growing cybercrime activities partly due to the vulnerability of the information systems in these contexts which gives rise to the increased number of threats (Kshetri, 2019). Prior studies have documented the challenges associated with cybersecurity in Africa and strategies for addressing them. Yet, cybersecurity concerns remain and are increasing day by day. The persistence and dangerous nature of this problem confirms that researchers and practitioners are yet to understand the cybersecurity landscape and its associated challenges in Africa. This study proposes a cybersecurity community of practice that seeks to address African contextual cybersecurity challenges. A CoP has the potential to create opportunities for leveraging knowledge from key stakeholders such as various government, industry, and academia experts (Wenger, 2011). This knowledge would contribute towards a better understanding of cybersecurity challenges. Thus, this study seeks to address the question: what should be the key characteristics, and objectives, of an African cybersecurity community of practice (CoP)?

2. Related work on Cybersecurity and Community of Practice

Cyber attackers have become more technologically advanced in imposing threats and intrusions to computer systems, networks, or mobile devices as the cyber space is a fast-evolving technological environment (Fischer, 2016). These attacks are voluminous, evolve constantly, have high speed, very sophisticated, and persistent which causes substantial challenges to the preventive security services (Thames & Schaefer, 2017). Some attacks experienced such as, Denial of Service attacks can slow or stop authorised users from gaining access to their systems. In some cases, attackers even take full control of the system leaving organisations crippled (Fischer, 2016). However, despite some organisations implementing cybersecurity strategies, incidents such as cyber-attacks still show a rising trend (Deloitte, 2021). For example, Kenya experienced a spike in cyber threats within the second quarter up until December 2020. A report by the Communications Authority of Kenya stated that cyber threats increased in cost from 35.1 million dollars in the previous quarter to 59.8 million dollars which is a 59.8 % increase in cyber threats. (Telecompaper, 2021). Other cybersecurity challenges affecting African organisations include cyber-attacks such as, hacks (Sawyer & Hancock, 2018), breaches (Mitts & Talley, 2019), ransomware and phishing (Kaspersky, 2021). Nigeria had lost N127 billion annually to cyber-crime attacks (This Day, 2019); and in South Africa, cyber-attacks cost more than R2.2 billion annually. In 2018 there was approximately 75.3% rise in cyber-attacks within the banking sector (The Banking Association South Africa, 2020). These cyber-attacks and threats have become more sophisticated and are thus, capable of causing greater damage as cyber attackers have become more focussed and experienced in issuing their attacks (Smith, 2021). For example, phishing attacks in South Africa have risen by 57% from the time the Covid-19 pandemic began (Smith, 2021). This could be as a result of, more organisations working remotely but with little or no cybersecurity mechanisms in place to fight against such cyber-attacks.

These cybersecurity challenges become more complicated to resolve as the cyber space is a dynamic fast evolving technological environment comprising of a myriad of challenges in the form of costs, SETA, ransomware threats (Mohurle & Patil, 2017), malware (Iliev et al., 2019), cultural and legal components (Fischer, 2016). One of the significant challenges in tackling cybersecurity has been the cost as far more specialised technology and strategies are used to defend modernised businesses more effectively (Milne, 2021). These strategies involve significantly large investments in human and financial resources which allow organisations to conform to the information security procedures (Tatar et al., 2014). Moreover, educating employees within organisations about cybersecurity strategies is also quite expensive as, the activities are hands-on, experiential and the learning follows a guided approach, making it quite labour and time intensive (McGettrick et al., 2014). Another challenge pertains to the security education and training (Razvan et al., 2018) and awareness, which are limited in most African organisations setting. Global Cyber Alliance report (2019) stated that the cost of cyber-crime in Africa increased from approximately half a billion dollars in 2015 to 3 billion dollars in 2019; making it paramount to enhance cybersecurity education and hygiene to mitigate threats in businesses. Yet, such awareness, training and education program as well as strategies for addressing cybersecurity challenges are costly for most developing countries, and Africa in particular. To address these challenges, this study proposes the adoption of an African cyber security Community of Practice (CoP) - a group of people that share passions and concerns for a common idea or something they engage in, and they learn to improve on it through further interactions (Wenger, 2011). A CoP is defined by three characteristics namely, practice (Wenger, 2011) which is the contribution, sharing and exchange of information between the members of a team. Secondly, community (Nobles & Burrell, 2018) which is described as the interactions between members for the purpose of knowledge management and finally, the domain (Wenger, 2011) which addresses the subject to be dealt with in interactions and helps with the integration of members. Some of the key features offered by a community of practice include knowledge preservation and reuse, knowledge transfer mechanism (Huang & Perng, 2017), clear focus (King, 2016), diversity (Pohjola et al., 2016), active learning (King, 2016), and participation commitment. In addition, performance improvements such as, increased core competencies, heightened innovation learning as well as, enhanced work efficiency, and amplified responsiveness can be gained by organisations which operate CoPs both internally and externally (Chu & Khosla, 2009).

