

A Guide to Establishing Computer Security Incident Response Team (CSIRT) For National Research and Education Network (NREN)

Y.M. Wara

Directorate of Information and Communication Technology
Usmanu Danfodiyo University
Sokoto Nigeria
E-mail: mywarra@udusok.edu.ng

D. Singh.

Faculty of Information Science and Technology
Universiti Kebangsaan
Malaysia
E-mail: dalbir@ukm.edu.my

ABSTRACT

Academic institutions worldwide embrace communication network and Internet services for their academic activities and collaboration. Communication network enable members of institutions to collaborate with each other and as well access Internet. Therefore, sophisticated cyber-attack emanating from one segment of the network or from the greater Internet can undoubtedly trigger crisis that can affect various stakeholders both within and outside the academic institutions. Consequently, a coordinated concerted effort is required for a more protected network and safe internet. This joint effort is mostly referred to as CERT (Computer Emergency Response Team) or CSIRT (Computer Security Incident Response Team). This paper provides the guides on establishing Computer Security Incident Response Teams (CSIRTs) for securing the National Research and Education Network (NREN) in Nigeria. Focused synthesis method using published articles and archival data has been collected and analysed in this study. Finally, the proposed guide would improve the management of cyber security issues in NREN.

Keyword: CSIRT; Nigeria; Network; Security; Research

African Journal of Computing & ICT Reference Format:

Y.M. Wara & D. Singh J. Isabona & M. Ekpenyong (2015). A Guide to Establishing Computer Security Incident Response Team (CSIRT) For National Research and Education Network (NREN). Afr J. of Comp & ICTs. Vol 8, No. 2. Pp1-8.

I. INTRODUCTION

The advents of communication network and Internet services have turned the world in to a virtual environment or even a global village. Virtual world connects organization's critical infrastructure to both public and private sectors and as well as academic institutions. A sophisticated cyber-attack can undoubtedly trigger crisis that affect various stakeholders both within and outside the organization. Consequently, numerous communities started to cooperate for a more protected and safe internet. These joint efforts are mostly referred to as CERT (Computer Emergency Response Team) or CSIRT (Computer Security Incident Response Team).

A CERT or CSIRT is an organization of devoted and responsible cyber security experts that plans and responds to cyber security incidents. The organization is responsible for taking, studying, organizing and responding to cyber security incidents and activities [1]. This is very critical since communication networks and information systems have turned out to be crucial element in academics, economics and other social services and development. Therefore, the safety and security of these systems is of high concern to the organization.

To this end, it is imperative for developing National Research and Education networks in Nigeria and the Africa in general to implement superior cyber security mitigation and practices that can efficiently respond to the ever growing information systems attacks through developing plans and supporting resources. One kind of this plans is to have an organize Cyber Security Incident Response Team (CSIRT).

The purpose of this article is to review the steps on establishing Computer Security Incident Response Teams (CSIRTs) for securing the National Research and Education Network (NREN) [2].

This article comprises of four sections, whereby section one explains the concept of NRENs, section two focuses on cyber security incidents, section three reviews on attributes of the CSIRT and section four explains on the application of CSIRT framework in a typical developing NRENs. The contribution of this paper is to guide the development of NRENs in Nigeria and Africa in general to implement a Cyber security incident handling and response team by adopting the guidelines stated herein.

2. NATIONAL RESEARCH AND EDUCATION NETWORK (NREN)

Over the years Research and Education Network (REN) have matured significantly in various countries as a sustainable solution for ICT needs of Higher Education Institutions (HEI). A REN organization generally owns and administers a high performance national backbone network interconnecting all member campuses. National Research and Education Network (NREN) is the interconnection of researched and teaching focused institutions that centred on making use of scarce resources to offer solutions for the purpose of realizing their set organizational goals [3].

Having the need for seamless interconnectivity and interoperability within any network does not warrant compromising security within the Network. There are different levels of security for each user set. For every network on which the national information infrastructure is built must have series of security policies and procedures implemented that will enforce authorized access to the network and any system within it [3]. Networks and its related systems services are considered critical in supporting dispersed research organizations around the globe [3]. In this regard, academic network in African countries can utilize the advancement of these network services to get connected to other NREN around the world for improve academic services.

