

ORGANIZATIONAL FRAMEWORK FOR CSIRT: A CASE FOR DEVELOPING
NATIONAL RESEARCH AND EDUCATION NETWORK

YAHYA MOHAMMED WARA

THESIS SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS
FOR THE DEGREE OF MASTER OF CYBER SECURITY

FACULTY OF INFORMATION SCIENCE AND TECHNOLOGY
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI

2015

**RANGKA KERJA ORGANISASI UNTUK CSIRT: A CASE UNTUK
MEMBANGUNKAN NEGARA PENYELIDIKAN DAN RANGKAIAN
PENDIDIKAN**

YAHYA MOHAMMED WARA

**TESIS DISERAHKAN BAGI MEMENUHI DARIPADA SYARAT
PENGANUGERAHAN IJAZAH SARJANA KESALAMATAN SIBER**

**FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI**

2015

DECLARATION

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledge.

8 May 2015

YAHYA MOHAMMED WARA
GP02547

ACKNOWLEDGMENT

All praises are due to Allah (SWT) for sparing my life in good health to accomplish this study. My profound gratitude and deep appreciation goes to my supervisor, Associate Professor Dr. Dalbir Singh for his understanding, patience, support and motivation throughout the period of this study. His professional advice and willingness to provide the necessary support would not be forgotten. My special thanks go to him for his valuable discussions, critiques and suggestions for this study to see the light of the day. His understanding and accommodation was exceptional. Despite his busy schedules, he was always ready to give me audience, thoroughly read, corrected the drafts and make recommendations. I would remain grateful for your kindness and insightful comments. My profound appreciation goes to the Head of Cyber Security program, Professor Dr. Zarina Shukur for making it possible for me to attend this program (Master of Cyber Security). Her accommodation and understanding was excellent. Regardless of her busy schedules, she was always ready to give audience to students. I would always remain indebted for your kindness. Equally, I am greatly appreciative to the National Information Technology Development Agency (NITDA) for providing me with full financial scholarship to attend Master of Cyber Security at National University of Malaysia. I would always remain grateful to you. Finally, I am sincerely thankful to the CEO of NgREN, Mr. Ahmed Isah Chafe for assisting me with information for this study. Your insightful comments during the validation of the framework are highly appreciative. I would ever remain grateful for your professional advice.

To all my fellow graduate students of Master of Cyber Security for the good time we spent together in this journey. I am appreciative for being with you. My profound gratitude goes to my friends in the Cyber Security program UKM; Isla, Ronie and Jalil. I am highly appreciative for your brotherly hood and companionship. To my family members, I hold all of you in high esteem for your prayers, encouragement, sacrifice, patience, support and forbearance despite the physical and psychological deprivations. Particularly to my wife Rukayya and my children; Ahmed, Abdul-Rahman and Zainab for your prayers and continuous show of love and who put up with my absence for so long. They identified and support this dream in many ways and never did they show any sign of fatigue.

Some names are just too precious to be forgotten for their contributions towards my success. Names like that of Dr. Abubakar Muhammad Miyim, Dr. Hussaini Kwami, Muazu shamaki, Ahmed Aliyu, Ahmed Chinade, Mohammed Dantani Idris, Aliyu Ahmed and others. I say thank you all.

ABSTRACT

Academic institutions worldwide embrace communication network and Internet services for their academic activities and collaboration. National Research and Education Network (NREN) is a network that enables academic institutions in a particular country or region to come together for collaboration. Despite preventive measures being implemented, security incidences occur occasionally. A sophisticated cyber-attack can undoubtedly trigger crisis that can affect the entire network. Managers of NRENs, particularly in Nigeria, have to re-strategize to contain these attacks in an organized fashion. This calls for effective and efficient cyber security incident response team (CSIRT). Several frameworks addressing cyber security incident response team exist. However, only few are generic and organization non-specific. In this thesis a study for adoption and proposing of organizational CSIRT framework was conducted. The research was conducted as a case study for Nigerian Research and Education Network (NgREN), where the data collection methods include interview and focused synthesis method using published articles, industries papers and archival data. Our findings show that NgREN lacks the structure for cyber security incident response team, policies and guidelines for cyber security incident management. We found that organizational CSIRT framework to be an important factor to an effective and efficient cyber security incident management. Finally, we contributed by identifying challenges of cyber security incident management within the NgREN. We also created an organizational CSIRT framework for an effective and efficient cyber security incident management in NREN. We recommended NgREN to implement the framework for cyber security incident management, develop security policies and guidelines for better cyber security incident management, sign memoranda of understanding (MOU) with other CERTs for problem escalation and conduct regular trainings for employees regarding sensor network incident detection and analysis.

ABSTRAK

Institusi akademik di seluruh dunia menggunakan rangkaian komunikasi dan Internet untuk aktiviti akademik dan kolaborasi. Rangkaian Penyelidikan dan Pendidikan Kebangsaan (NREN) adalah satu rangkaian yang membolehkan institusi akademik di sesuatu negara atau kawasan tertentu berkumpul bagi tujuan kolaborasi. Walaupun langkah pencegahan dilaksanakan, insiden keselamatan masih berlaku. Serangan siber yang canggih nescaya boleh mencetuskan krisis yang boleh menjejaskan seluruh rangkaian. Pengurus NRENs, terutamanya di Nigeria, perlu mengatur semula strategi untuk mencegah serangan-serangan mengikut langkah-langkah yang teratur. Ini mencetus kewujudan pasukan keselamatan dan respon terhadap insiden siber (CSIRT) yang berkesan dan cekap. Terdapat beberapa rangka kerja berkaitan pasukan keselamatan dan respon terhadap insiden siber. Bagaimanapun, hanya terdapat beberapa rangka kerja generik dan tidak spesifik terhadap organisasi yang tertentu. Dalam tesis ini, satu kajian bagi mengadaptasi dan mencadangkan rangka kerja organisasi CSIRT dijalankan. Penyelidikan dijalankan sebagai satu kajian kes untuk Rangkaian Penyelidikan dan Pendidikan Nigeria (NgNREN), di mana kaedah pengumpulan data merangkumi temuramah dan penumpuan kaedah sintesis menggunakan artikel, kertas industri dan data arkib yang telah diterbitkan. Penemuan menunjukkan bahawa NgREN mempunyai struktur organisasi yang kurang sesuai untuk pasukan keselamatan dan respon terhadap insiden siber beserta dasar dan garis panduan untuk pengurusan kejadian keselamatan siber. Kami mendapati rangka kerja organisasi CSIRT menjadi satu unsur yang penting di dalam pengurusan kejadian keselamatan siber yang lebih berkesan dan cekap. Akhirnya, kami menyumbang dengan mengenal pasti cabaran pengurusan kejadian keselamatan siber untuk NgREN. Kami juga mewujudkan rangka kerja organisasi CSIRT untuk pengurusan kejadian keselamatan siber yang berkesan dan cekap di NREN. Kami mengesyorkan NgREN untuk melaksanakan rangka kerja untuk pengurusan kejadian keselamatan siber, membina dasar keselamatan dan garis panduan untuk pengurusan kejadian keselamatan siber yang lebih baik, menandatangani perjanjian persefahaman (MOU) dengan CERTs lain untuk masalah yang kian meningkat dan menjalankan latihan yang kerap untuk kakitangan yang berkaitan rangkaian penerima pengesanan dan analisis kejadian.

CONTENTS

	Page
TITLE PAGE	ii
DECLARATION	iii
ACKNOWLEDGEMENT	iv
ABSTRACT	v
ABSTRAK	vi
CONTENTS	vii
LIST OF APPENDIXES	x
LIST OF TABLES	xi
LIST OF FIGURES	xii
LIST OF ABBREVIATIONS	xiii

CHAPTER I	INTRODUCTION	
1.1	Introduction	1
1.2	Problem Statement	2
1.3	Motivation for the Study	3
1.4	Scope	3
1.5	Justification for Using the Framework	3
1.6	Objectives	4
1.7	Research Questions	5
1.8	Methodology	5
1.9	Research Project Structure	5
1.10	Summary	6
 CHAPTER II	 LITERATURE REVIEW	
2.1	Introduction	7
2.2	National Research and Education Network	7
	2.2.1 NREN Technology	8
	2.2.2 Nigerian Research and Education Network	8
	2.2.3 NgREN Topology	10

	2.2.4 IP MPLS Network	10
2.3	Cyber Security Incidents Defined	11
2.4	Cyber Security Incidents Management	12
2.5	Computer Security Incidents Response Teams	13
	2.5.1 Description of CSIRT	13
	2.5.2 The evolution of CSIRT	14
2.6	CSIRT Types	17
2.7	CSIRT Framework	17
	2.7.1 Mission Statement	19
	2.7.2 CSIRT Constituency	20
	2.7.3 Place in Organization	21
	2.7.4 Relation to Other Teams	23
	2.7.5 CSIRT Services	24
	2.7.6 Quality Assurance	26
	2.7.7 Policies and Procedures	26
2.8	CSIRT Funding and Support	27
2.9	Review of CSIRT Organization Models	28
2.10	Existing National Research and Education Network CSIRT (NREN CSIRT)	36
2.11	Summary	37
CHAPTER III	METHODOLOGY	
3.1	Introduction	38
3.2	Research Methodology	38
	3.2.1 Qualitative Research Method	39
	3.2.2 Qualitative Interview	39
	3.2.3 Focused Synthesis	40
	3.2.4 Participants	41
	3.2.5 Documents Study	41
3.3	Research Methodology Phases	41
	3.3.1 Literature Analysis	42
	3.3.2 Cyber Security Incident Analysis in NgREN	42
	3.3.3 Proposition of the Framework	43
	3.3.4 Validating the Framework	44
3.4	Summary	44

CHAPTER IV	RESULTS AND DISCUSSION	
4.1	Introduction	45
4.2	Literature Analysis	46
	4.2.1 Analysis and Finding	46
4.3	Cyber Security Incident Analysis in NgREN	48
	4.3.1 Data Analysis and Finding	48
4.4	Proposition of the Framework	53
	4.4.1 Proposed CSIRT Framework for the NgREN (NgREN-CSIRT)	53
	4.4.1.1 Major NgREN-CSIRT components	54
	4.4.1.2 NgREN CSIRT organizational model	55
	4.4.1.3 Reporting and communication	58
	4.4.1.4 NgREN-CSIRT services	58
	4.4.1.5 Security quality assurance	61
	4.4.1.6 Policies and procedures	62
	4.4.1.7 NgREN CSIRT resources	63
	4.4.1.8 Management support and funding strategy	69
4.5	Validating the Framework	70
4.6	Discussion	70
4.7	Summary	74
CHAPTER V	CONCLUSION	
5.1	Introduction	75
5.2	Main Contributions	75
5.3	Limitations	78
5.4	Future work	79
5.5	Conclusion	79
REFERENCE		80
APPENDIXES		83