Prior studies have shown that a cybersecurity community of practice has been used in developed economies to leverage knowledge from government, industry, and academia experts (Nobles & Burrell, 2018). Pittman and Pike (2016) presented a study were a CoP was adopted in order to support peer learning centered on cybersecurity education amongst high school learners. They advocated for further studies in peer learning and CoP structures to support cybersecurity education. Chen et al. (2017) also discussed how a CoP was adopted by medical students to develop their levels of innovation, leadership skills, knowledge, and peer support. Some researchers have suggested there is some level of difficulty associated with choosing the most appropriate CoP type for a particular business or event as, their characteristics differ according to culture, type of business, structure, and scale of organisation (Hong, 2017). A CoP can be classified into categories, namely informal, sponsored, and strategic CoPs. In an informal CoP, members participate through free will and no one should be forced to engage or participate in various activities (Hong, 2017). Additionally, the members also engage based on a shared common interest but, formal CoPs usually have goals that are closely linked to the organisation's objectives and its purpose. In terms of strategic CoP employees can only gain membership through applications and adherence to CoP rules (Hong, 2017). Although this classification provides a starting point of describing a CoP, this study seeks to identify the type and characteristics of an African cyber security Community of Practice (CoP). Given that contextual challenges in Africa differ from those of developed economies, and the fact that "Africa is a region with one of the highest rates of cybercrime and significant financial losses" (Bada et al., 2019) it becomes imperative to explore and describe a CoP that befits this context.

3. Methodology

A qualitative enquiry approach to the study was adopted. To the best of the researcher's knowledge, they have not found a paper in Africa that addresses the topic of a Cybersecurity Community of Practice, despite Africa being one of the leading regions in terms of Cybersecurity attacks (Bada et al., 2019). The study population comprised of large organisations that have the resources to have cybersecurity strategies in place on the African continent – bearing in mind that such strategies tend to be quite costly (Tatar et al., 2014). The study adopted a purposeful/selective sampling technique, commonly used by qualitative researchers to recruit participants who can provide in-depth information on the phenomenon under investigation (Palinkas et al., 2015). The researcher chose participants from Linked In, and some were selected from various guest lectures that came to speak to the Honours students. Additionally, others were selected through referrals, and some were within the academia industry. Thorough selection process was conducted and only participants that were aware of and experienced in cybersecurity were selected.

Data was collected from seven organisations using qualitative semi-structured interviews. The development of the research instrument was guided by the research question. and cybersecurity and CoP key concepts from literature: Cybersecurity challenges, and the perceptions of a Community of Practice (CoP) for addressing cybersecurity challenges and concerns. The instrument was structured as follows, Section A: Demographic information of respondents and the goal of this section was determine, whether the respondents are an accurate representation of the research sample. Additionally, to elicit information based on organisation background in terms of its establishment, size (based on turnover levels- the higher the turnover the better as such organisations are more likely to afford cybersecurity strategies), industry, and sector classification. Section B was Cybersecurity Challenges because the key research objective was identifying the key characteristics and objectives of an African cybersecurity CoP. In order to do so it was essential for the researcher to ask questions related to the cybersecurity challenges that have been experienced in the organisations, and the corresponding cybersecurity strategies that were implemented to mitigate these challenges. Finally, Section C was Perceptions of a CoP and these aimed to identify whether the interviewees are aware of the existence of CoPs, and their benefits, challenges even the types of Cops as well as, their Critical success factors.

Secondary data was also used to elicit information that could assist in improving the quality of this study. To accomplish this, the researcher attended 1 Organisational Cybersecurity Webinar which was centered on cyber threats and attacks in Sub-Saharan Africa (SSA) and cybersecurity vulnerabilities of people SSA.

This research adopted thematic analysis to identify and analyse various patterns of themes within qualitative data. Firstly, the qualitative interviews were transcribed into text by manually listening to the audio recordings recorded through MS Teams and typing the transcribed data into Microsoft Word. After the data was transcribed, all the sensitive or confidential information provided by the interviewees were replaced with pseudonyms. For example, the interviewees' personal details such as names and their company names were given unique IDs in order to adhere to the ethical considerations of the Ethics Committee. The files were also renamed according to the company pseudonyms and their corresponding participant's ID, for example UNV03_L07 or IT01_L12. This process of transcription of the data was a good way for the researchers to start familiarising themselves with the data. Moreover, according to Bird (2005) transcription is a critical phase which must be done in an interpretive qualitative study. Following the transcription phase, the researcher actively read the transcribed data repeatedly to avoid missing out on any important themes or concepts alluded to in the responses given. Then, the code generation was initialized to identify various features that may be interesting in the data regarding cybersecurity community of practice. The codes generated were colour coded to represent what emerged as cybersecurity challenges, CoP perceptions or any links between the codes were shown as relationships. After having the initial codes, NVivo 12 Pro was then used to assist with the pattern identification.

4. Findings

4.1 Descriptive Findings

The researcher interviewed 12 participants from 7 organisations situated in Africa. The participants where all based in the countries indicated on the demographic table.