3. COMMUNICATION NETWORK AND NREN TECHNOLOGIES

It is of high important to perceive that even in the present day, Internet has been feasible to have a perfect combination of enterprise, academics, government and military systems. For sure, the more such diverse organizations continue to connect to the Internet, the more on the increasing opportunity of these intermediate level network systems to have a number of unrestricted clients [3]. Presently, the Internet is properly serving the public but widely vulnerable to mass attacks. This is because Internet is a public network with a wide access to a very large variety of users. It is imperative to know that, as time goes on; many institutional users will support local area networks and will use this network to have access to NREN and as well the Internet. According to [3] there are presently some NRENs that provide research network platform, contents sharing among member institutions and as well provide Internet services without necessarily providing cyber security incident response capability.

These networks include South African National Research Network (SANReN), whereby it was meant to provide Internet services and global research network to south Africa; TENET (Tertiary Education and Research Network of South Africa), is a platform that provides Internet and ICT services to higher educational institutions in south Africa; The Ghanaian Academic and Research (GARNET), is supporting the research and education communities within Ghana promoting academic collaboration; Research and Education Network for Uganda (RENU) is fostering and nurturing teaching, learning and content development in Uganda. West and Central African Research and Education Network (WACREN) is responsible for giving the necessary support for the creation and sustenance of NRENs in the region.

NgREN (Nigeria Research and Education Network) was designed to provide a platform for all higher education institutions in the country to communicate, collaborate and share resources using ICT to promote research and education in the Nigeria. Despite desires and importance of these networks security issues should not be compromised or taken for granted. Different NRENs require different levels of security but there must be a common organized cyber security incident handling procedure and response to mitigate cyber security issues within and the outside NREN.

4. NIGERIA RESEARCH AND EDUCATION NETWORK (NgREN)

Nigeria Research and Education Network (NgREN) like any other NREN was designed to provide a platform for all higher education institutions in the country to communicate, collaborate and share resources using ICT to promote research and education in the Nigeria. Presently, the network has connected all the 27 Federal Universities, National Universities Commission (NUC) and the Committee of Vice-Chancellors' secretariat to a 10gbps core network and a 155mbps last-mile capacity to each University. A 3*STM-1 bandwidth capacity was also provided as a proof of concept.

Each University has a set of Video Conferencing facilities installed. In addition, several efforts are being put in place to connect the remaining Universities, Polytechnics and Colleges of Education and also to promote inter institutional collaboration on the network. NgREN provides connectivity between Nigerian institutions as well as connectivity with other global Research and Education Networks as shown in Figure 1. It is viewed holistically, as a network of educational networks.