LIST OF APPENDIXES

Appendix No.		Page
I	Introductory letter to Conduct Research at NgREN	83
II	Confirmation letter of conducting interview	84
III	Interview Questions	85

LIST OF TABLES

Table No.		Page
2.1	CSIRT Funding Strategy	28
2.2	Critical Review of CSIRT Organizational Models	33
3.1	Research Targets of Interview Questions	40
3.2	Research Methodology Phases	42
4.1	Experts Comments on the Framework	72

LIST OF FIGURES

Figure No.		Page
2.1	NgREN IP MPLS Network	11
2.2	Internet Domain Host Count	16
2.3	FIRST Number of CSIRTs	16
2.4	CSIRT Framework	18
2.5	CSIRT Services List	24
4.1	NgREN CSIRT Organizational Placement	55
4.2	NgREN CSIRT Organizational Model	56
4.3	NgREN CSIRT Expanded Organizational Model	57
4.4	NgREN CSIRT Security Team	58
4.5	Incident Handling Process Model	60
4.6	NgREN-CSIRT network model as recommended by expert	68
4.7	Security team network model as recommended by expert	68
4.8	NgREN CSIRT Functional Framework	73
4.9	NgREN CSIRT Process Model	74

LIST OF ABBREVIATIONS

ACERT/CC	Army Computer Emergency Response Team Coordination Center
AFCERT	Air Force Computer Emergency Response Team
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CERT/CC	Computer Emergency Response Team Coordination Center
CMU	Carnegie Mellon University
CONOPS	concept of operations
CSIRC	Cyber Security Incident Response Capability
CSIRT	Cyber Security Incident Response Team
DARPA	Defense Advanced Research Projects Agency
DOD	Department of Defense
FIRST	Forum of Incident Response and Security Teams
HEI	Higher Educational Institution
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IP	Internet Protocol
ISC	Internet Software Consortium
MPLS	Multiprotocol Label Switching
MYCERT	Malaysia Computer Emergency Response Team
NASA	National Aeronautics and Space Administration
NAVCIRT	NAVAL Computer Incident Response Team
NgREN	Nigerian Research and Education Network
NIST	National Institute of Standards and Technology
NMC	Network Management Center
NREN	National Research and Education Network
REN	Research and Education Network
SEI	Software Engineering Institute
VPN	Virtual Private Network

CHAPTER I

INTRODUCTION

1.1 INTRODUCTION

The increasing complexity and rate of Cyber-attacks, as well as the impossibility to completely secure IT systems made modern organizations to be prepared earlier for cyber security incidents and information drips. A sophisticated cyber-attack can undoubtedly trigger crisis that affect various stakeholders both within and outside the organization. Cyber-attacks are becoming more advanced and sophisticated, and are increasingly targeting intellectual property and other proprietary information held by businesses as well as individuals, government organizations, and critical infrastructures. Such attacks are seen across the globe (Ruefle et al 2013). In the light of this, it is important that organizations including National Research and Education Networks review their information security needs, regulations and Technologies. One of such needs and regulations is having an organized CSIRT framework.

Cyber Security Incident Response Team (CSIRT) provides services and supports for preventing, handling and responding of computer security incidents, like systems and services crash, malware analysis, unauthorized access, improper use and combined attacks (Naseri et al, 2012). To this end, it is imperative National Research and Education networks world-wide to respond to this increasingly cyber-attacks by building strategies and supporting resources to help them develop and implement security defences and practices. One kind of this strategy is to have an

Organize Cyber Security Incident Response Team (CSIRT).

1.2 PROBLEM STATEMENT

Cyber Security Incidents have turned into daily affairs for most organizations since reliance on Information and Communication Technology (ICT) is crucial in their daily activities. In their efforts to exploit these opportunities that ICT provides, known and unknown security threats which need to be handled immediately also emanate. Handling these security incidents presents the need for organize Cyber Security Incident Response Team (B. Line et al, 2014, Ahmad et al, 2011, Ruefle et al, 2013), which can be bestowed the responsibility of coordinating and handling Cyber Security Incidents.

Attack to software, network and system is the cause of cyber security incidents. Cyber Security Incident Response Capability (CSIRC) prevents attacks by responding, predicting and safe guarding quality management services (Naseri et al, 2012). Hence, organizations need to be prepared to handle Cyber Security Incidents caused by both known and unknown vulnerabilities. A number of factors and options are involved in determining how successfully organizations can develop CSIRT framework to respond to information security incidents.

The most widely used and fundamental generic framework is the one developed by the Software Engineering Institute (SEI) of Carnegie Mellon University (Brown et al, 2003, Ruefle et al, 2013). This is because generic frameworks are not centered on any nation or organization. This was supported by (West-Brown et al, 2003), where it says that the framework is generic to enable the organization to apply it to any type of CSIRT environment, from a fee-for-service team, to an in house team for a given organization, or an international coordination center. In addition, (West-Brown et al 2003) stated that “No single set of CSIRT service definitions, policies, and procedures could be appropriate for any two CSIRTs”. This is because no single organization has the same demographic features. For this, every CSIRT must make decisions on the type and nature of services they hope to provide based on their own unique circumstances. For instance, what has worked well for CERT/CC may not be

suitable for MYCERT. Therefore, in this thesis, an organizational framework for CSIRT: A case for developing National Research and Education Network is proposed for NgREN. This framework when implemented will help in mitigating Cyber Security Incident in the chosen case study area.

1.3 MOTIVATION FOR THE RESEARCH

For organizations to achieve better security in their information systems, they need an organized way to handle security incidents. However, it is more efficient to establish a centralized team that can support the entire organization in handling a security incident. This is because the team will be able to handle and follow up security incidents, and provide security support to the users within the organization.

Presently, CSIRT framework appears to be the most effective way of handling cyber security incident in organizations. Having seen the functions of the CSIRT in handling cyber security incident to organizations, one is encouraged to explore the possibility of incorporating the CSIRT framework as part of the NgREN policy framework. This is because it will help in mitigating cyber security incident within the National Research and Education Network of Nigeria, which at the moment is not in existence.

1.4 SCOPE

This research project is going to concentrate on Nigeria's research and education network. This network was created to serve the academic institutions and research organizations in Nigeria. In this regard, CSIRT framework will be discussed with the aim of adopting it as a framework for use in academic networks in Nigeria to mitigate cyber security incidents.

1.5 JUSTIFICATION FOR USING THE FRAMEWORK

The existing frameworks on implementing cyber incident response are mostly based on particular form of nations or organizations with full developed infrastructure,

adequate funding, and human resource and a wide adoption of Internet utilization. The consequence is that the current frameworks do not directly address the needs of the nations with emerging infrastructure like Nigeria. However, the document presented in the CSIRT framework by West Brown et al, 2003 is generic to enable the organization to apply it to any type of CSIRT environment, from a fee-for-service team, to an in house team for a given organization, or an international coordination center.

In addition, West-Brown et al, 2003 stated that “No single set of CSIRT service definitions, policies, and procedures could be appropriate for any two CSIRTs”. This is because no single organization has the same demographic features. Due to lack of available resources in the area of operational policies and procedures, e.g., generic CSIRT policies, procedures, and templates that can be adapted or revised for use by the newly forming teams. Either existing teams have nothing documented to share or they are unable to share their documentation due to its sensitive nature. Seeking expert advice is also difficult because there is still a shortage of experts in the field. Existing experts are highly sought after, have little time to make available, and can be expensive to engage (West-Brown et al, 2003). This is why CSIRT framework becomes relevant in developing a unique model for Nigeria Research and Education Network (NgREN).

1.6 OBJECTIVES

The major objective of this study is to propose an organizational CSIRT framework for the Nigerian Research and Education Network (NgREN) for centralize and efficient handling of information security incidents. The following are the goals of this study

- To conduct critical review on cyber security incident response management;
- To propose an efficient organizational CSIRT framework for the NgREN; and
- To validate and refine the proposed framework.

1.7 RESEARCH QUESTIONS

The central research question of this thesis is:

“How CSIRT framework can be proposed to efficiently mitigate cyber security incidents in Nigeria Research and Educational Network”? To answer this question, the following sub-questions need to be answered:

1. What is generic CSIRT framework and its component?
2. How NgREN manages cyber security incidents?
3. How would the generic CSIRT framework be customized for Nigerian Research and Education Network?
4. How the proposed framework can be validated and refined?

1.8 METHODOLOGY

The methodology that would be used for this research is qualitative while the data collection comprises of primary and secondary sources generated from CSIRT framework by West-Brown et al, 2003, literature review and interview with NgREN stakeholders.

The literature review comes from various CSIRT frameworks, academic and technical write-ups on cyber security. The interview was conducted in English language with stakeholders that comprise the CEO and technical staff. Appendix II shows a letter from NgREN indicating that the interview was conducted.

1.9 RESEARCH PROJECT STRUCTURE

The structure of this project follows the sub questions that were derived from the research question.

Chapter I focused on the introduction and followed by the background, problem statement of the research, motivational factors that made the research to

conduct the research. Furthermore, the scope, model and methodology together with objectives were discussed and finally the summary of the chapter.

Chapter II focuses on National Research and Education Network (NREN) as a vital tool to improving collaboration among Higher Educational and Research institutions in facilitating teaching and learning. It also reviews CSIRTs and their functions as well as the CSIRT basic framework that is described in “Handbook for Computer Security Incident Response Teams (CSIRTs)” (West-Brown, et al, 2003, Ruefle et al 2011) and justified why this framework is useful for the new forming CSIRT like NgREN. It further discusses the different organizational model of CSIRT, briefly described some NREN CSIRT and finally the chapter summary.

Chapter III this chapter paid attention on how the research was conducted and the methodology used in achieving the final result. It further describes the methods and techniques used and reasons for choosing the methods.

The purpose of Chapter IV is to develop an organizational CSIRT framework for NgREN by using the results of qualitative analysis of direct interview and literature review from chapter two. In addition, the chapter discusses how the objectives of the study were achieved. Finally, the organizational CSIRT framework for NgREN was validated and refined by experts from NgREN and Cyber Security Malaysia.