The findings showed that most of the respondents were male. There were various organisations that were interviewed which fall within the tertiary education sector. According to respondent UNV03 _L07 "the UNV03 *the institution is very mindful of security and has cybersecurity strategies in place to combat cyber threats and attacks*." The other organisations that were interviewed where within the Transport and Logistics, Accounting, Information Technology, and Health sectors. For example, "*Organization IT 01 was in the Information Technology space and had recently merged with several organisations from Kenya and South Africa. The company employs about 28000 people across 46 countries and makes use of cybersecurity strategies religiously to fight cyber - attacks."* (IT01_L12). Table 1 shows the respondent's profile and experiences in different sectors. For example, respondent IT01_L12 was *"previously a Cybersecurity Engineer and consultant; but currently working as a Practice Lead Manager for Security Services.*"

Organisation	Participant	Gender	Position	Years (#)	Industry/sector	Country
UNV01	UNV01_L01	Male	Senior Technical Specialist	6	Higher Education Institution	South Africa
	UNV01_L02	Male	Professor	21		
	UNV01_L03	Male	Senior Researcher	3		
UNV02	UNV02_L05	Male	Lecturer	13		
UNV03	UNV03_L07	Male	Professor	20		
ACC01	ACC01_L08	Male	Senior Manager	4	Advisory/Consulting	South Africa, Uganda, Algeria, Botswana
TL01	TL01_L09	Female	Chief Executive Officer (CEO)	3	Transport/Logistics	Zimbabwe
	TL01_L10	Male	Junior Manager	3	Transport/Logistics	
PM01	PM01_L11	Female	CEO/Founder	3	Pharmaceutical	
IT01	IT01_L12	Male	Practice Lead Security Manager	10	Financial, Health, Telecommunications, and government.	Kenya, South Africa
TL01	TL01_L13	Male	Manager	5	Transport/Logistics	Zimbabwe
PM01	PM01_L14	Male	Manager	4	Pharmaceutical	
UNV01#SD	Secondary Data				Information Technology	South Africa

Table 1: Demographics of details of respondents

Participant UNV03_L07 holds a top management role and acts as a coordinator for a short program in Cybersecurity at the institution. Participant ACC01_L08 worked with cybersecurity strategies as a top management personnel. His role as a senior manager consultant involves advising clients on cybersecurity measures and *perform audits on cybersecurity controls… and gauge the cybersecurity state to help the clients we are auditing to improve.* Participants from countries such as, Zimbabwe had the least years of experience as compared to those from more developed African countries such as, South Africa where two of the interviewed respondents had more than 20 years of experience. For the more experienced respondents, the 20 years of working with cybersecurity strategies was attained in corporate and 5 years attained in academia as respondent *UNV03_L07* explains*: "I have worked with cybersecurity strategies - From an academic point of view, 5 years. From a corporate point of view 20 years."* Although the findings show that countries that are more developed tend to have more experienced employees; it should be borne in mind that the number of years one is in a particular position does not directly translate into the knowledge or level of experience in cybersecurity.

4.2 Empirical findings

4.2.1 Cybersecurity Awareness, Training and education

Cybersecurity awareness and education was consistently identified as a challenge and according to respondent ACC01_L08, the need for continuous improvement in strategies cannot be understated. The respondent explains that employees lack awareness and if they are aware, they fail to practice security measures and still fall victim to attacks such as phishing. The respondent posits that "*the root cause can be traced back to a lack of understanding of cybersecurity by business leaders as a business risk. They would see Cybersecurity as just an IT risk without realising that it is something that could tear the business to pieces. They lack governance of cybersecurity.* Due to the limited knowledge organisations have on cybersecurity, several cybersecurity practitioners engaged in training and education programs *as a means of educating and helping clients to understand [cybersecurity challenges] so that they are able to make the best decisions when choosing how to secure their systems most effectively."* (IT01_L12). According to some respondents, for training to be effective and acted upon by all members of the organisation, the training was to start at management level. Respondent ACC01_L08 clarifies: "*Yes, how seriously do organisations take security? It starts with leadership and governance".* In addition to training, there was a need for cyber security practitioners to be sensitive to the terminologies used during the training and education programs. For example, it was noted that "*some of the terms used that are related to cybersecurity are not easily understandable to clients*" (IT01_L12)

The lack of awareness, training and education on cybersecurity according IT01_L12 was seen to negatively impact security monitoring processes despite having the tools to avoid security concerns because *"when clients are unaware; they really don't know what they don't know, and they can still be hit by ransomware even when they have the tools to curb this from happening… we conduct training as a means of educating and helping clients to understand so that they are able to make the best decisions when choosing how to secure their systems most effectively*."(IT01_L12). A consistent note from respondents was that most organisation failed to implement comprehensive solutions or tools in place not because they do not have the tools or basic resources, but because cyber security practitioners in these organisations lack awareness and the education to know what solutions to implement. A further concern from most respondents was that "*some clients implemented improper cybersecurity framework which does not match their organisation or is incompatible with the way in which the organisation is run due to lack of awareness and education, and this resulted in various security loopholes*" (ACC01_L08). According to the findings in the secondary data collected from Organisational cybersecurity Webinars which were centred on cyber threats and attacks in Sub-Saharan Africa (SSA), this was problematic and called for: "*The need to build in-house capacity, specifically technical and non-technical indigenous solutions tailored to address contextual challenges. We need solid awareness and training programmes, and this should be a shared responsibility"* (UNV01_SD#1). Respondents saw a CoP not only as a potential strategy that would allow stakeholders to come together and engage in capacity building, sharing of knowledge and awareness creation of cybersecurity challenges in

Africa; but also, as a starting point of addressing silo initiatives that fail to provide context specific solution tackling cybersecurity challenges to the continent (UNV01_SD#1).