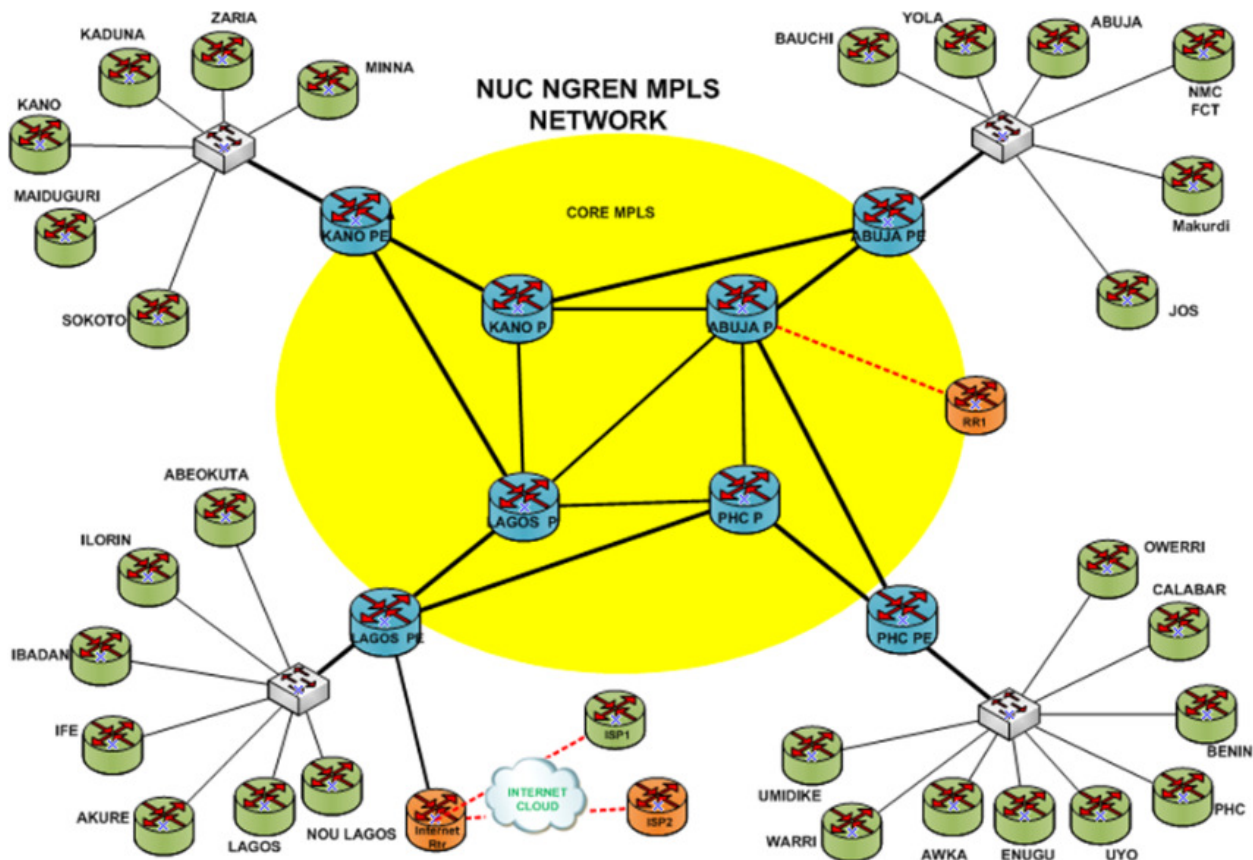


Figure.1 NgREN MPLS Network source: www.ngren.edu.ng

5. CSIRT FUNDING AND SUPPORT

This is the first step in establishing a CSIRT within the organization. In many instances, the individuals serving on the project team as well as intermediate managers must be aware and supportive of the project [1]. The management should demonstrate ability and willingness to promote and move the project forward. Besides demonstrating the willingness to support the project, management committee must be ready to release enough funding for the project [1]. It is must for any new forming and existing CSIRT to secure the top level management support of the funding organization.

Any CSIRT that fails to secure initial and continuous management support of the main organization will end of struggling for recognition from the management [4]. This signifies the commitment of stakeholders to 'buy into' the decision of forming the CSIRT, that is, to agree to provide support, especially monetary and other resources. Funding is critical and centred to forming CSIRT. The fund should be obtained for start-up, short and long term plans. The funding would be used not only for start-up costs (software, computing equipment, capital furniture expenditures, supplies, Internet domain registration fees, facilities costs, phones, fax machines) but human resources costs (salaries and benefits).

6. COMPUTER SECURITY INCIDENTS RESPONS TEAMS

6.1. Description of a CSIRT

A CSIRT is a solid authoritative element or capability (i.e., one or more staff parts) that is saddled out the obligation of providing piece of the incident response management for a specific organization [2]. This means that CSIRT is a unit dedicated to guaranteeing that suitable technology and best systems management practices are utilized to counter attacks on networked environment and in addition to restricting harm and guaranteeing coherence of critical services despite effective attacks. Once an incident happens, participants of a CSIRT can aid its constituency in figuring out what happened and what moves need to be made to remedy the circumstances.

This is particularly vital since communication network systems have turned into an important component in financial, educational and social development. Furthermore, the security of these network systems is of growing concern to society [1].