Chapter V this chapter concludes this study by summarizing the main contributions of the study, discuss research limitations, recommendations and propose potential ideas for future work.

1.10 SUMMARY

In this Chapter an introduction was made and followed by the background, problem statement of the research, motivational factors that made the researcher to conduct the research. Furthermore, the scope, model and methodology together with objectives were discussed and finally the summary of the chapter.

CHAPTER II

LITERATURE REVIEW

2.1 INTRODUCTION

The expectation of this chapter is to have a first look on the National Research and Education Network (NREN) and field of Computer Security Incident Response Teams (CSIRTs). To begin with the National Research and Education Network (NREN) will be quickly examined to give us an insight to why using computer Network to improve collaboration among Higher Educational Institutions and Research institutes is critical in research, teaching and learning. Next to this, depiction will be given of what CSIRTs are, after which their history will be quickly examined. Secondly, the general framework of the "Handbook for Computer Security Incident Response Teams (CSIRTs)" (West-Brown et al., 2003, Ruefle et al, 2011) will be examined for a further investigation of CSIRTs. This handbook will be taken as an issue for depicting the environment a CSIRT is in. This framework was chosen as bases for this study because of it being a pioneer and generic CSIRT framework.

2.2 NATIONAL RESEARCH AND EDUCATION NETWORK (NREN)

National Research and Education Network (NREN) can be defined as a interlinking of researched and teaching focused institutions that is centered on making use of scarce of resources, offering solutions and enhancing infrastructure for the purpose of

realizing their set organizational goals (Ajayi et al, 2011).

Having the need for seamless interconnectivity and interoperability within any network does not warrant in compromising security issues within the Network. There are different levels of security for each user community. 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 the any system within it (Ajayi et al, 2011). Networks and its related systems services are considered critical in supporting dispersed research organizations around the globe. Despite the advancement of these network services in other part of the world, it is still at it stages in African countries and developing nations in to grow in years to come in (Ajayi et al, 2011).

2.2.1 NREN Technologies

It is of high important to perceive that even in the present day Internet, it has been feasible to have a perfect combination of enterprise, academics, government and military systems. For sure, the very capacity to acknowledge such a differing domain turns on the increasing opportunity of the intermediate level network systems to have a number of unrestricted clients (Ajayi et al, 2011). Presently, the Internet is properly serving the public but widely vulnerable to mass attacks, this is because the linkages between the Internet and the public make the system widely accessible 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.

2.2.2 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 Country. 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 as is provides connectivity between Nigerian institutions as well as connectivity with other global Research and Education Networks. It is viewed holistically, as a network of educational networks. The need for interconnectivity and interoperability of this kind of network does not imply that security issues should be compromised.

NgREN Network, like any other traditional Business Network is increasingly coming under attack by a variety of malicious sources. These range from hackers looking for attention, Security breaches, misconfiguration of equipment and software, copy-right infringement and even friendly sources that inadvertently bring malware onto a site. Above all there is lack of Cyber Security Incidence Response Capability within the network.

Different user communities require different levels of security. Each network on which the national information infrastructure is built must have a number of security procedures implemented that will prevent unauthorized access to the network and the systems that comprise it (Ajayi et al 2011).

The Nigerian REN has been built with the following infrastructure:

- (1) Networking instruments such as own routers, switches and various network management devices.
- (2) A set of backbone and access links that would connect these switches and routers and customer routers.
- (3) Peering with other national internet exchanges and other national providers' networks to exchange traffic.
- (4) Peering internationally to join the global network of RENs.

- (5) Links needed for backbone, access and peering are to be acquired from telecom/fiber operators- on a competitive and cost-effective basis.

NgREN also administers

- (6) A Network Management Center (NMC) to monitor and manage the operation of the entire network. The same facility is also housing its administration, help desks, interest group meeting rooms and training programs, and,
- (7) A set of network services (and host servers) which will bear access and authentication systems, packet shapers, firewalls, distributed caching, edu-roaming, multi-casting, VPN, bandwidth on demand, etc. to improve the overall network service.

2.2.3 NgREN Network Topology

The NgREN IP/MPLS network topology is defined by the presence of MPLS core network routers and interconnections between locations. The 27 Federal Universities and two additional locations now inter-connected to each other and to the NMC as shown in the Figure 2.1.

2.2.4 IP MPLS Network Topology

From the architectural perspective, the IP/MPLS core network is designed hierarchically.

The network topology is divided into two discrete logical layers: CORE and EDGE. Each layer focuses on a specific function so that the devices pertaining to that layer conduct only limited set of functions.

The Core layer provides a scalable, easily managed, high-speed architecture for delivering the NgREN Services. It is providing a high speed IP backbone with good levels of resilience and effective management for all existing services.

MPLS is being used in the core to make it scalable and robust. It is optimized for packet throughput, low latency and manageability. The diameter of the core layer is limited and consistent which provides predictable performance. Adding a distribution layer device does not increase the core layer diameter.

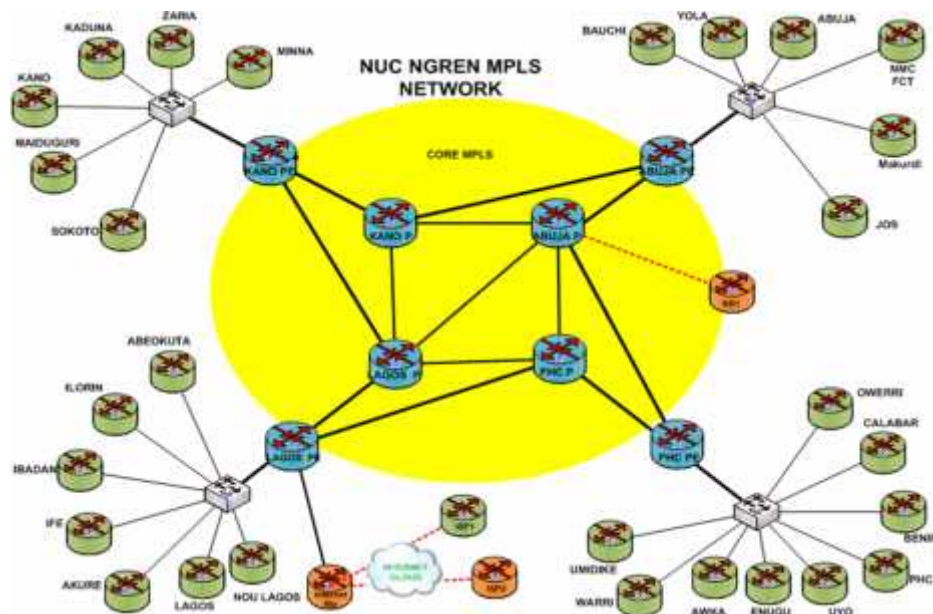


FIGURE 2.1 NgREN MPLS Network source: www.ngren.edu.ng

2.3 CYBER SECURITY INCIDENTS DEFINED

NIST Special Publication 800-61 states, “A computer security incident is a violation or imminent Violation of computer security policies, acceptable use policies, or standard computer security practices” (Devoe et al, 2013). For the purposes of this project cyber security incident will also be defined as any illegal activity involving academic and research education networks and computers, data or both. This definition assumes that adequate polices are in place to protect the intellectual property of the organization; the employees, and partners; and Protection of staff and students.

Incidents are made when events are triggered that give an evidence of an adverse activity. Events are things like IDS signature triggers, against virus infection

detection, firewall detecting a computer connecting to a malicious site, a phishing email is opened, or a firewall hindering a connection attempt. Actually, even something like a "computer becoming slow" is an event. Not all events produce incidents some are essentially false positives. An illustration would be a web filter hindering certain content on a website page. For instance, a client visits an authentic website like cnn.com; on that page are different notices and connections that divert the client to other sites. In the event that the web browser attempts to pre-fetch the hyperlinks and resolve them it may show up an end client attempted to get access to an unapproved web site. Truly, the client did no such thing.

Incidents can occur at random times and there can be multiple incidents occurring at the same time. The complexity of the incident can also vary as can the duration. A simple virus infection may only require cleaning the host while a data breach or discovery of illegal activity may take an extensive investigation and lengthy remediation. Finally, it is entirely possible to have multiple incidents that are all connected and interrelated. As can be seen, the response to the incident may vary in size, scope, and necessary resources (Devoe et al, 2013).

2.4 CYBER SECURITY INCIDENT MANAGEMENT

The ability to provide end-to-end, cross-enterprise management of events and incidents that affect information and technology assets within an organisation is called incident management.

Organisations require a multi-layered strategy to secure and protect their critical assets and infrastructures. That strategy requires technical, organisational, and procedural approaches to manage computer security incidents as part of the overall goal of achieving business or mission objectives in the face of risks and attacks. Organisations do not want to just survive attacks; they want to be resilient.

In defense of its assets against threats organization usually conduct risk assessments of its assets and proffer various solutions such as software updates, install

perimeter defenses, updates user and security policies and formalize incidents management capability.

An incident management capability provides coordination and resolution of computer security events and incidents. It implies end-to-end management for controlling or directing how security events and incidents should be handled. This involves defining a process and supporting policies and procedures; assigning roles and responsibilities; having appropriate equipment, infrastructure, tools, and supporting materials; and having qualified staff identified and trained to perform the work in a consistent, high-quality, and repeatable way.

An incident management capacity gives coordination and resolution of computer security incidents and events. It infers end-to-end management for controlling or administering how security events and incidents ought to be taken care of. Incident management is different but inclusive of incident handling and incident response. Incident handling is one service covering all the processes, tasks, or functions associated with handling events and incidents.

2.5 COMPUTER SECURITY INCIDENTS RESPONSE TEAMS

2.5.1 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 (Ruefle et al 2013). 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. A CSIRT is a team of dedicated information security specialists that prepares for and responds to information security incidents. It is responsible for receiving, reviewing, coordinating and responding to computer security incidents and activities (Grobler et al, 2010). 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 paramount since communication network systems have turned into a vital component in financial, educational and social development. In like manner, the security of these network systems is of growing concern to society.

The goal of a CSIRT is to minimize and control the damage resulting from incidents, provide effective response and recovery, and work to prevent future incidents (Ruefle et al 2013).

2.5.2 The evolution of CSIRT

Of course, the first CSIRT was made in response to an incident -the 1988 Morris worm. That worm was named for the 23-year-old college who developed it, spread itself from machine to machine by abusing different vulnerabilities. Most of the infected systems are email systems and Internet backbone servers. For this reason many Internet sites were removed from the network and this result to total outage of Internet (Ruefle et al 2013).