4.2.2 Shared Values, Knowledge sharing and trust amongst stakeholders

Some respondents argued that it is important for stakeholders who intend to participate in the CoP to have a shared understanding of cybersecurity and shared values around it. Respondent UNV02_L05 remarked that "*we must have shared values and understanding to help work together more effectively." R*espondent UNV03_L07 stated that "*Having shared values or rather the same mind about cybersecurity helps in its successful implementation*." According to respondent UNV01_L02 "*If a shared understanding exists it will increase the level of the knowledge shared. People can share knowledge that's either tacit or explicit. So, a CoP can work if we are of the same mind. I would say it can work even more effectively in our African context due to the existence of ideologies like Ubuntu given that cybersecurity is now a social problem"* (UNV01_L02). Shared values can be fostered when members have the same knowledge and understanding about cybersecurity. Knowledge sharing was highlighted as crucial aspect of a CoP in Africa due to the minimal cybersecurity awareness, education, and training. According to respondent IT01_L12 *"One bank can be hacked in one way and 3 other banks will be hacked in the same way. But because they don't share* knowledge, *they all suffer the same fate*." According to respondent *UNV01_L01 "the more knowledge that is shared pertaining to cybersecurity the higher the level of cybersecurity education and awareness" (UNV01_L01).* This perception was shared among all participants. The more cybersecurity challenges are treated as a shared responsibility in which cybersecurity knowledge is shared within and across organisations, the easier it would be to address the challenges. However, sharing of knowledge was hampered by a lack of trust Respondent IT01_L12*points that: "It is important to note that this knowledge can only be shared most effectively when trust has been built and the individuals are committed to solving the challenges at hand whilst working as one team."* (IT01_L12). The lack of trust was seen to be triggered by the lack of successful prosecution of cybercriminal activities. Whilst cybersecurity education was important, there was also a need to strengthen how cybercrimes were addressed. According to respondent UNV03_L07:

"*people don't understand cyber-crime; especially the cyber laws in the country; they have not actually seen a successfully prosecuted cyber-criminal in any one of the courts. People have lost confidence in the legal system as there are no concrete actions taken, which makes it feel pointless for some individuals to share their knowledge of cyber related crimes as there is no concrete regard that those who commit cyber-crimes will be 'brought to book*." (UNV03_L07). IT01_L12 stated that: "*In Africa we need to change our policies and governance, so that we can share information. For example: sharing information as countries and having regular meetings were we talk about EDR, and someone explains how that is helping them*." (IT01_L12) Respondent UNV01_L01 agreed and suggested that: "*cybersecurity policies and legislation development should always be seen as an iterative process, the strategies are effective, but they can always be continuously improved*."

4.2.3 Commitment, collaboration and Continuous learning

The findings showed that it is important for all stakeholders participating in a CoP to be committed to the mission of addressing cybersecurity. This commitment was highly linked to how resources such as knowledge are shared in the CoP and how trusting individuals are (UNV01_L01). According to UNV02_L05 "*the sharing of knowledge will allow members to be more committed to solving the problems at hand especially if they trust each other enough to share their intellectual property. Mutual trust and respect are important as it fosters commitment, and this commitment will have a positive influence on the way in which people work as a team*." Whilst commitment to the CoP cybersecurity agenda was perceived as important, there was also a perception that collaboration in African states was key to its success (PM01_L11). Respondents mentioned *that "there is no perfect solution for* *cybersecurity (*UNV01_L02) as the attacks come about in various forms." The respondent noted that "*organisations must develop a culture of continuously improving the strategies in place because strategies can never be 100% fool-proof. There must be a continuous effort, the organisation must work with other institutions to fight against cyber-attacks." (UNV01_L02)*. Respondent ACC01_L08 noted his observation that "*organisations do not have a broad range of cybersecurity strategies in place and when they do, there is a lack of consistency in applying cybersecurity controls which then affects incidence response planning and recovery."* Respondent IT01_L12 explained that these challenges can easily be addressed within a CoP "*where a culture of continuously learn to improve the strategies and thus successfully combat cybersecurity concerns exists"* (IT01_L12).

4.2.4 Identify and understand the threat landscape

Every participant provided the researcher with various cyberattacks experienced within their organisations. Respondent IT01_L12 explained that organisations are not only attacked from external sources, but insiders can attack their own to give cyber attackers access to insert malicious software in the system. *"In some instances, employees were offered a lot of money to install malicious software on the company system. This is dangerous because some employees may be in tough positions and thus, engage in such actions."* (IT01_L12). Respondent ACC01_L08 further explained that insider attacks can also transpire through non-malicious threats. *"There are also non-malicious cyber threats such as, attaching the wrong file and sending to the wrong recipient. These attacks are serious and, in most cases, would occur because the strategies in place can never be 100% fool-proof. Measures can only be effective for now."* (ACC01_L08). Several respondents identified human behaviour as the main threat that exacerbated the challenges of cybersecurity. Respondent UNV01_L02 explained that some employees still refuse to adhere to cybersecurity good practices but prefer to share their passwords with their lovers or save them on unsecure websites which shows that cybersecurity can be identified as a social problem. He explains: "*the solution to cyber-crime cannot be just infrastructure as it is more of a social problem (dealing with human beings). For example, have the people been brought up to speed on cyber related challenges - (that is questionable). We still have people that leave their passwords under the keyboard or save them on their browsers, give passwords to their lovers*" (UNV01_L02). Other respondents identified cybersecurity as more than a technical or social problem but rather as a cultural problem and they advised that in order to solve this problem "*punitive measures such as cybersecurity policies and governance must be put in place and anyone who violates the cybersecurity legislation in place must be apprehended."* (UNV03_L07). These findings were supported by the secondary data from the cybersecurity panel who not only called for *the need to coordinate and collaborate to solve these cyber threats* but *proposed the need to comprehensively identify, document and understand the threat landscape – "we need to know what threats we are facing to solve the cybersecurity challenges" (*UNV01_SD#1). To have a coordinated and shared understanding of the threat landscape, is perceived as key in the development and implementation of a CoP in Africa (ACC01_L08).