6.2. The evolution of CSIRT

The first CSIRT was made in response to an incident -the 1988 Morris worm. The worm was made to spread across network abusing different vulnerabilities. Consequently, systems such as email and Internet backbone servers were infected. For this reason many Internet sites were removed from the network and this result to total outage of Internet [2]. This problem made US Defence Advanced Research Projects Agency (DARPA) to believe that lack of correspondence between the organizations within the network to evaluate the severity of the worm brought about the failure to avert the situation at an early stage. For this reason DARPA board resolved that an official coordination method was needed to handle such computer security attacks and related analysis and response. In 1988, DARPA chose the SEI as the home of a coordination centred for Internet security incidents [2].

SEI was charged the responsibility of coordinating security emergencies and building awareness across the Internet community. As a result of this, SEI established the CERT coordination Centre (CERT/CC), which metamorphosed over the years into the CERT Division (www.cert.org). Internet had grown from 60,000 host computer systems as at 1988 to 1.2 billion hosts in July 2014 (see figure 2) as measured by the Internet Systems Consortium (see Internet Domain Survey at the Internet Software Consortium). The number of forming CSIRT teams will be increasing to commensurate the growing Internet community worldwide, servicing varieties different sizes domains from organizations, regions and countries (FIRST.org Inc, 2014). Obviously, such a vast constituency would be in effectively served by a single CSIRT.

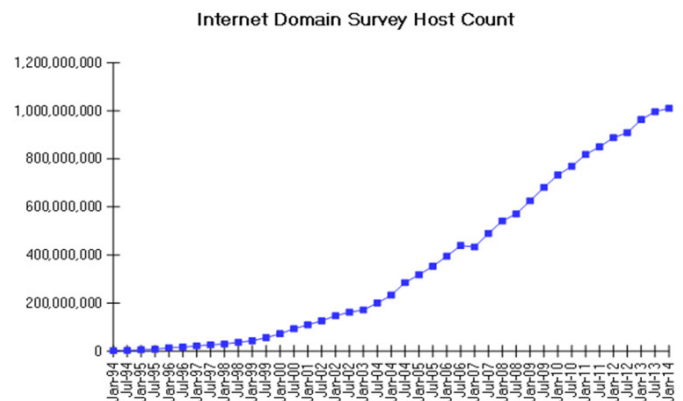


Figure. 2 Internet domain host count

Source: www.isc.org

For this reason, there are many CERT-teams nowadays. The Forum of Incident Response and Security Teams (FIRST) in 2014 projected the growth of these teams across the globe as shown in figure 3.