After the Morris worm, a US Defense Advanced Research Projects Agency (DARPA) board resolved that an absence of correspondence between the organizations evaluating and reacting to the worm brought about repetitive investigation as well as deferred protective and restorative measures. Better correspondence and coordination would have prompted both speedier control of the worm and prior systems recuperation (Ruefle et al, 2013). This corresponds to the mission of any NREN, which is coordination between member organizations.

The 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 center for Internet security incidents (Ruefle et al, 2013).

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 Center (CERT/CC), which metamorphosed over the years into the CERT Division (www.cert.org).

Department of Energy, NASA, the National Institute of Standards and Technology (NIST), and different military extensions created groups. In 1990, the CERT/CC, NIST, and a few different CIRTs helped secure the Forum of Incident Response and Security Teams (FIRST: www.first.org) for CSIRTs and security groups. Initially FIRST is a global consortium of CSIRTs that nurtures incident prevention and response cooperation, coordination, and information sharing. In the 1990s and early 2000s, more educational institutions, state governments, commercial organizations, nations and economies, and even law enforcement agencies established CSIRTs.

The Internet's fast development and its significance in Latin America and Africa highlighted the requirement for all geographic areas to have government cybersecurity programs. This was headed by the Organization of American States and the International Telecommunication Union, among others, to help nations in those areas create CSIRTs to act purposely as point of contacts for sharing of information, incident coordination, and capacity building.

The Internet had grown from 60,000 host computer systems at the time of the Morris Worm, to 1.2 billion hosts in July 2014 (see figure 2.2) as measured by the Internet Systems Consortium (see Internet Domain Survey at the Internet Software Consortium). Many companies now rely on the Internet in their daily business transactions. Incident response and security teams will continue to form around the globe, covering a range of constituencies from whole countries, to multi-national organizations (FIRST.org Inc, 2014). Clearly, a single CSIRT would not be able to effectively serve such a vast constituency. Also, the individual needs of the diverse communities could not be met, due to time zone, language, cultural, and organizational issues (West-Brown et al., 2003). This is a justification for creating CSIRT within the Nigerian Research and education Network. From figure 2.2 the vertical line shows number of hosts while the horizontal line indicates year.

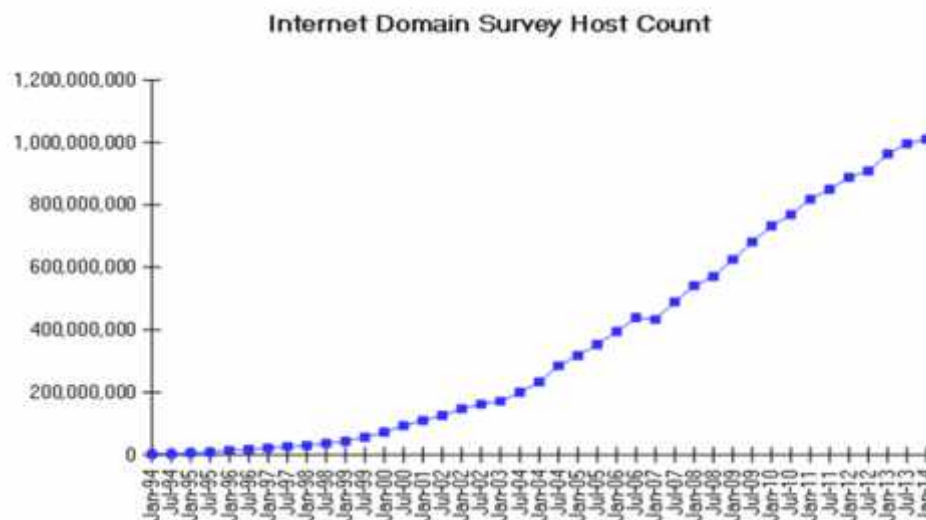


FIGURE 2.2 Internet domain host count

Source: www.isc.org

For these reasons, there are many CERT-teams nowadays. Although no exact numbers are available of the number of CSIRTs, the Forum of Incident Response and Security Teams (FIRST), which is “a task force for the collaboration of incident response teams in Europe” (West-Brown et al., 2003), still watches its number of members grow. This is shown in figure 2.3 which was published by FIRST (FIRST.org Inc, 2014). From figure 2.3 the vertical line represents number of CSIRTs while the horizontal shows continents and regions.

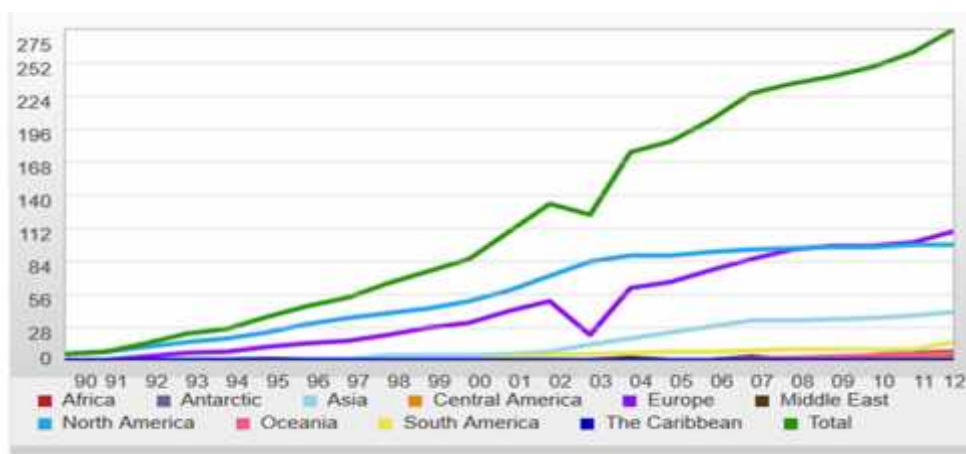


FIGURE 2.3 FIRST CSIRTs membership around the world

Source: www.first.org

2.6 CSIRT TYPES

Different structures are proposed for CSIRT by missions, goals, requirement and services. Teams may be established in different sections like commercial, governmental, military, research and development, IT and have different structures like management, services and organizational model. Therefore, CSIRTs are divided by shape, size and function to internal, national CSIRTs, coordination centers, analysis centers, manufacturer's team and incidents response service (Naseri et al 2012).

There is no one way to categorize the CSIRTs. But research has shown that CSIRTs can be categorized using different aspects such as size, shape and functions etc. However, despite these categorization the CSIRTs roles, mission and responsibility remains the same (Naseri et al 2012).

Finally, whatever the type, CSIRTs are meant to respond to actual security incidents and decreases attack effects. They play roles like protecting the systems, detecting, diagnosing and analyzing security damages, protecting against destructive activities, cyber security incidents coordination and effective response to computer attacks.

2.7 CSIRT FRAMEWORK

At present, a brief description of CSIRTs and their evolution has been discussed above and we are now going to have a close look at the main functions of CSIRTs together with fundamental issues that need to be considered and addressed by every CSIRT. To do this, the framework of the “Handbook for Computer Security Incident Response Teams (CSIRTs)” (West-Brown et al., 2003) will be used. This framework was developed in 1998 by the Carnegie Mellon Software Engineering Institute, and describes the basic issues that affect every CSIRT.

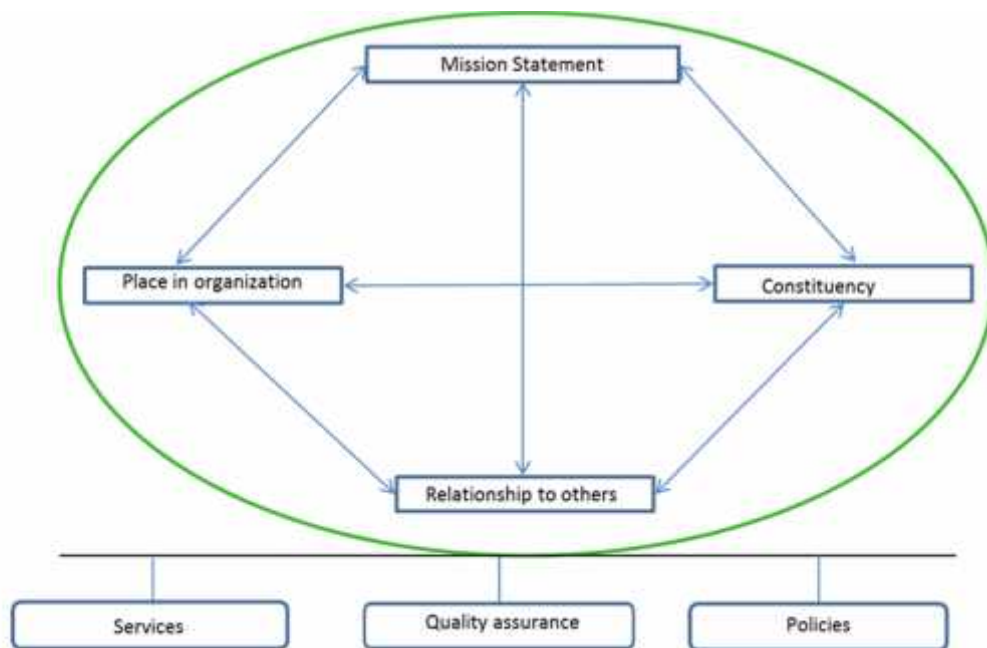


FIGURE 2.4 CSIRT framework based on (West-Brown et al. 2003)

There are numerous reasons to use this framework. Firstly, the framework describes the issues that affect every CSIRT, for both newly forming and existing teams. For newly forming teams it can be used as the basis for understanding the issues involved in establishing a CSIRT, whereas for existing CSIRTs, the framework could be used to ensure they have covered the main issues and options that are appropriate for their organization (West-Brown et al., 2003).

As stated in the CSIRT evolution section, the Carnegie Mellon Software Engineering Institute was charged with setting up one of the first CSIRTs in 1988 (CERT/CC, 2014). The handbook aims to offer help for new teams to establish appropriate and reliable services, by offering their experience to help them develop and implement more effective teams (West-Brown et al., 2003). Since this relates with the aim of this project, it is by all accounts a valuable resource.

The framework consists of the questions “what to do,” “for whom,” “in what local setting,” and “in cooperation with whom”. This question is then captured by identifying (West-Brown et al. 2003):

- Mission statement
- Constituency
- Place in organization
- Relationship to other teams

As indicated by the writers of the handbook, these four elements are closely identified with one another. If for example the tiered position in an organization is too low, it will be difficult for the CERT-team to have a very much-demanding mission within a massive constituency.

