ISSN 2614-0047

Towards academic computer emergency response teams in African developing countries

Leonard Mutembei [a,1,*], Fredrick Ishengoma [b,2]

[a] Institute of Accountancy Arusha, Tanzania
[b] The University of Dodoma, Tanzania
[1] leonardmut31@gmail.com*; [2] ishengomaf@gmail.com
* corresponding author

ARTICLE INFO

Article history
Received August 6, 2021
Revised August 27, 2021
Accepted September 2, 2021

Keywords
Computer emergency response teams
Computer security incident response team
African developing countries

ABSTRACT

The increasing number of cyberattacks on African universities demonstrates the critical need for a more profound shift in perspective from a simple IT problem to the implementation of more resilient security measures and policies, and thus, Computer Emergency Response Teams (CERTs). Fortunately, even though there are numerous CERTs worldwide, there are relatively few studies in the literature that address academic-CERT in the African context. This article summarizes the CERT landscape in African countries and proposes a framework for academic-CERT. The proposed framework aims to fortify African academic institutions' resilient security measures. The paper will serve as a foundation for developing academic CERTs in African countries, which will eventually result in the implementation of national CERTs and the protection of online users.

1. Introduction

According to the International Telecommunication Union (ITU) (2019), the number of Internet users has continued to grow from 2005 to 2019, reaching approximately 4.1 billion users in 2019. Technological advancements bring an increasing number of security threats, such as cyber-attacks [1]. Cyber-attacks are increasing year after year as criminals advance their technologies and methods. A case in point is the ransomware attacks, which continue to target organizations, businesses, universities, and public administrations worldwide.

Universities are the primary generators of innovation in countries and the economy as a whole. Recent studies indicate that universities and research institutions have risen to prominence as new targets for cyber-attacks [2]. This is because universities are hubs for research, innovation, and solutions to global problems. For instance, the race to develop a COVID-19 vaccine has shifted cyber-attacks to universities seeking research data and information [3]. Meanwhile, university-wide standards generally do not favor resilient security measures, owing to the high volume of students and staff accessing the network, device sharing, the dynamic nature of enrollment and graduation, and the Bring Your Own Device (BYOD) practice [4]. Universities' position as knowledge generators and disseminators outweighs the importance of information security in research, development, processing, access, and sharing [5].

Perhaps it is unsurprising that universities are targeted by cybercriminals, given the volume of research data, personal, economic, and scientific data stored by these institutions. Hackers have spent the last decade researching network vulnerabilities in universities and research institutions [6]. Theft, manipulation, or disruption of research data has a detrimental effect on the research community, intellectual property, nation, and economy. Examples of attacks include using brute force on the networks of research facilities, which involves rapidly attempting millions of login and password combinations [7].

Cybercriminals have targeted African universities as a result of lenient security protocols. With Africa's universities lagging in terms of ICT and infrastructure development (in comparison to western universities), the need for academic Computer Emergency Response Teams (CERT) is critical [8]. Academic-CERT would respond to security incidents, conduct vulnerability analysis, and develop incident management skills in an academic setting.

In light of the preceding, this paper proposes an academic-CERT framework for African universities. The following is the structure of this paper: Section 2 contains a review of the literature on CERT. Section 3 discusses the state of academic CERT in African universities and the need for it. Section 3 details the study's methodology. Section 4 summarized the findings of the study, and Section 5 concludes this paper.

2. Literature Review

2.1. Computer Emergency Response Team (CERT)

CERT –Computer Emergency Response Team Coordination Center (CERT/CC) is associated with the emergency of worms within computers. November 1988, Morris worm was released by a student and affected computers on the Internet which led to the formation of the first CERT at the University of Carnegie Mellon [9]. Other names used to refer CERT/CC are Computer Emergency Response Team (CERT), Computer Security Incident Response Team (CSIRT), Cyber Incident Response Teams (CIRTs) and Cyber Security Incident Response Teams (CSIRTs). However, the researcher uses the term Computer Emergency Response Team (CERT) to refer to any emergency team in this study. CERT collaborates with information security experts who collaborate on planning, detecting, monitoring, and responding to cyberattacks [10]. CERT's mission is to respond to security incidents involving computers and information systems as they occur. The team is required in various settings, including government agencies, private businesses, the military, large and small businesses, and academia. In this study, our focus would be on academic settings.