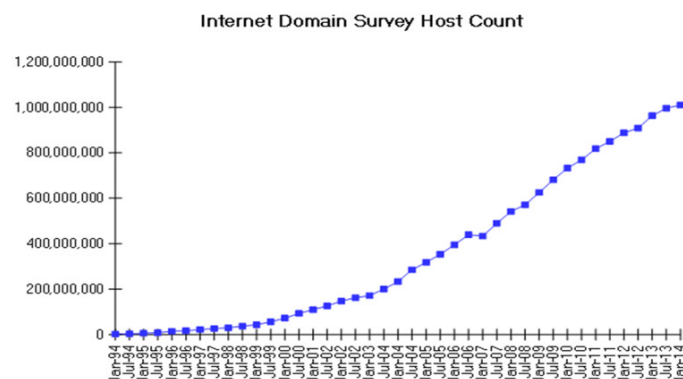


Figure. 3 Worldwide distribution of CSIRT

Source: www.first.org

7. CSIRT FRAMEWORK

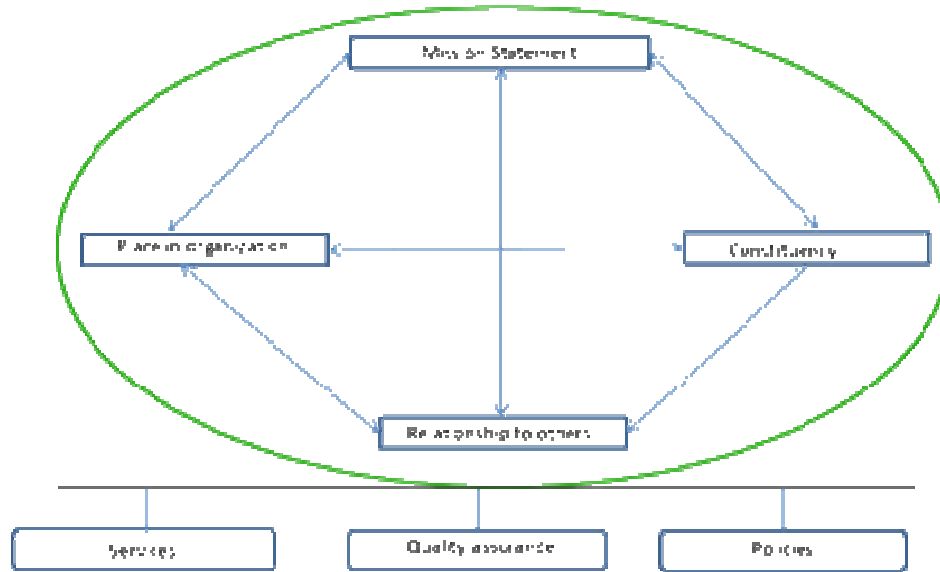


Figure. 4 CSIRT Framework by [4]

At present, a brief description of CSIRTs and their evolution has been discussed section 6.2 and we are now going to have a close look at the main fundamental subjects that must be considered and resolved by every CSIRT. According to the [4] the framework consists of:

- CSIRT Mission
- Constituency
- Organizational placement
- Relationship to other CERTs

As indicated by [4], these four rudimentary components are directly linked to one another as shown in figure 4. If for example, one of the elements is changed or affected the other ones will also change.

7.1. CSIRT mission

This is typically considered as the organization overall goal and objective. A mission statement can be defined as a way in which the organization communicates the business it is in to the outside world [5]. Mission clarifies the organization's reason of being. The mission of an organization is a pronouncement which distinguishes it among other organizations, issues its character and announces to the outside world why the organization is carrying out its functions [6]. For a CSIRT, the statement of purpose (mission statement) pronounces which services will be given, and the quality of these services. The overall mission's statement of each CSIRT within its constituency ought to be about giving a decent security to its constituency. The focus of mission statement of a CSIRT should be the team main functions, which is to be a focal point for preventing, receiving and responding to computer security incidents [7].

7.2. CSIRT constituency

A typical meaning constituency rose as a gathering of individuals with differing qualities who are connected by social ties, offer regular viewpoints, and participate in joint activity in topographical areas or settings. The members varied in the emphasis they set on specific components of the definition. The CSIRT constituency can be described as "a particular organization, region or country the CSIRT is design to provide services" [4]. A CSIRT constituency can be boundless or bounded. Most of CSIRTs today are bounded meaning that they only serve the funding organization. Understanding the CSIRT's constituency will make the team focus for the needs of organization and assets to be protected [2].

7.3. Place in Organization

Diverse structures are proposed for CSIRT by missions, objectives, necessity and services. Teams may be formed in distinctive units such as business, governmental, military, research work, IT, and have diverse structures. Along these lines, CSIRTs are partitioned by shape, size and function to internal, national CSIRTs, coordination centres, investigation centres, vendor's team and incidents response service. In first step, CSIRT responses to genuine security incidents and decreases attack effects [8].

7.4. Relationship with other Teams

"The Internet is the realm of CSIRTs, and by extension the world. There are many CERT teams around the world that are being served by a CSIRT" [4]. In this respect, at some level these CSIRTs need to inter-operate so as to accomplish their job. This participation and coordination exertion is at the very heart of the CSIRT framework: simply expressing the mission, defining constituency, and deciding the CSIRT's place within the organization are not sufficient without likewise covering the coordination issue [4].