Based on the four rudimentary elements cited above, the services, policies and quality can be derived that a CSIRT provides to its constituency (West-Brown et al., 2003). The framework and dependencies of its internal components are shown in figure above. In this section these internal components will be debated in more detail. Firstly, the main internal components will be discoursed; the mission statement, constituency, place in organization and relationship to other. Finally, after having described these components, services, policies and quality, which are the products of these internal components, will be discussed in more detail.

2.7.1 Mission Statement

The mission statement is mostly referred to as the overall goal of an organization. A mission statement can be defined as a way in which the organization communicates the business it is in to the outside world (Papulova, 2014). Mission explains the organization's reason of existence. The mission of an organization is a manifesto which distinguishes it among other companies, gives it its identity and declares to the external environment why the organization is carrying out its activities. Mission keeps the manager and the personnel together in order to realize the defined objects. Besides providing organizational motivation, mission also guides the personnel towards understanding their responsibilities. Mission helps the organization in finding and utilizing the resources for reaching its objectives (Altuok, 2011). 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 mission statement will help provide a basic understanding of what the team is trying to achieve; and it will provide a focus for the overall goals and objectives of the CSIRT” (West-Brown et al., 2003). The mission statement of a CSIRT should focus on the team’s core activities, which is to be a focal point for preventing, receiving and responding to computer security incidents (Wiik et al, 2005).

A mission statement is rudimentary to empower the CSIRT to launch services and quality system, including the nature and scope of services to be launched, the description of its strategies and techniques, and the nature of service together with the description of the constituency, this service and quality system drives and limits all CSIRT exercises. Plainly, if the team is housed inside a superior organization or is supported from an outside body, the CSIRT mission statement must supplement the missions of those organizations (West-Brown et al., 2003). “Additionally, numerous CSIRTs also provide purpose statement that supplements the mission and clarifies the reason(s) that brought about the team being launched” (West-Brown et al., 2003).

2.7.2 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 “the specific community that the CSIRT was established to serve” (West-Brown et al., 2003). A CSIRT constituency can be unbounded (the CSIRT will provide service to anyone requesting it), or it can be bound by some constraints. Most commonly, CSIRTs have bounded constituencies that tend to reflect the CSIRT’s funding source. The most common constraints are determined by nation, geography, political divisions (e.g., government departments), technical specifications (e.g., use of a specific operating system), the organisation (e.g., within a given corporation or company), the network service provider (e.g., connection to a specific network), or contracts (e.g., the customers of a fee-for-service team) (Ruefle et al 2013).

Understanding the CSIRT's constituency will help focus their needs, the assets that need to be secured, and the requirements for the CSIRT. This information will, thus, help the team figure out what services it can offer and what hierarchical model will fit the required services delivery (Ruefle et al 2013).

Characterizing the CSIRT's constituency will likewise help scope the team's activity when it gets to be operational. It will help figure out what demands the team will handle and what solicitations will be passed on to different CSIRTs or other significant parties (Ruefle et al 2013).

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 like business, governmental, military, research work, IT, and have diverse structures like administration, services, organizational model, Along these lines, CSIRTs are partitioned by shape, size and function to internal, national CSIRTs, coordination centers, investigation centres, vendor's team and incidents response service. In first step, CSIRT responses to genuine security incidents and decreases attack effects (Naseri et al, 2012).

There are three situations that may occur in an organization. The first is that the CSIRT may constitute the entire security team. Secondly, the CSIRT may be totally distinct from an organization's security team. This could also be the case when there is no distinct CSIRT, but its role is served by the security team. The third option is that the security team of the organization and its CSIRT overlap. To prevent confusion there should not be too much overlap, nor should there be an area in computer security that is not covered by either a CSIRT or a security team (West-Brown et al, 2003).

CSIRT play roles like protecting the systems, detecting, diagnosing and analyzing security damages, protecting against destructive activities, cyber security incidents coordination and effective response to computer attacks. CSIRTs have different organizational models such as the available security teams, centralized

model, and distributed model, combined and coordinating model. It is better to use centralized models in small organizations while combined model acts in the best manner for large and disperse covered organizations and centers (El Naseri et al, 2012).

As specified above, it is of incredible significance that the place in the organization is hard coupled with the mission statement and constituency. For example, the hierarchical position within the organization is excessively low; it will be unthinkable for the CSIRT team to have a high demanding mission (West-Brown et al., 2003).

A CSIRT can take numerous organizational forms or structures. It can be a different element with staff allocated to perform incident handling and associated activities 100 percent of the time, or it can be a temporary team, pulled together based on expertise and roles of the members when a security incident happens. Taking part in proactive exercises, for example, security and enlightenment training, security evaluations, dissemination of security information and network system monitoring is more troublesome for temporary CSIRTs on the grounds that their regular activities are not so much identified with incident response (Ruefle et al, 2013).

2.7.4 Relationship to Other Teams

“The realm of CSIRTs is the Internet, and therefore the world. There are many constituencies around the world, and a growing number are served by a CSIRT” (West-Brown et al., 2003). 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 (West-Brown et al., 2003).

Inside the setting of CSIRTs as they exist today, there is some various tiered structure that can be seen between the diverse sorts of teams. There are teams providing services to plainly marked constituency and different teams who serve

coordination role crosswise over teams (ordinarily national or international) of CSIRTs. In any case, this structure is not a formal hierarchy of command, and by and large the structure is both unintentional and intentional. This unintentional structure is seen as an advantage, as it permits teams the adaptability to impart information rapidly and adequately to different CSIRTs that they trust and to be more careful of different teams with which there has not been as much chance to determine dependability (West-Brown et al., 2003).

Some formal hierarchies do exist, such as within the U.S. military. For example, the U.S. Army, Air Force, and Navy (ACERT/CC,12 AFCERT, and NAVCIRT, respectively), serve their own constituencies; while the U.S. Department of Defense DOD-CERT coordinates across all the U.S. military teams (West-Brown et al., 2003).

2.7.5 CSIRT Services

The CSIRT service is one of the derivatives of mission statement of a CSIRT. The services offered by a team are the methods used to carry out the team's mission and are usually provided to the team's constituency (West-Brown et al., 2003). CSIRTs around the world may not provide the same set of services. The services provided rely on upon the needs of the constituency, the know-how available, and the funding and assets allocated. CSIRTs ought to strive to pick a little set of services that are most required and guarantee they are operational before growing. One of the major concerning issues a team can have is to attempt to offer many services at once parties (Ruefle et al, 2013). There are many services that a CSIRT can choose to offer. Each CSIRT is different and provides services based on the mission, purpose, and constituency of the team. Providing an incident handling service is the only prerequisite to be considered a CSIRT (Ruefle et al, 2013). The services that a CSIRT could provide to its constituency can be characterized in reactive services, proactive services and security quality management (CERT C/C, 2005). In the following sections, we are going to discuss these types of services that we can consider as the functions of CSIRTs. Figure 2.4 shows the list of the CSIRT services.

- Reactive services

These services are triggered by an event or request, such as a report of a compromised host, wide-spreading malicious code, software vulnerability, or something that was identified by an intrusion detection or logging system. Reactive services are the core component of CSIRT work (Ruefle et al 2013). Reactive services are services that are provided as a reaction on incidents, such as a report of a compromised host, wide-spreading malicious code, or something that was detected by an Intrusion Detection System (IDS) (CERT C/C, 2005). Reactive services include alerts and warnings, incident handling, vulnerability handling and artifact handling (West-Brown et al., 2003). Incident handling includes receiving, triaging, and responding to requests and reports, and analyzing incidents and events (West-Brown et al., 2003). Triageing is the sorting, categorizing and prioritizing of incoming incident reports or other CSIRT requests (Killcrece et al., 2003).

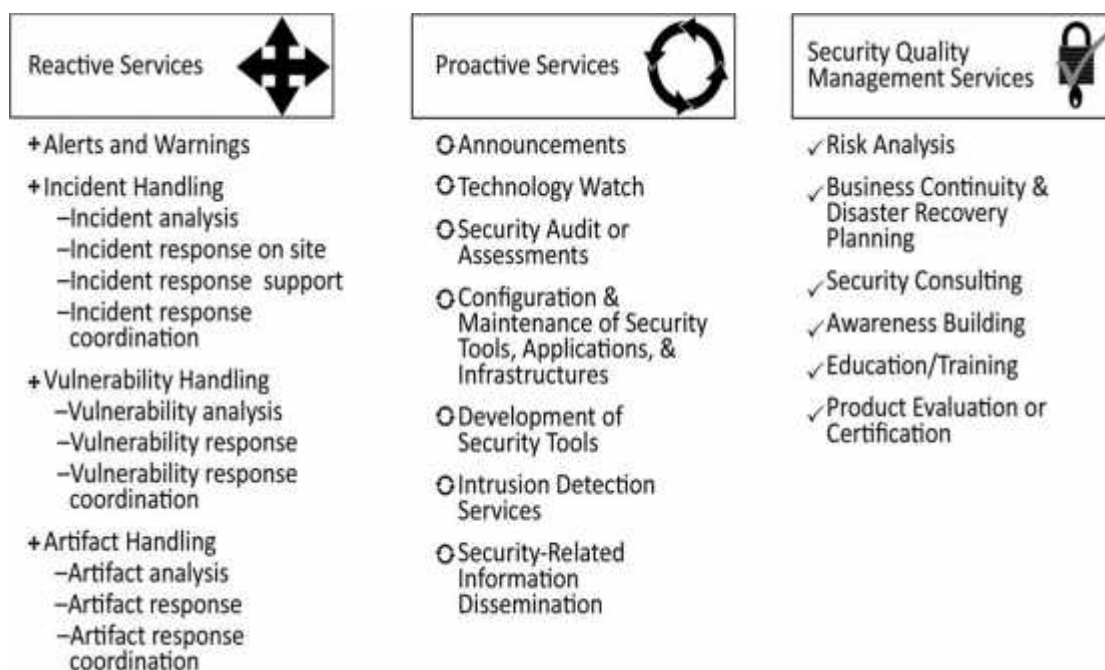


FIGURE 2.5 CSIRT Services list by Ruefle et al (2013)

- Proactive services

These services provide assistance and information to help prepare, protect, and secure constituent systems in anticipation of attacks, problems, or events. Performance of these services will directly reduce the number of incidents in the future (Ruefle et al, 2013). These proactive services try to prevent incidents, and are designed to improve the infrastructure and security processes of the constituency before any incident or even occurs or is detected (CERTC/C, 2005). Proactive services are services such as, technology watch, security audit or assessment, announcements, configuration and maintenance of security tools, development of security tools, intrusion detection services and security related information dissemination.