Numerous studies have been conducted to demonstrate how to establish CERTs in various industries. Wara and Signh [11], conducted a study that shows how to set a CERT within a research and education network. Their guidelines apply to the formation of a security team within the academic community. While difficulties may arise during the formation of CERTs, teams should not surrender but should persevere to the end. Grobler and Bryk [10], conducted a study to determine the number of difficulties encountered when establishing a CERT within a nation. The same issues can arise during the formation of academic CERTs. Numerous ideas can be incorporated into their research to assist academic institutions in establishing CERTs.

The formation of CERTs is contingent upon member trust in order to function effectively. Kruidhof's study [12], demonstrates that trust in people is more critical for the CERT to carry out its functions. Additionally, due to advancements in technology and cybersecurity, the researcher suggests that CERTs are a necessity in our countries for resolving cyber-attacks both internally and collaboratively. He concluded that trust must exist between individuals and organizations to foster a culture of information sharing. Thus, effective collaboration is contingent upon CERTs developing trust in one another. The importance of CERTs worldwide cooperating and sharing information in order to resolve cyber problems. The researchers demonstrate how well-established CERTs can raise cybersecurity awareness among team members and thus be more effective at defending against cyberattacks. The CERT team contributes to network security by providing alerts and solutions to problems. In May 2017, a report revealed that approximately 100 countries worldwide had been impacted by a cyber-attack known as ransomware (The Guardian, 2017). Academic institutions conducted studies and made recommendations to their communities on how to avoid such attacks; a good example comes from Norway's University of Oslo (2017). The formation of CERTs is contingent upon member trust in order to function effectively. Then, the trust in people is more critical for the CERT to carry out its functions. Additionally, due to advancements in technology and cybersecurity, the researcher suggests that CERTs are a necessity in our countries for resolving cyber-attacks both internally and collaboratively. He concluded that trust must exist between individuals and organizations in order to foster a culture of information sharing. Thus, effective collaboration is contingent upon CERTs developing trust in one another. The importance of CERTs worldwide cooperating and sharing information in order to resolve cyber problems.

2.2. CERT in Africa vs World

Worldwide, international organizations contribute to the development of standards and certify nationals and their constituencies as CERTs based on agreed-upon criteria. Additionally, they collaborate with nations to establish CERTs and assist in maintaining databases of available CERTs for researchers to study and recommend appropriately. Africa has its own entity, the Forum of Computer Security Incident Response Teams (AfricaCERT), which facilitates capacity building, awareness, coordination, and information sharing among member states. 22 African member states have CERTs, according to (AfricaCERT 2020). Several CERTs exist in African developing countries, including EG-CERT in Egypt, ghCERT in Ghana, CSIRT in Kenya, ECS-CSIRT in South Africa, and TZ-CERT in Tanzania (Tanzania).

However, additional work must be done to ensure that at least half of Africa's nations have CERTs and encourage other sectors, such as academia, to establish their own. This will strengthen regional cybersecurity and also aid international organizations in combating cyber-attacks. According to the Forum of Incident Response and Security Teams' (FIRST) annual report, there will be over 530 CERT member teams by July 2020. They classified members according to their geographical origins. The researcher searched the FIRST website and discovered 535 CERT members who met the criteria for grouping them into six regions. Fig. 1 depicts CERTs members in FIRST, indicating that Africa is still lagging other regions worldwide.