4.2.5 Cost

A continuous claim by respondents was that cybersecurity education was expensive and this negatively impacted training and awareness. Apart from the cost of education, implementing cybersecurity strategies was also perceived as expensive (TL01_L09). Respondent TL01_L10 felt that the costs associated with implementing cybersecurity solutions have affected their ability to effectively combine various strategies to manage cybersecurity challenges more robustly. He explains: *"The strategies need to be continuously improved to ensure they can mitigate all the challenges being experienced. I would think combining the strategies we have with other strategies would be helpful. However, the issue of cost has crippled our capacity to do that."* (TL01_L10) "*One potential avenue* *for addressing cost related to cybersecurity was through a CoP were people with knowledge on cybersecurity can share ideas and help educate other employees who may be unaware. You can start in-house then go outside. i.e.: set up short programs where professors and lecturers with sufficient knowledge teach others about cybersecurity"* (UNV03_L07). Some respondents noted that cybersecurity frameworks were too expensive to implement and maintain in order to obtain defence mechanisms to fight against cyber-attacks and were also very time consuming to set up (ACC01_L08).

5. Discussion of the findings

The findings show that an African cybersecurity CoP is characterised by three main structures: the cybersecurity landscape, structures that create shared understanding of cybersecurity in Africa (Kshetri, 2019), and shared values and trust as presented in Figure 1. These structures are not static and each structure influences and is influenced by the other. Starting with the cybersecurity landscape, the findings showed that most respondents were males employed in top management positions of the organisations. Although these findings could be brought upon by sampling limitation, these findings still confirm and reiterate that gender gaps are still prevalent within the Information Technology sector and more specifically in the cybersecurity space (Kamberidou & Pascall, 2019). In the year 2019 women comprised of only 9% of these professionals in Africa (Poster, 2018). Women underrepresentation in the information technology remains a persistent challenge despite the efforts to ensure equal opportunities in legislation and government policies (Reinking & Martin, 2018; Wang & Degol, 2017). One of the reasons for the gender gaps in Africa has been the belief that cybersecurity is a male-dominated and highly specialised field (Peacock & Irons, 2017) and therefore not a suitable fit for women. In addition to providing government intervention of having inclusive policies that target gender gaps, there remains a need for a conscious cultural and society shift in Africa to allow women to venture into male dominated fields and specialisation (Akinola, 2018).

A cybersecurity CoP for Africa was well received by participants who perceived a CoP as a means of addressing the ongoing dynamic challenges of cybersecurity in Africa. They however identified pertinent attributes that the CoP needs to possess and engage in for it to adequately address African contextual cybersecurity challenges. Firstly, there was a need for individual states and private sectors to collectively embark on cybersecurity awareness, training and education programs that serve as a foundation for *understanding what it is, what you don't know and using what you already have, how can you address what you know* (IT01_L12). These findings reiterate prior studies that lack of awareness of threats and risks within the cyber space is a challenge (Bada et al., 2019), which is compounded by the lack of cybersecurity education and training (Security Boulevard, 2021) brought upon by the inadequate infrastructure required to offer cybersecurity training programs in Africa (Barinov & Sharova, 2021; Goussard, 2021; Gregory & Sovacool, 2019) as well as the high levels of computer illiteracy and inadequate regulatory measures against cyber-attacks. Once the cybersecurity landscape has been explored and understood, for example foundation of awareness, training and education on cybersecurity have been implemented, this will serve as a steppingstone for African states to come together and collectively develop and form shared understanding of cybersecurity concerns and strategies that could lead to having shared view and values on how to address cybersecurity challenges. In Africa, prior studies have noted that when a community has shared values and a shared understanding of some phenomenon, those attributes help to uphold the Ubuntu principles of solidarity, cohesiveness, collectivism, and participatory leadership (Kamwangamalu, 1999; Mulaudzi et al., 2009). Practising and upholding these principles, allows members to learn (Barinov & Sharova, 2021; Goussard, 2021; Gregory & Sovacool, 2019). A cybersecurity CoP in Africa that demonstrated Ubuntu principles *which encourages unity and working together to achieve one goal of "I am because we are"* (Kamwangamalu, 1999; Mulaudzi et al., 2009) was perceived as an important step towards the agenda of addressing cybersecurity challenges in Africa. Knowledge sharing and building trust amongst stakeholders was regarded as one of the mechanisms of keeping to the principles of Ubuntu. With shared knowledge, comes shared understanding and in due course shared values (IT01_L12). With shared values, stakeholders can ultimately build trust, a key prerequisite for a successful CoP in Africa (Pohjola et al., 2016). It is therefore imperative that conducive structures for knowledge sharing are made to facilitate the process of trust building in a CoP within the context of Africa where challenges such as culture, and language make it difficult to arrive at a shared understanding (De Barros Jerônimo et al., 2018). Such structures should lead members of a CoP to become committed and allow them to easily collaborate when addressing cybersecurity concerns. A lack of commitment and collaboration could negatively impact knowledge shared, and consequently leading to lack of trust within the CoP (De Barros Jerônimo et al., 2018).