- Security quality management

Next to the proactive and reactive services, a CSIRT may also provide security quality management services. 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. On the off chance that the CSIRT performs or helps with these services, the CSIRT's perspective and expertise can give understanding to help enhance the general security of the organization and identify threats, and systems shortcomings. These services are by and large proactive yet help by reducing the number of occurrence of incidents (Ruefle et al, 2013). These services are designed to improve the overall security of an organization (CERT C/C, 2005). The aim at incorporating feedback as well as lessons learned based on knowledge gained by responding to incidents, vulnerabilities and attacks (West-Brown et al., 2003). Security Quality Management services include risk analysis, business continuity and disaster recovery planning, security consulting, awareness building, education and training (CERT C/C, 2005).

It should be perceived that a CSIRT ought to take a peek at performing just those functions that fit its mission and purpose. Not all these services are required to be provided by any team. Rather the CSIRT ought to pick a little set of services to at

first provide and afterward become as resources, demand, and need increase (Ruefle et al, 2013).

2.7.6 Quality Assurance

Next to CSIRT Services, another derivative of CSIRT mission is Security Quality Assurance. Quality is an aspect that is rather difficult to measure. Agreements have to be made with the constituency, on the level of quality provided. These agreements may vary from “best effort” to well-defined service level agreements. It is important that the criteria used to judge the quality on are easily measurable (West-Brown et al., 2003). Having a quality assurance system is important, since a lack of quality assurance results in inconsistencies in the service provided, services that do not fulfill their purpose, and inappropriate use of staff resources (West-Brown et al., 2003). A Quality Assurance system consists of three parts: definition of a quality system, checks and balances. The definition determines the quality parameters that can be used to estimate the quality level. These parameters are then checked for their value within the CSIRT, and feedback will be fed into the system to balance the quality (West-Brown et al., 2003)

2.7.7 Policies and Procedures

Another derivative of internal components of CSIRT framework is policy. “All services and CSIRT functions should be supported by well-defined policies and procedures” (Ruefle et al, 2013). Policies can be regarded as 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, like how to deal with media (West-Brown et al., 2003). Procedures for how the policies of the CSIRT can be conducted should also be put in place. After the CSIRT is established, the organisation should establish the essential policies, procedures, or process guidance. The organisation will not be able to create them all before the team is implemented, but it should create the key pieces. Specifically, the incident management plan and any supporting concept of operations

(CONOPS) or charter that defines the purpose and operation of the team should be in place, approved by management, and disseminated to the constituency.

2.8 CSIRT FUNDING AND SUPPORT

It is must for any new forming and existing CSIRT to have the backing and support of senior management in the parent organization (e.g., the corporate security officer, head of information technology, board of directors, or equivalent). Without such backing the CSIRT will struggle to obtain recognition and resources (West-Brown et al., 2003). This signifies the commitment of stakeholders to 'buy into' the decision of forming the CSIRT, that is, to agree to give it support both monetary and otherwise. It is imperative for CSIRT to a have full support of management (Ruefle et al, 2013). One of the kinds of support that is expected for any CSIRT to get from the stakeholders after official endorsement is fund. Fund is critical and center to forming CSIRT; that is to say no funding, no 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 also personnel costs (salaries and benefits). Once the CSIRT is operational, there will be continuing sustainment costs, both for operational expenditures (ongoing facilities maintenance, support of equipment, upgrades, supplies, travel) and personnel costs (raises, professional development and training) (Killcrece, 2003). (Ruefle et al, 2013), has described different funding strategies for CSIRT. Some of the several funding strategies are shown in the Table 2.1 below.

From the table 2.1 above, it can be deduced that CSIRTs have different funding strategies base on their model. The table shows different nations and organizations using different funding plans. This doesn't mean that all nations and organizations will use same strategies mentioned above as no any two nations or organizations have the same demographic features. In addition, mission and services may not be the same.

TABLE 2.1 CSIRT Funding Strategies

S/N	Funding Sources	CSIRT Name
1	Membership Subscriptions	AusCERT [Australia]
2	Contract or fee-based services	CanCERT [Canada], MyCERTs [Malaysia]
3	Government Sponsorship	FedCIRC
4	Academic or Research	CERT-NL, SURFnet, NORDUnet
5	Parent organization	CERT
6	Government and Private	FIRST
7	Contract Services	CERT/CC
8	Government	IBM, ISS, CISCO
		US-CERT (USA)

2.9 REVIEW OF CSIRTs ORGANIZATIONAL MODELS

Organizational model has long been described as a mechanism through which effort is integrated through the coordination and control of activities (O'Neill et al, 2001). Organizational structure can be viewed as the way responsibility and power are allocated inside the organization and work procedures are carried out by organizational members. Organizational structure is the organization's internal pattern of relationships, authority, and communication. Similarly, define organizational structure as “the network of relationships and roles existing throughout the organization” (Teixeira et al, 2013). An organizational model, is a hierarchical structure, defines framework through its system, including lines of power, communications, obligations and asset allocations. A model of organization is also determined by the organization's objectives and serves as the connection in which processes work and business is carried out. The perfect model relies on upon the way of the business and the difficulties it confronts. Thus, the organizational model decides the number of employees required and their obliged expertise sets.

Killcrece et al, 2003 defines CSIRT organizational model as CSIRT's place in the organization—that is, its organizational position and reporting relationships. It

may also describe the physical and geographic location of the team. Ruefle et al, 2013 has categorized CSIRT model base on the size and geographical distribution. Five models were described by Robin Ruefle et al, 2013 namely:

- (1) Security team;
- (2) Internal distributed team;
- (3) Internal centralized team;
- (4) Combined distributed and centralized team;
- (5) Coordinating CSIRT.

These models would be discussed briefly later in this chapter.

- (1) Security team

This is a model where by an organisation has no recognized CSIRT. So in this situation system and network administrators usually perform incident handling activities as part of their other duties (Ruefle et al, 2013).

In this kind of arrangement maintaining responsibility for incident response at the local system and network administrator level has several consequences. This confined strategy does not allow the security team to collect security data across the organisation, analyse that data to identify current and future threats, and alert the organisation and distribute preventive and remedial actions (Ruefle et al, 2013).

The advantage of this model is that no additional resources is required for handling incident responses as existing staff and equipment will be used; is very suitable for small organization. The disadvantage of this model is that it lacks information sharing and organized mechanism for managing and reporting incidents.

- (2) Internal distributed team

In this model, existing staff provide a virtual, distributed CSIRT. A manager or team lead oversees and coordinates activities affecting the virtual team. Individuals across

the organisation are identified as the appropriate points of contact for particular functional areas or divisions, based on their experience and expertise with various operating-system platforms, technologies, and applications. These staff members may perform incident handling on a full-time or part-time basis. Such a model also allows information to flow across the organisation, including incident reports and response strategies (Ruefle et al, 2013).

Effective management and coordination of this virtual organisation may become a problem. It will take a strong, central leader to develop a team spirit and keep all sites operating according to general standards (Ruefle et al, 2013). The advantage of this model is that no additional resources is required for handling incident responses as existing staff and equipment will be used; is very suitable for small organization; well organized information and mechanism for managing and reporting incidents.

The disadvantage of this model is that very difficult to manage as members will be reporting to two different managers, difficult for the team members to prioritize activities and neither effective in small organization nor for large.

(3) Internal centralized team

In this model, a fully staffed, dedicated CSIRT is given the resources to provide the services outlined in its mission. All team members spend 100 percent of their time working for the CSIRT. The team leader reports directly to high-level management, and the team is centrally located. This dedicated CSIRT model provides a very stable structure for building manageable, predictable incident handling capabilities (Ruefle et al, 2013).

The strength of this model is that there is a stable central manageable and predictable incident handling capabilities. The main weakness of the internal centralized CSIRT is that the incident handling capability is separate and distinct from the operational units (Ruefle et al, 2013). This model requires that a new, specialized

unit be created, staffed, and integrated into the organisation's operations (Ruefle et al, 2013).

(4) Combined distributed and centralized team

This model attempted to combine the best features of the distributed model with the best features of the centralized model. It take full advantage of the utilization of existing staff in strategic locations throughout the organisation with the centrally located coordinating capabilities of the dedicated team to provide a broader understanding of the security threats and activity affecting the constituency (Ruefle et al, 2013).

The advantage of this model is that it provides a stable core of full-time CSIRT professionals along with a network of part-time affiliated members from the operating units. This arrangement can increase acceptance or buy-in from all parts of the organisation (Ruefle et al, 2013).

The disadvantage of this model is that two systems must be managed and coordinated. If this is not handled well, the dedicated team will be disconnected from the rest of the organisation and the distributed component ineffectual and this model doesn't necessarily work well for small organisations, as they do not usually have the needed expertise distributed across the organisation (Ruefle et al, 2013).

(5) Coordinating CSIRT

A CSIRT can likewise be model as coordinating center instead of a direct incident response service. The coordinating CSIRT assists organize response efforts across topographically scattered CSIRTs or even across business units that have their own CSIRTs. These scattered groups execute the main incident response methods and mitigations plans. The coordinating CSIRT creates incidents statistics and reports from all territories to find the general security position of the organization and its weakness to attack. It likewise handles information consolidation so that a precise

picture of incident activity over the organization can be communicated as required (Ruefle et al, 2013).

It major responsibilities as coordinating center is to coordinate responses to security breaches, intruder activity and proffer solutions to security problems and well as report to it constituency or other CSIRTs (Ruefle et al, 2013). This model is best for a country, state or province.

The advantage of this model is that there is centralized and proper reporting mechanisms, dedicated staff and well organized policies and procedures for handling incidents. The disadvantage of this model is that in large scattered setup coordination may be difficult and can be impacted by the parent organization.