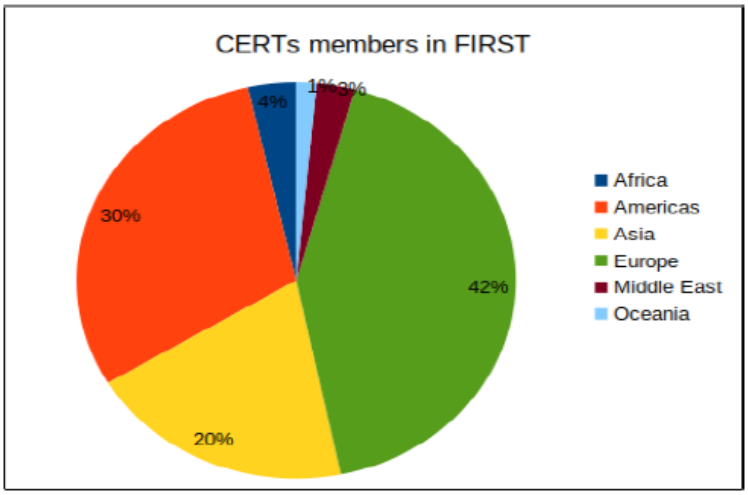

Fig. 1.CERTS members in FIRST

According to international organizations, Africa is still lagging behind other continents in terms of CERT establishment. When deciding to research a particular area, academia can play an essential role in stimulating the formation of CERTs.

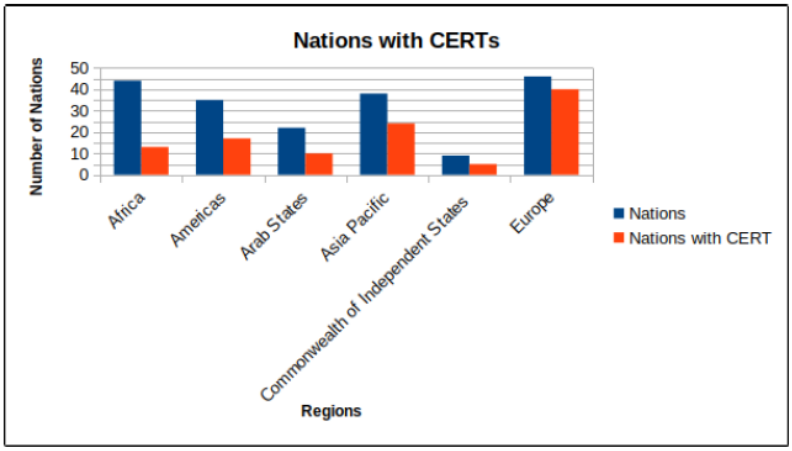

Fig. 2. Nations with CERTS

2.3. The Need for Academic CERT in Africa

At the most fundamental level, cyber threats faced by African universities are broadly similar to those faced by universities in other parts of the world. However, contextual factors distinguishes African universities from the rest of the world. Contextual factors include poor ICT infrastructure such as inadequate access to the Internet with the high cost and low bandwidth, frequent power failures and outages, a lack of adequate maintenance and routine patching, a shortage of skilled staff, natural causes (such as natural disasters), political, cultural, and social factors. Academic institutions frequently use out-of-date or unpatched software, which makes them particularly vulnerable. For example, computers running software that the development teams no longer support (no longer receiving security updates).

While Africa offers numerous opportunities, it also faces countless cyber challenges in academia. Numerous university students and faculty members use hardware and networks that are incapable of running current software, posing a security risk to their systems. Additionally, some pirated software is used, posing significant security risks due to the likelihood that it will not be updated to address vulnerabilities. Further, some academic institutions do not publicly disclose security breaches. This complicates determining the scope of attacks on universities in Africa and developing solutions. As a result, a trustworthy environment (academic CERT) should be established to benefit everyone (including developers and end-users) from cyber-attacks.

While several cybersecurity solutions developed outside of Africa may be applicable to African universities, Africa does have some unique characteristics. Except for a few developing nations, most African countries are distinct from the rest of the world in the following ways: 1) Professional human resources are scarce in the field of cybersecurity. 2) Universities have limited resources to devote to cybersecurity (including funds, sophisticated software, and hardware equipment). 3) Africa's universities lack adequate infrastructure (poor Internet connection, regular power cuts etc.). 4) There is a lack of understanding among key stakeholders regarding cybersecurity issues. 5) A deficiency of awareness of the dangers inherent in the use of ICTs.

Despite these constraints, African universities host a significant amount of research and innovation. University ecosystems are prosperous "breeding grounds" for IT experimentation and research, attracting the attention of hackers from both within and outside the university community. However, the security of information systems is frequently not a well-organized or transparent process in African universities, mainly where IT services are decentralized. As a result, computer networks in African universities are insufficiently secured, frequently leaving them vulnerable to manipulation and targeted attacks by malicious code. Additionally, infected computers could be remotely used to launch coordinated attacks and engage in various other malicious activities on different networks throughout the world.