7.5. CSIRT services

The CSIRT service is one of the derivatives of mission statement of a CSIRT. CSIRT mission is actualized through the services offered by a team to the team's constituency [4]. CSIRTs around the world may not provide the same set of services. The services to be provided by the team depend on the desires of the organization, the available technical know-how and funding. CSIRT services vary based on organization, purpose and mission of the team. A CSIRT team must provide an incident handling service before it can be considered as a CSIRT. Figure 5 shows the categories of services that a CSIRT could provide to its constituency [2].

i) Reactive services

Reactive services are the core component of CSIRT work. These services are activated by an action or solicitation, for example, a report of a vulnerable host, wide-spreading malicious code, vulnerable software, or something that was identified by an intrusion detection or logging system. Receptive administrations are the centred segment of CSIRT work [2].

ii) Proactive services

These will enable the CSIRT team to immediately prepare to protect the organization assets in expectation of attacks. Security incidents occurrences can greatly reduce by performing these services [2]. Proactive services meant to improve the security of infrastructure and processes within the organization before any incident or even occurs is detected (CERT/C, 2005).

iii) Security quality management

These services enhance existing and well-implemented services that are free of incident handling and generally performed by different segments of an organization, for example, the IT, audit, or training development. These services are by and largely proactive yet help by reducing the number of occurrence of incidents [2]. These services are meant to improve the general security of an organization (CERT C/C, 2005).

7.6. Quality assurance

Next to CSIRT Services, another derivative of CSIRT mission is Security Quality Assurance. This involves ensuring security quality is maintained for the entire services provided by the CSIRT. This is done by using feedback, risk assessment and business impact analysis.

7.7. Policies and procedures

Another derivative of internal components of CSIRT framework is policy. "It is important to sustain all CSIRT functions and services be sustained by clear policies and procedures" [2]. Policies are considered the guidelines for a CSIRT. These policies includes security policy, incident handling policy, data sensitivity policy, data storage and handling policy, acceptable use policy and as well as internal and external communication, for example handling the media [4]. Procedures for how the policies of the CSIRT can be conducted should also be put in place.

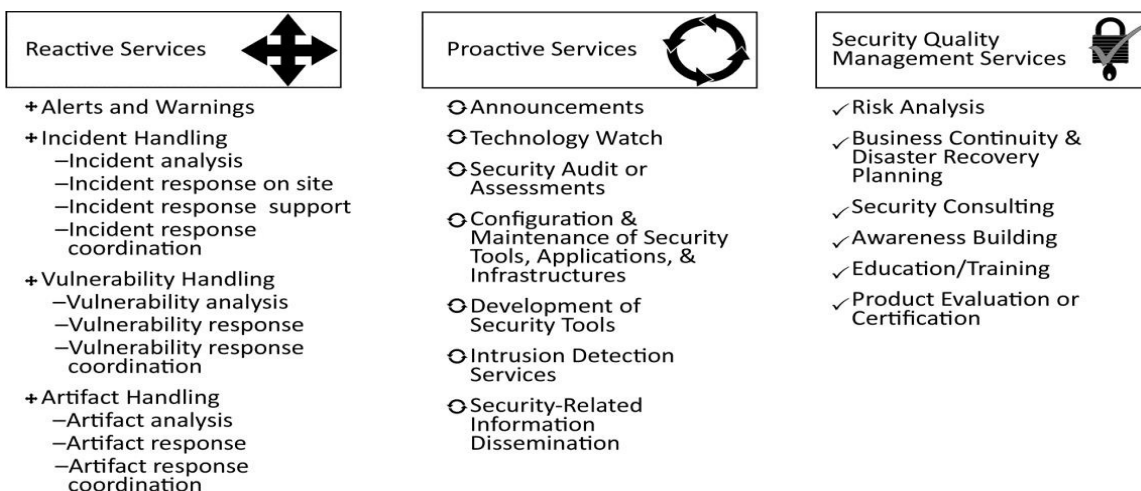


Figure 5: CSIRT Services list by [2]

8. CSIRTs ORGANIZATIONAL MODELS

Organizational structure is the organization's internal pattern of relationships, authority, and communication. Similarly, organizational structure is defined as "the network of relationships and roles existing throughout the organization" [9]. An organizational model, is a hierarchical structure, defines framework through its system, including lines of power, communications, obligations and asset allocations. Organizational model is also determined by the organization's objectives and serves as the connection in which processes work and business is carried out. Thus, the organizational model decides the number of employees required and their obliged expertise sets [9].