TABLE 2.2 Critical Review of CSIRT Organizational Models

Models	Security Team	Internal Distributed Team	Internal Centralized Team	Combined Distributed & Centralized Team	Coordinating CSIRT
Constituency	Small organization with specific needs	This is found in large, distributed organizations such as multinational corporations, government and educational institutions	Can be used by both small and large organization	Support very large distributed organizations or constituencies	This model coordinate incident handling activities for organization that shares same characteristics
Organizational Structure	No real organizational structure	The structure depend on the size of the parent organization	The team is centrally located at one physical site, close to their upper-level manager.	It merges the characteristics of centralized and distributed	Centralized dedicated team

Triage	There is no centralized mechanism for sorting and reporting	Team members at the distributed site do the initial triage of the requests and reports	In this model triage is central and very important for sorting and reporting	It merges the two depending on where the report come from	This function is central to the operation of coordinating CSIRT
Services	Recovering and repairing damaged systems and networks. Other incident services are done at the surface	There is organized management and issues are treated deeply (alerts, analysis and response)	There is organized management and issues are treated deeply (alerts, analysis and response)	Combined the two with a centrally dedicated facilities for incident handling	Deep Coordinating of alerts, analysis and response
Impact on Security Quality	Very minimal as the team members may have enough time to attend to some issues that does directly relate to their job	This depends on the expertise and available resources at distributed team	This positively impact the system as the staff have dedicated time and resources to handle security	With distributed team at the lower level and dedicated team at centralized level the impact is high	This model does not directly impact the system as it is limited to producing guide lines

			issues		
Resources	No additional Staff, equipment and infrastructure is required	This has small centralized management and team members, existing infrastructure can be used	The management is centralized with dedicated staff, equipment and infrastructure	Staff are devoted to duties 100% , separate equipment and infrastructure are also needed	Staff are devoted to duties 100% , separate equipment and infrastructure are also needed
Limitation	This model lacks coordinating in incident handling, reporting and analysis	Due to the disperse nature of the staff making to work as a whole would create problem	This will pose problem in a large organization with diverse services	Building the diapered team and making them communicate efficiently with the center	Difficulty of building effective relationships with all entities in the constituency and gaining their trust so that incidents are reported and recommended mitigation and prevention strategies are followed

2.10 EXISTING NATIONAL RESEARCH AND EDUCATION NETWORK CSIRT (NREN CSIRT)

A CSIRT which is officially launched to provide a platform for National Research and Education Network of a particular country or region to respond and handle cyber security incidents is called NREN CSIRT. The primary objective of NREN CSIRT is to provide a platform which enables National academic networks to respond effectively to information security incidents – proactively, during or immediately after an incident is discovered, as well as in a preventive fashion. It will also serve as a platform for collaboration and sharing information security incidents and research. There are many NREN CSIRT but for the sake of review only three will be discussed. They are SURFnet (Netherlands NREN), UM (Universiteit Maastricht) and NORDUNet (Nordic countries, Finland, Denmark, Iceland, Norway and Sweden Research networks) certs.

(1) SURFnet CERT

Netherlands National Research and Education computer Emergency Response Team was established to provide member institutes with security-incident support 24 hours a day, seven days a week. SURFcert also uses tools and other resources to optimize security within institutions themselves. Institutes report security breaches (incidents) to SURFcert, who will keep the institute informed of the progress of the incident, and provide any necessary advice on how to resolve it. SURFcert has been accredited by FIRST.

(2) UM CERT

The primary objective of UM-CERT (Universiteit Maastricht) is to provide a platform which enables UM (Universiteit Maastricht) to respond effectively to information security incidents – proactively, during or immediately after an incident is discovered, as well as in a preventive fashion. Activities are not only corrective in nature but may sometimes also focus on the collection of evidence. UM-CERT's target group is Universiteit Maastricht as well as all other persons and bodies connected to the MAASnet institutional network. Although UM-CERT's primary focus is on the

central UM infrastructure and thereby the continuity of operational activities, the activities also include all workstations, users and information (systems) which utilize UM facilities in any way whatsoever.

(3) NORDUNet CERT

NORDUnet CERT performs security incident handling in cooperation with the Nordic national research networks. It was established in the 1990 in Denmark to provide cyber security incident handling and response for Nordic countries, Finland, Denmark, Iceland, Norway and Sweden Research networks. This concludes that there are already existing CSIRT within the National Research and Education Network, which further justify the title of this study and justification for needs of the CSIRT within the NgREN.

2.11 SUMMARY

This chapter discussed the National Research Networks and how these networks helped in improving collaboration and sharing of information. In addition, the chapter discussed a generic CSIRT framework that aimed at helping new forming teams in developing and implementing a more effective way of handling cyber security incidents. It further, made effort to describe how this framework can be applied within an organization to handle cyber security incidents. In order to utilize this framework, an adoption was made to the framework using qualitative method of interview to collect data. The framework that will be created will consist of all the required components and derivatives of CSIRT framework by West Brown et al 2003, to give a more detailed idea of how NgREN might handle security incident

CHAPTER III

METHODOLOGY

3.1 INTRODUCTION

This chapter discoursed on how the research was conducted and the methodology used in achieving the final result. It further describes the methods and techniques used and reasons for choosing the methods.

3.2 RESEARCH METHODOLOGY

Research methodology is a science of studying how research is to be conducted. Basically, it is the procedures by which researchers go about their work of describing, explaining and predicting phenomena (Rajasekar et al, 2013). Research methodology is considered as the central point for the researchers to achieve their objectives. This is because it gives direction on how to systematically solve the research problem. It also shows what tools and techniques to use to achieve the desire goals. Researchers used many research methodologies to achieve their desire targets (Rajasekar et al, 2013). The basic and applied researches can be quantitative or qualitative or even both. Quantitative research is based on the measurement of quantity or amount. While qualitative research is concerned with qualitative phenomenon involving quality (Rajasekar et al, 2013). (Fortier 2012), used the combination of both qualitative and quantitative methods to achieve result. In this methodology the researcher used opened and closed ended questions and observation to conduct his research.

Dehlaw et al. (2013) used the explanatory case study methodology to answer research questions based on accessible text sources. (Newmeyer, 2014) used qualitative methodology based on case study approach in which the researcher answered research questions via case study by interviewing different interviewees. (Sen, 2001) used focused synthesis method for his master thesis to find solution to the research questions of his study. (Naseri et al, 2012) used a qualitative methodology to get the needs and requirements by extracting information from meeting sessions with stakeholders and surveyed from experimental documents to propose a CSIRT model for the Telecommunication Company in a Province of Iran. The methodology for this research was adopted from (El Naseri et al, 2012) using qualitative case study based on focused synthesis (archival data, published and unpolished articles, literature review and personal experience) and interview/meeting session to provide solution to the research questions mentioned in section 1.7. In addition to this, the study also used the concept from (West-Brown et al, 2003, Killcrece et al, 2003, Ruefle et al, 2013) for the proposition of CSIRT framework for the Nigerian Research and Education Network.

3.2.1 Qualitative Research Method

A qualitative research method based on relatively few participants was used for this research. Instead of using a quantitative approach by using questionnaires to gather information from a large number of participants, the researcher used qualitative because it allow detailed information from selected participants. The qualitative research method allowed us to perform a rich and detailed analysis (Hove et al, 2013).

3.2.2 Qualitative Interview

Qualitative interviews was used as part of this research because it is a well-known and dominant tool for data collection in qualitative research (Myers et al, 2007). The main objective of qualitative interviews is to allow the research topic to be seen and understand from the interviewees' perspective (Cassell et al, 2004). To realize this objective, a semi structured open questions that centered on a specific condition and familiarities were constructed. The interview guide and questions were

modified from (Kennedy, 2006, Mulligan, 2012). The table below shows the questions and how they met the requirement of this study.

TABLE 3.1 Research Interview Questions

Question	Targets	Source
Q1	This will enable us to test NgREN familiarity with CSIRT organization	Kennedy, 2006, Mulligan, 2012
Q2	We want to know the commitment of NgREN management towards creating CSIRT	
Q3	We want to know about organizational structure of NgREN, financial support base and its readiness to finance the CSIRT	
Q4	The researcher wants to know the entities to be served by the CSIRT when it eventually comes up	
Q5	This will enable me to know whether NgREN has any existing structures for security incident handling	
Q6	We want to know the predominant and disturbing cyber threats within NgREN.	
Q7	This will enable us to know whether there is an existing detecting and reporting mechanism for cyber threats in the NgREN	
Q8	We want to know whether there is a cyber security handling mechanism within the NgREN and who is responsible	
Q9	This is just a broad question to Q5, Q6, Q7 & Q8	
Q10	We want to know whether there is a unit already responsible for handling cyber security	
Q11	This is just a follow-up question	
Q12	Here we discussed the major components of NgREN with stakeholders and what is expected from them specifically the mission statement definition	

3.2.3 Focused Synthesis

The method of focused synthesis has been selected to support the case study method. The focused synthesis which is rooted in a policy research methodology, calls for the use of different sources of data to sustain the inquiry of policy problem. Focused

synthesis involves a critical reading, analysis of different informational sources around the same issue (Silvestre, 2008).

This research utilized the method of focused synthesis. Thus different data sources were collected and analyzed. These included archival data, literature review, published and unpublished articles and interviews/meeting sessions with NgREN stakeholders.

3.2.4 Participants

The participants of this study are CEO and stakeholders of the Nigerian Research and Education Network (NgREN). They included CEO and technical officers (Network admins, Systems admins and Security analyst). These participants have many years of experience and were involved in different level of NgREN management. Their core activities belong to areas of management and information security. This could indicate that they are experienced and well equipped to be interviewed on information security incidents management. It is interesting to examine how such assumed experienced staff perform incident management and what challenges they face within the NgREN. Additionally, the participating staffs have quite different technical and managerial expertise, which we believed could lead to interesting findings.

3.2.5 Documents Study

To complement information gathered from interviews and meetings, the researcher studied relevant academic literature, standards, frameworks, models and organization-specific documents such as policies and plans. This enabled us to know more frameworks, models, procedures, plans and current organizational practice of cyber security incident response management.

3.3 RESEARCH METHODOLOGY PHASES

The research was conducted with the aim of achieving the objectives stated in section 1.6 by using qualitative case study methodology based on focused synthesis and

qualitative interview and meeting session with the relevant stakeholders of Nigerian Research and Education Network. Sections 3.2.4 to 3.2.5 have elaborated more on these data collection strategies. The methodology of this study was divided in phases to enable us efficiently achieve the objectives of the study. Table 3.2 shows the phases of the study methodology.

Table 3.2 research methodology phases

Research objective (RO)	Research question (RQ)	Phase
RO 1	RQ 1	Phase 1
RO 2	RQ 2	Phase 2
RO 3	RQ 3	Phase 3
RO 4	RQ 4	Phase 4

3.3.1 Literature Analysis

In this phase different literatures were reviewed (published and unpublished articles) to explore CSIRT framework and models. This enabled us to answer our first research question and thereby achieving the first objective, which is the critical review on cyber security incident response management CSIRT framework and existing models. Literature review at chapter two was used in achieving the first research question and objective respectively of this study. The phase was beneficial to this study as it allowed us to know more about frameworks, models, procedures, plans and current organizational practice of cyber security incident response management. Understanding these made us asked relevant questions during meeting session with NgREN stakeholders. In addition to this, this phase made us to know components of CSIRT framework and its derivatives and as well as other models and their shortcomings.