A security breach could result in data loss, lost time, and diminished credibility for the institution, its students, faculty, and the entire country. While student identification numbers are not as valuable as they once were in African universities, other potential targets include the accounting and finance department, research data, student, human resources, and payroll processing departments, as well as any hosted computer systems or services. Universities in Africa, regardless of country, face a cybersecurity threat. Academic institutions must establish academic CERTs to prepare for and monitor cyber-attacks on their networks. Higher education institutions must employ best security practices to safeguard data and educate students and staff about cybersecurity issues. Thus, African universities must develop and implement academic CERT in light of the preceding arguments.

3. Proposed Academic CERT Framework

This section proposes an academic CERT framework for African developing countries, using a top-down approach as illustrated in Fig. 3. The proposed framework is divided into five clusters, which include the Academic CERT Board, Academic CERT managers, Academic CERT technical team, Academic CERT operational team, and Academic CERT users. This way, all levels of IT authority report issues to their assigned boss. For example, if a user discovers a virus on his or her computer, he or she must immediately contact the academic CERT operational team, which will handle the situation appropriately. In exchange, the academic CERT operational team will report all information security incidents to a higher management level, specifically to the academic CERT managers.

This method pre-arranges and implements information security responsibilities according to authority levels. For example, the Board of Directors must approve the information security policy, whereas managers are accountable for the institution's information security policy. Additionally, it is self-evident that all levels of information technology authority should be proactive in implementing the organization's information security policy.

The academic CERT Manager is responsible for ensuring that all information security policies and practices adopted by the board are adhered to rigorously and correctly by those who fall under their jurisdiction. Academic CERT managers are also responsible for defining the technical team's roles and responsibilities. They are accountable to the academic CERT committee.

The academic CERT technical team is responsible for effectively managing technical security issues on the university network. This ensures that the University's information is completely secure at all times. Individuals working at this level of information technology should have extensive knowledge of information security and significant professional experience. This expertise is frequently acquired through academic training such as tertiary degrees/diplomas or industry-specific information security certifications such as the Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), and Offensive Security Certified Professional (OSCP) (OSCP).