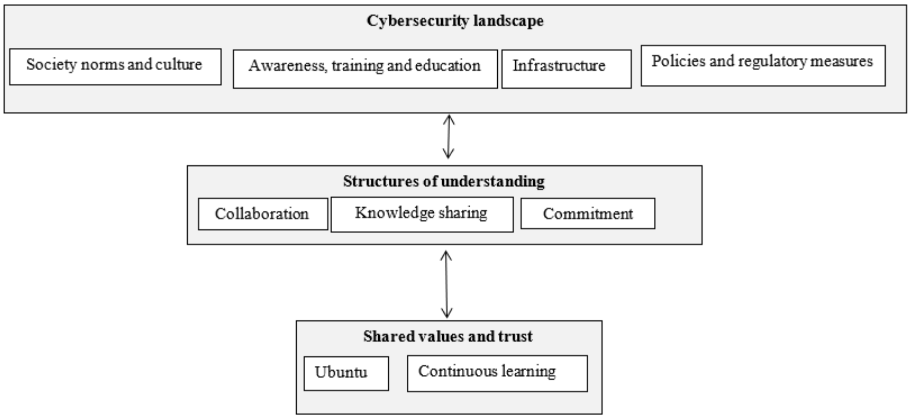

Figure 1: A Cybersecurity CoP for Africa

Findings in this study identified the need for members of a cybersecurity CoP to cultivate a culture of continuous learning and improvement of cybersecurity strategies, given the already existing limited awareness, education, and training programs around the phenomenon. These findings echo prior studies in the field of continuous learning (Shafqat & Masood, 2016; Teoh & Mahmood, 2017). The continuous improvement of cybersecurity strategies would require an ongoing process of identification and understanding of the cyber security threat landscape in Africa where the cyber threat landscape is continuously evolving (Fischer, 2016). There was a continuous call from participants that an African cybersecurity CoP should possess structures that allow cost effective implementation of the proposed strategies and solutions. The findings pointed to costs being high and reflect those of Milne (2021) who stated that organisations that implement cybersecurity strategies face the challenge of using exorbitant amounts of money as, far more specialized technology is used to defend modernized businesses more effectively. This challenge is more prominent in Africa where most organisations do not have sufficient resources to implement cybersecurity strategies (Dlamini & Mbambo, 2019; Leenen et al., 2020).

Based on these findings, and the presentation by Hong (2017), this study advocates for a formal CoP that mirrors the characteristics of both a sponsored and strategic formal CoP. The objectives of the African cybersecurity CoP are to create awareness, education, and training on cybersecurity, establish a culture of continuous learning and develop structures of developing cost-effective solutions for cybersecurity. The CoP objectives further includes the identification and solving of cybersecurity concerns, establishment of collective shared values and the development of structures for knowledge sharing, trust building, commitment and collaboration. The development of the African cybersecurity CoP should be a strategic endeavor and includes members who have a shared goal of addressing cybersecurity challenges. Thus, CoP membership participation is by free will of those interested in addressing cybersecurity concerns; or invited by colleague/cybersecurity expert/practitioner. By doing so, the CoP is not limited to individuals who work or participate in the formal cybersecurity space alone but is open to other stakeholders who are affected by cybersecurity challenges. However, to ensure social inclusion and gender justice as an integral part of the CoP, membership should include targeted identification of individuals that meet transformative agenda of social inclusion, who share the common interest of addressing cybersecurity concerns. As Chiweshe (2019,1) reiterates that without "a concerted effort to undertake socially inclusive processes the Information technology revolution will in many ways fail women, especially in Africa". These efforts should be accompanied by, among other solutions, policy frameworks for social inclusion programmes in cyber security education to train more young women in science, technology, engineering, and mathematics (Chiweshe, 2019). A CoP that follows a public–private partnership (PPP) model is advocated for in this study to ensure that stakeholders such as the government and the industry collaborate and prepare resilient cybersecurity strategies; bearing in mind of course, the critical success factors of implementing a PPP model in developing countries such as those in Africa (Pomerleau & Lowery, 2020). A PPP model would assist in reducing the exorbitant costs, resources and infrastructure challenges associated with cybersecurity in Africa (Barinov & Sharova, 2021; Goussard, 2021; Gregory & Sovacool, 2019; Milne, 2021) and challenges posed by cybersecurity management

6. Conclusion

Africa continuous to experience cyberattacks and is perceived by many as the haven for cyber criminals. Although several strategies are proposed in literature on how to address cybersecurity in Africa, the challenges associated with cyber related crimes remain. This study proposes a formal cybersecurity community of practice as a starting point for Africans to collectively address cyber related challenges. Following a qualitative enquiry approach across the continent with cybersecurity experts and practitioners, the study presents key characteristics and espoused objectives of an effective formal African cybersecurity CoP. Such descriptive findings contribute towards a better understanding on how to implement a formal cybersecurity CoP that seeks to address Africa's cybersecurity challenges and concerns.

References

Akinola, A. O. (2018). Women, Culture and Africa's Land Reform Agenda. *Frontiers in Psychology, 9*(1), 1-3. https://doi.org/https://doi.org/10.3389/fpsyg.2018.02234

Bada, M., von Solms, B., & Agrafiotis, I. (2019). Reviewing National Cybersecurity Awareness in Africa: An Empirical Study. Paper presented at the *The Third International Conference on Cyber-Technologies and Cyber-Systems, CYBER 2018,* 78-83. https://doi.org/10.17863/CAM.40856 https://www.repository.cam.ac.uk/handle/1810/293742

Barinov, A. K., & Sharova, A. Y. (2021). Infrastructure development in Africa (East African Transport). *Asia and Africa Today,* (7), 38-46.