Diverse CSIRT organizations contains missions, objectives, needs, and services. CSIRT teams can be setup in any type of organization. Consequently, CSIRTs are categorized by nature, scope such as internal or national CSIRTs and the kind of services it provides such as incident response, coordination and analysis and product team [8].

Presently, there is no single way to classify CSIRTs. However, research has indicated that CSIRTs can be classified using different features such as scope, nature and functions etc. But, despite these categorization the CSIRTs roles, mission and responsibility remains the same [8]. In the case of NREN, a combined central coordination and a security team is recommended. This is because of the diverse nature of the network. Central coordination is serving as the central coordination for the network and security team will be providing onsite support and as well track attacks within its own local network and report to the central coordination committee.

9. CONCLUSIONS

Due to sophistication of cyber-attacks and lack of cyber security coordination within the developing NRENs, managers have to strategize to contain these attacks in coordinated and organized way by implementing Cyber Security Incident Response Teams (CSIRT). Thus, article has examined the guidelines for establishing Computer Security Incident Response Teams (CSIRTs) for securing the National Research and Education Network (NREN) as its main contribution.

The importance of this paper lies in the practical guidance on what to do at the planning stage of the CSIRT establishment. Even though the paper is aimed at identifying the critical steps needed to establish a CSIRT within an NgREN, all the steps and guidance are relevant for other NRENs. Having a dedicated centralized coordination for cyber security issues as a point of contact for security incidents within an NREN will help in mitigating and preventing major security issues before it becomes disastrous. The weaknesses of not having a CSIRT structure within interconnected network devices are obvious. The inability to contain an incident can lead to repeated incidents. This continual cycle can only lead to disaster.

Future work is proposed to further refine these guidelines, especially regarding establishment of CSIRT for NREN particularly in Nigeria as the case study.

ACKNOWLEDGEMENT

The creation of this paper required support and guidance of a number of people. I therefore, deem it my major duty to show gratitude to my thesis supervisor who provided me constructive criticisms during the development of this paper. Lastly, I am thankful to National Information Technology Development Agency for providing with full financial sponsorship.

REFERENCES

- [1] Marthie Grobler and Harri Bryk. 2010. Common Challenges Faced During the Establishment of a CSIRT. IEEE: 978-1-4244-5495-2/10
- [2] Robin Ruefle, Ken van Wyk & Lana Tomic. 2013. New Zealand Security Incident Management Guide for Computer Security Incident Response Teams (CSIRTs). New Zealand National Cyber Security Centre Government Communication Security Bureau. Developed in cooperation with the CERT® Division of the Software Engineering Institute at Carnegie Mellon University.
- [3] Olutayo Ajayi & Ibironke Ajayi. 2011. Fostering a Secure Framework for National Research and Education Network. Proceedings and reports of the 4th UbuntuNet Alliance annual conference: 29-44.
- [4] Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece Robin Ruefle & Mark Zajicek. 2003. Handbook for Computer Security Incident Response Teams (CSIRTs).
- [5] Papulova, Z. 2014. The Significance of Vision and Mission Development for Enterprises in Slovak Republic. Journal of Economics, Business and Management 2(1):
- [6] Pinar Altıok. 2011. Applicable vision, mission and the effects of strategic management on crisis resolve. Procedia Social and Behavioral Sciences 24: 61–71.
- [7] Wiik, Johannes & Gonzalez, José J. 2005. Limits to effectiveness of Computer Security Incident Response Teams (CSIRTs). In 23rd International Conference of the System Dynamics Society. The System Dynamics Society, Boston, MA.
- [8] Ali Naseri & Omid Azmoon. 2012. Proposition of Model for CSIRT: Case Study of Telecommunication Company in a Province of Iran. IJCSI International Journal of Computer Science Issues 9(1): 1694-0814.
- [9] Teixeira, R., Koufteros, X.A. & Peng, X.D. Organizational Structure, Integration, and Manufacturing Performance: a Conceptual Model and Propositions. Journal of Operations and Supply Chain Management 5 (1): 69 – 81.