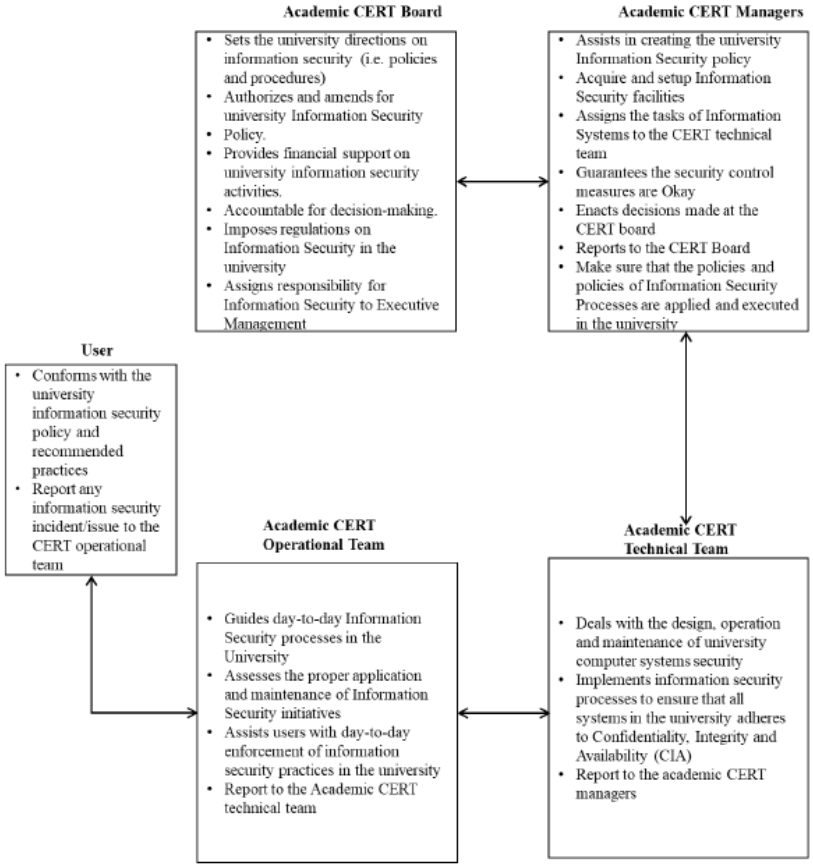

Fig. 3. Proposed academic CERT framework for African developing countries

Academic CERT's operational team is dedicated to taking all necessary precautions. Additionally, the team is committed to ensuring that all university information security policies and procedures are followed. For example, the team can ensure that routine information security procedures, such as applying software security patches and updating computer antivirus, are carried out correctly. The academic CERT technical team reports directly to this team.

The term "users" refers to all University's computer network users and computer systems (students, staff, and professors). Users should be informed of all university policies and guidelines governing the security of university data and computer systems. With numerous sophisticated malicious techniques being developed daily, awareness campaigns for information security are critical at this stage. Hence, this approach taken by the proposed framework ensures that all information security

circumstances and events are communicated to the board, which has the authority to adjust information security policies and practices as necessary.

4. Proposed Practices towards Enhancing Academic CERT

We propose several practices in this subsection that should be enforced under academic CERT in order to improve security in African academic institutions. The first is limiting the number of sessions. By limiting students to a single valid Windows session and requiring them to use only one valid Windows connection at a time, significant security vulnerabilities can be avoided. This prevents fraudulent users from using the login credentials concurrently with the legitimate owner.

The second is enforce accountability. Attempting to prevent multiple logins frequently leaves authorized users liable for any unauthorized action they take, whether it's a data breach, virus distribution, phishing, or more severe hacker attacks. It ensures that access to an institution's critical assets is delegated to a single individual, minimizing threat situations. To address any violations that occur, rules and regulations should then be adhered to systematically.

Then, enforcing different level of access according to users. The University's network security should be addressed differently depending on the user type, i.e. faculty, staff, or students so that the level of access granted is appropriate for each individual's position within the University. Visiting scholars, professors, and staff should also be addressed separately to ensure that their access is withdrawn upon their departure. The first line of defense for a Windows network is the control of user accounts according to user type, target audience, and organizational structure, with login privileges granted according to the user's position within the University. Consideration should also be given to requirements such as workspace or computer (including personal devices), duration, work schedules, and session format (as well as wireless access). For example, a student who obtains a professor's credentials can access sensitive information from any computer connected to the university network (examination questions, assignments, grades, etc.). UserLock can prevent account abuse by allowing the administrator to specify which computers a user may or may not access (via IP range). Thus, a student will not access the system via a professor's authentication and the network's free-access computers.

And the last is BYOD security policy. BYOD security protocols must be implemented because bring your own device (BYOD) practices expose the university's network to security threats [13]–[15]. To mitigate the risks associated with the inability to retain a BYOD device, the university's security protocol should enforce the Mobile Device Management (MDM) security approach and remote wipe services. University staff and students can use this software to monitor a missing computer and have the computer's data deleted as of a last resort. All university users should back up their data regularly. By implementing backup and restore procedures, the effects of a missing or stolen computer can be significantly mitigated.

5. Conclusion

Due to increased technological sophistication and reliance on the Internet, African universities face a slew of new cyber threats. Cyberattacks, like those carried out in other parts of the world, are becoming increasingly sophisticated. African universities' latest research and financial opportunities are attracting an increasing number of attackers with various motives. Their influence has grown beyond the confines of individual universities to encompass national security concerns. Africa developing countries are particularly vulnerable due to a lack of knowledge about information security, financial constraints, stakeholders' willingness to combat cybercrime, and a scarcity of cybersecurity expertise. Regrettably, African universities will continue to face difficulties protecting their networks from cyber-attacks.

This paper aims to highlight the importance of academic CERTs in universities of African developing countries and propose a framework for their implementation. The proposed academic CERT framework is structured to assist security professionals in advancing universities' information security programs in African universities.