Chiweshe, M. K. (2019). *Fourth Industrial Revolution: What's in it for African Women?* Africa Portal. https://www.africaportal.org/publications/fourth-industrial-revolution-whats-it-african-women/

Chu, M., & Khosla, R. (2009). Index evaluations and business strategies on communities of practice. *Expert Systems with Applications, 36*(2), 1549-1558. https://doi.org/10.1016/j.eswa.2007.11.053

De Barros Jerônimo, T., Coutinho de Melo, Fagner José, Tomaz de Aquino, J., Gonzaga de Albuquerque, André Philippi, & Dumke de Medeiros, D. (2018). Knowledge management alignment to the community of practice in a company of cutting and bending steel. *Brazilian*

Journal of Operations & Production Management, *15*(1), 1-11. https://doi.org/10.14488/BJOPM.2018.v15.n1.a1

Deloitte. (2021). *Impact of COVID-19 on Cybersecurity*. Deloitte. https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

Dlamini, S., & Mbambo, C. (2019). Understanding policing of cyber-crime in South Africa: The phenomena, challenges and effective responses. *Cogent Social Sciences*, *5*(1), 1675404.

Fischer, E. A. (2016). Cybersecurity Issues and Challenges: In Brief. *Congressional Research Service, Senior Specialist in Science and Technology* , 1-9.

Goussard, H. (2021). *Expert Eye: A new way to analyse African Infrastructure | Industry Insights.* Africa Outlook Magazine. https://www.africaoutlookmag.com/industry-insights/article/1094-expert-eye-a-new-way-to-analyse-african-infrastructure

Gregory, J., & Sovacool, B. K. (2019). The financial risks and barriers to electricity infrastructure in Kenya, Tanzania, and Mozambique: A critical and systematic review of the academic literature. *Energy Policy, 125*, 145-153.

Hong, J. (2017). A method for identifying the critical success factors of CoP based on performance evaluation. *Knowledge Management Research & Practice*, *15*(4), 572-593. https://doi.org/10.1057/s41275-017-0066-6

Huang, H., & Perng, Y. (2017). Factors Influencing the Success of Communities of Practice in the Interior Decoration Industry. Paper presented at the Proceedings of the 2017 International Conference on Organizational Innovation,341-345. https://doi.org/10.2991/icoi-17.2017.59

Iliev, A., Kyurkchiev, N., Rahnev, A., & Terzieva, T. (2019). *Some models in the theory of computer viruses propagation*. LAP LAMBERT Academic Publishing.

Johnson, J. (2021). *Global number of internet users 2005-2019.* Statista. https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

Kamberidou, I., & Pascall, N. (2019). The digital skills crisis: engendering technology–empowering women in cyberspace. *European Journal of Social Sciences Studies, 4(6), 1-33.*

Kamwangamalu, N. M. (1999). Ubuntu in South Africa: A sociolinguistic perspective to a pan-African concept. *Critical Arts*, *13*(2), 24-41.

Kaspersky. (2021). *Over half of ransomware victims pay the ransom, but only a quarter see their full data returned.* Kaspersky. https://www.kaspersky.com/about/press-releases/2021_over-half-of-ransomware-victims-pay-the-ransom-but-only-a-quarter-see-their-full-data-returned

King, M. (2016). 6 Key Features of a successful Community of Practice.*37*(6), 1-3.

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

Leenen, L., van Vuuren, J. J., & van Vuuren, A. J. (2020). Cybersecurity and Cybercrime Combatting Culture for African Police Services. Paper presented at the *IFIP International Conference on Human Choice and Computers*, 248-261.

McGettrick, A., Cassel, L., Dark, M., Hawthorne, E., & Impagliazzo, J. (2014). Toward curricular guidelines for cybersecurity. Paper presented at the 81-82. https://doi.org/https://doi.org/10.1145/2538862.2538990

Milne, A. (2021). *The rising cost of cyber security expertise.* Field Effect. https://fieldeffect.com/blog/rising-cost-cyber-security-expertise/

Mitts, J., & Talley, E. (2019). Informed trading and cybersecurity breaches. *Harv.Bus.L.Rev.*, *9*, 1.

Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack. *International Journal of Advanced Research in Computer Science, 8*(5), 1938-1940. https://doi.org/10.26483/ijarcs.v8i5.4021

Mulaudzi, F. M., Libster, M. M., & Phiri, S. (2009). Suggestions for Creating a Welcoming. *International Journal for Human Caring, 13*(2)

Namasudra, S., Devi, D., Kadry, S., Sundarasekar, R., & Shanthini, A. (2020). Towards DNA based data security in the cloud computing environment. *Computer Communications*, *151*, 539-547. https://doi.org/10.1016/j.comcom.2019.12.041

Nobles, C., & Burrell, D. (2018). Using Cybersecurity Communities of Practice (CoP) to Support Small and Medium Businesses. Paper presented at the *ICIE 2018 6th International Conference on Innovation and Entrepreneurship: ICIE 2018*, 333. https://search.proquest.com/docview/2291516634

Oforji, J. C., Udensi, E. J., & Ibegbu, K. C. (2017). Cybersecurity challenges in Nigeria: The way forward. *SosPoly Journal of Science and Agriculture*, *2*, 1-5.

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health, 42*(5), 533-544. https://doi.org/10.1007/s10488-013-0528-y

Peacock, D., & Irons, A. (2017). Gender inequality in cybersecurity: Exploring the gender gap in opportunities and progression. *International Journal of Gender, Science and Technology, 9*(1), 25-44.

Pittman, J. M., & Pike, R. (2016). An Observational Study of Peer Learning for High School Students at a Cybersecurity Camp. *Information Systems Education Journal*, *14*(3), 4. http://isedj.org/2016-14/n3/ISEDJv14n3p4.html

Pohjola, I., Puusa, A., & Iskanius, P. (2016). Antecedents of Successful Collaboration in Community of Practice between Academia and Industry: A Case Study. *Electronic Journal of Knowledge Management : EJKM*, *14*(3) https://search.proquest.com/docview/1816797111

Pomerleau, P., & Lowery, D. L. (2020). *Conclusions and Implications for Practice and Future Studies on Public–Private Partnerships In Countering Cyber Threats to Financial Institutions* . Palgrave Macmillan.

Poster, W. R. (2018). Cybersecurity needs women. *Nature,555(7698)*, 577-580.https://doi.org/10.1038/d41586-018-03327-w

Razvan, B., Dat, T., Cuong, P., Ken-ichi, C., Yasuo, T., & Yoichi, S. (2018). Integrated framework for hands-on cybersecurity training: CyTrONE. *Computers & Security*, *78*, 43-59. http://hdl.handle.net/10119/16450

Reinking, A., & Martin, B. (2018). The gender gap in STEM fields: Theories, movements, and ideas to engage girls in STEM. Journal of New Approaches in Educational Research, 7(2), 148-153. https://eric.ed.gov/?id=EJ1185331

Sawyer, B. D., & Hancock, P. A. (2018). Hacking the human: the prevalence paradox in cybersecurity. *Human Factors*, *60*(5), 597-609.

Schatz, M. C., Salzberg, S. L., & Langmead, B. (2010). Cloud computing and the DNA data race. *Nature Biotechnology; Nat Biotechnol*, *28*(7), 691-693. https://doi.org/10.1038/nbt0710-691

Security Boulevard. (2021). *Navigating Cybersecurity Gaps in Uncertain Times.* Security Boulevard. https://securityboulevard.com/2021/04/navigating-cybersecurity-gaps-in-uncertain-times/

Shafqat, N., & Masood, A. (2016). Comparative analysis of various national cyber security strategies. *International Journal of Computer Science and Information Security*, *14*(1), 129.

Smith, C. (2021, May 1,). Move aside malware, the rising threat is stalkerware. *Fin24* https://www.news24.com/fin24/companies/ict/move-aside-malware-the-rising-threat-is-stalkerware-20210501

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems, 92*, 178-188. https://doi.org/10.1016/j.future.2018.09.063

Tao, H., Bhuiyan, M. Z. A., Rahman, M. A., Wang, G., Wang, T., Ahmed, M. M., & Li, J. (2019). Economic perspective analysis of protecting big data security and privacy. *Future Generation Computer Systems*, *98*, 660-671.

Tatar, Ü, Çalik, O., Çelik, M., & Karabacak, B. (2014). A Comparative Analysis of the National Cyber Security Strategies of Leading Nations . *International Conference on Cyber Warfare and Security. Academic Conferences International Limited, 34*, 211. https://search.proquest.com/docview/1779459625

Telecompaper. (2021). *Kenya registers spike in cyber threats in Q2.* Broadband. https://www.telecompaper.com/news/kenya-registers-spike-in-cyber-threats-in-q2--1378150

Teoh, C. S., & Mahmood, A. K. (2017). National cyber security strategies for digital economy. Paper presented at the *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*, 1-6.

Thames, L., & Schaefer, D. (2017). Cybersecurity for Industry 4.0 and Advanced Manufacturing Environments with Ensemble Intelligence. *Cybersecurity for Industry 4.0. Analysis for Design and Manufacturing* (pp. 243-265). Springer, Cham. https://doi.org/https://doi.org/10.1007/978-3-319-50660-9_10

The Banking Association South Africa. (2020, Jun 23,). Sabric Annual Crime Stats. *Sabric* https://www.banking.org.za/news/sabric-annual-crime-stats-2019/

This Day. (2019, -06-19T03:16:01+00:00). Nigeria Losses About N127bn to Cybercrime Annually. https://www.thisdaylive.com/index.php/2019/06/19/nigeria-losses-about-n127bn-to-cybercrime-annually/

Wallinheimo, A., & Evans, S. L. (2021). *More Frequent Internet Use during the COVID-19 Pandemic Associates with Enhanced Quality of Life and Lower Depression Scores in Middle-Aged and Older Adults*https://doi.org/10.3390/healthcare9040393

Wang, M., & Degol, J. L. (2017). Gender gap in science, technology, engineering, and mathematics (STEM): Current knowledge, implications for practice, policy, and future directions. *Educational Psychology Review*, *29*(1), 119-140.

Wenger, E. (2011). Community of Practice: A brief introduction. Scholars' Bank, 1-7. http://hdl.handle.net/1794/11736