Capacity building and information exchange are critical components of cybersecurity in African universities. Universities must have access to cutting-edge software and hardware to assist in ensuring

cybersecurity. This includes current and actionable information on vulnerabilities and security strategies and guidance on how to implement them. To accomplish this goal, the academic-CERT should initiate capacity-building initiatives. These initiatives will introduce cutting-edge technologies, techniques, and activities to universities through awareness-raising activities. Meetings, training sessions, and seminars may all be incorporated into the program.

Academic CERTs in Africa should promote the use of Internet exchange points (IXPs) and information sharing and connectivity. IXPs can help to mitigate cyberattacks. Reduced traffic loads on international connections complicate DDoS attacks on those services and infrastructure. Local traffic passing through an IXP is unaffected if a foreign connection is disabled due to an attack. Internet exchange points, or IXPs, are a subset of Internet exchange points. African academic CERTs can motivate academic actors to develop a cybersecurity culture through knowledge exchange, promoting guiding principles, and setting an example.

References

[1] I. Agrafiotis, J. R. C. Nurse, M. Goldsmith, S. Creese, and D. Upton, "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate," *J. Cybersecurity*, vol. 4, no. 1, Jan. 2018, doi: 10.1093/cybsec/tyy006.

[2] J. Chapman, A. Chinnaswamy, and A. Garcia-Perez, "The severity of cyber attacks on education and research institutions: a function of their security posture," 2018.

[3] J. Wiggen, *The impact of COVID-19 on cyber crime and state-sponsored cyber activities*. Konrad Adenauer Stiftung, 2020.

[4] H. V. Nguyen, "Cybersecurity Strategies for Universities with Bring Your Own Device Programs," Walden University, 2019.

[5] H. Van Thai and M. A. L. T. K. Anh, "The 4.0 Industrial Revolution Affecting Higher Education Organizations' Operation in Vietnam," *Int. J. Manag. Technol.*, vol. 4, no. 2, pp. 1–12, 2017.

[6] L. Coleman and B. M. Purcell, "Data breaches in higher education," *J. Bus. Cases Appl.*, vol. 15, no. 15, pp. 1–7, 2015.

[7] S. Coughlan, "Hackers beat university cyber-defences in two hours," *BBC News family and education correspondent*, 2019. https://www.bbc.com/news/education-47805451 (accessed Feb. 21, 2021).

[8] Internet Society, "Internet Infrastructure Security Guidelines for Africa: A joint initiative of the Internet Society and the Commission of the African Union," 2017. https://www.internetsociety.org/resources/doc/2017/internet-infrastructure-security-guidelines-for-africa/ (accessed Mar. 20, 2021).

[9] G. Killcrece, K. P. Kossakowski, R. Ruefle, and M. Zajicek, "State of the practice of computer security incident response teams (CSIRTs)," 2003.

[10] M. Grobler and H. Bryk, "Common challenges faced during the establishment of a CSIRT," in *2010 Information Security for South Africa*, Aug. 2010, pp. 1–6, doi: 10.1109/ISSA.2010.5588307.

[11] Y. M. Wara and D. Singh, "A guide to establishing computer security incident response team (CSIRT) for national research and education network (NREN)," *African J. Comput. ICT*, vol. 8, no. 2, pp. 1–8, 2015.

[12] O. Kruidhof, "Evolution of National and Corporate CERTs-Trust, the Key Factor," in *Best Practices in Computer Network Defense: Incident Detection and Response*, M. E. Hathaway, Ed. IOS Press, 2014.

[13] M. Olalere, M. T. Abdullah, R. Mahmod, and A. Abdullah, "A Review of Bring Your Own Device on Security Issues," *SAGE Open*, vol. 5, no. 2, p. 215824401558037, Apr. 2015, doi: 10.1177/2158244015580372.

[14] G. Disterer and C. Kleiner, "BYOD Bring Your Own Device," *Procedia Technol.*, vol. 9, pp. 43–53, 2013, doi: 10.1016/j.protcy.2013.12.005.

[15] B. Morrow, "BYOD security challenges: control and protect your most sensitive data," *Netw. Secur.*, vol. 2012, no. 12, pp. 5–8, Dec. 2012, doi: 10.1016/S1353-4858(12)70111-3.