3.3.2 Cyber Security Incident Analysis in NgREN

Here interview and documents assessment was conducted to answer the second research question and objective of this study that is to explore how Nigerian Research

and Education Network manage cyber security incidents. To achieve this objective archival data and interview guide to answer research question related to this second objective was used.

During the interview with Nigerian Research and Education Network stakeholders, questions were asked in accordance with sections 3.2.2 and 3.2.4 above. The interview guide was modified from (Kennedy, 2006).

The benefit of this phase was to ensure that all necessary information was gotten and for this an interview guide was used. The interview guide worked as an incomplete script and states the main goals for our research as well as the main research questions and topics for the interview. The questions were not asked in order as they are appeared on the guide during the meeting. This made follow-up questions to be asked for more elaboration. The participants in the meeting are being seen as members of the research rather than just answering questions (Hove et al, 2013).

The interview and meeting were performed face-to-face and voice recorded and via email. This is because when interview were conducted face-to-face helped build trust with participants and thus better and elaborate answer (Hove et al, 2013).

This made us to have an in depth investigation to issues on how cyber security incident management is being carried at NgREN. Discover how stakeholders within the NgREN think and feel about the concept of cyber security incident management. And finally, this made us to investigate the effectiveness and usefulness of CSIRT and its services to organization like NgREN. Detailed interview questions can found at appendix II.

3.3.3 Proposition of the Framework

This phase answered the third research question and objective of this study that is the proposition of CSIRT conceptual framework for the NgREN. The proposed framework was based on the findings of the two phases above. This objective was

achieved by adopting and customizing CSIRT framework by (West-Brown et al, 2003) which was later reviewed and used by (Ruefle et al, 2013) because it is more generic and less complicated (Ruefle et al, 2013). The essence was to use the discussion in chapter two and interviews and meeting sessions in phase II of this methodology to achieve our third objective.

3.3.4 Validating the Framework

In this phase the last research question was answered and the final objective of this study that is validating and refining the proposed CSIRT framework for its applicability to the NgREN. This was done by sharing the proposed framework with experts in the field of cyber security incident response from CSM (Cyber Security Malaysia) and the user organization (NgREN) for their inputs. This was done to allow the framework to be criticized for refinement. The experts would provide open ended comments. These experts were chosen based on their experience and current engagement. They included CEO and Head of cyber security training and development from cyber security Malaysia. These experts have many years of experience and were involved in either NgREN management or cyber security incident response. Their core activities belong to the field of NREN management and information security. This could show that they are well experienced and have the necessary expertise to serve as expert in validating this framework. Furthermore, the experts have quite different technical and managerial expertise, which we believed could lead to interesting improvements in the framework.

3.4 SUMMARY

In this chapter the methodology for this study was discussed and the reason for the choice of such methodology and techniques. In addition to this, the methodology of this study was divided in phases and explained how each of the phases was used in accomplishing the research objectives of this study.

CHAPTER IV

RESULTS AND DISCUSSION

4.1 INTRODUCTION

This chapter focused on result and discussion on the achievement of the objectives described in section 1.6 and methodology phases in achieving the objectives in section 3.3. The objectives are as follows:

- To conduct critical review on cyber security incident response management;
- To propose an efficient CSIRT framework for the NgREN; and
- To validate and refine the proposed framework.

These objectives are put in phases to allow the researcher to easily achieve the main objectives of the study. This was shown in chapter 3. This chapter will discuss each of these objectives as it relates to achieving the final objective. Finally, the literature and data gathered at NgREN will be used to propose a framework for the NgREN.

Now that the different literature about CSIRT were reviewed and interview has been conducted, it is time to start thinking of the way this information will be used to create a framework for handling cyber security incidents in NgREN. To start, the researcher takes each of the phases and elaborates.

4.2 LITERATURE ANALYSIS

This phase attempts to achieve the first objective of this study that is **“To conduct critical review on cyber security incident response management”**. This phase allowed us to have an insight in to CSIRT framework, models, procedures, plans and current organizational practice of cyber security incident response management. It further made us to understand relevant questions asked during meeting session with NgREN stakeholders. In addition to this, we are able to have a deep insight in to the components of CSIRT framework and its derivatives and as well as other models and their shortcomings.

4.2.1 Analysis and Finding

It was found in this phase that the evolution and development of CSIRT was dated back in the year 1988, when a computer worm named after a 23 year old college student Morris was discovered. This worm was programmed to spread itself in a computer network from machine to machine by abusing different vulnerabilities. Most of the infected systems at that time were email systems and Internet backbone servers. For this reason many Internet sites were removed from the network and this resulted to total outage of Internet (Ruefle et al 2013). Section 2.5.2 of chapter 2 of this study can be referred to for detailed information on the history of CSIRT. This worm made US agencies to rethink about information security. In response to this worm SEI (Software Engineering Institute) of Carnegie Mellon University was funded by DARPA to create coordination center for the handling of cyber security incident, that center was named CERT/CC. Since then, many CSIRTs were created ranging from organizational to national and international dimensions for speedier response to security incidents.

It further explored that CSIRT framework has four major components that is mission, constituency, place in organization and its relationship to other CSIRTs. All these components must be clearly defined and understood by the CSIRT planner before announcing the CSIRT. Besides the components there are three major derivatives which depend on the CSIRT mission that is services, quality assurance and

policies. Understanding mission of the CSIRT will clearly defined what the CSIRT is all out to achieve. Clearly, mission statement is rudimentary to empower the CSIRT to launch services and quality system, including the nature and scope of services to be launched, the description of its strategies and techniques, and the nature of service together with the description of the constituency, this service and quality system drives and limits all CSIRT exercises. These components and derivatives are explained in detail in section 2.7 of chapter 2 of this study.

In addition, funding and management support are needed for any CSIRT to function. That is to say prior to planning a CSIRT there must be a management buy-in from the CSIRT planners before embarking to planning otherwise the CSIRT will fail. This is because continuous funding is very critical for any CSIRT to exist. Section 2.8 of chapter 2 has this in detail.

Another important thing to consider when creating a CSIRT is the organizational model on how information flows within the CSIRT team. CSIRTs are organized either as internal, national CSIRTs, coordination centers, analysis centers, manufacturer's team and incidents response service. These models are discussed in depth in section 2.9 of chapter 2 in this study. It is very critical at this juncture to select the best model that can fit in to our organization as not each model is suitable for every organization. Therefore, extreme care must be taken when selecting organizational model for a CSIRT.

Finally, there are number of CSIRTs developed for the National Research and Education Network (NREN) since the evolution of CSIRT in 1988. These CSIRTs are meant to provide services within the academic networks for the protection of critical assets and infrastructure. All NREN CSIRTs have the same role in their respective area but slightly different in terms of providing services and constituency, expertise and nature of cyber-attacks. In section 2.10 of chapter 2 of this study three (3) NREN CSIRTs were discussed, they are SURFnet CERT, UM CERT and NORDUnet CERT.

4.3 CYBER SECURITY INCIDENT AT NGREN

This phase was meant to achieve the first objective of this study that is **“To conduct critical review on cyber security incident response management”**. This was achieved based on the interview/meeting and archival document analysis conducted.

4.3.1 Data Analysis and Finding

The following are determined during the meeting sessions with stakeholders. A complete list of all the questions asked the stakeholders can be found in Appendix II. The following describes the detailed patterns and the interpretations of the answers provided by the NgREN stakeholders for each interview question during our meeting.

Q1. The finding here is that the NgREN knew much about CSIRT but lack the capacity to develop the structure.

Q2. From the response of this question it is clear that NgREN has the desire to have the CSIRT in place for improve security coordination within the network. In line with section 2.8 of chapter II, this response is useful in determining the commitment and political will of NgREN to have the CSIRT.

Q3. This response also corroborate with 2.8 which is about financial support base. NgREN has very good financial backing from the Federal Ministry of Communication via (NCC- National Communication Commission, NITDA- National Information Technology Development Agency) and PTDF- Petroleum Technology Development Fund. These are in addition to direct funding from member institutions, which is the most sustainable funding source for the network. Q2 and Q3 are very important in setting up CSIRT, as no any organization can setup CSIRT without the top level management support and funding.

Q4. Taking from above, NgREN is a bounded constituency, as was defined in section 2.7.2; it provides its services only to the organizations explicitly mentioned

above. Furthermore, the Network team has full authority on its constituency; the members of the NgREN are allowed to disconnect computers from the network when necessary. Nevertheless, to do this, they need the support of the Network Operation Center, making it an indirect authority, described in section 2.7.2. According to Ruefle et al 2013, understanding the CSIRT's constituency will help focus their needs, the assets that need to be secured, and the requirements for the CSIRT. This information will, thus, help the team figure out what services it can offer and what hierarchical model will fit the required services delivery. From this, it can be concluded that the NgREN has a clear understanding of its constituency and met the requirement of one of the cardinal components of CSIRT framework. For this reason another objective and research question in phase I and II have been answered.

Q5. The finding here is that NgREN and connected network points solely depends on network and systems administrators for handling cyber security incidents. This shows some responsibility and commitment to handling cyber security issues. This will help in answering research question and objective of this phase. However, these staff will be overwhelmed with many activities, so there is need for improvement. This was broadly discussed in section 2.9.

Q6. As it is now NgREN lacks the capacity to know much about the causes of cyber security incident. The predominant cause of NgREN cyber security incident, according to the greater number of members in the meeting, was “cyber criminals that infringe copyrights.” Another cause of cyber security incident is the misconfigured devices and applications. The next most predominant cause given was “viruses and malwares.” Lack of user education and coordination in cyber security is another most important predominant cause of cyber security incident.

The NgREN definition of cyber security incident presented a different variety of understanding, approaches, and terms. In a large network like NgREN or a large security incident that covers multiple network points, a common understanding by these different network points, regarding how to plan for, respond to, or recover from the cyber security incident can be very important in a time-dependent situation. Furthermore, common approaches and terms are also beneficial when dealing with the

complex cyber security incidents within the cyberspace. This has contradicted the objective of number three which is about having a well-coordinated team to handle cyber security incident. Since this has contradicted the objective there is need for improvement.

Q7. The finding here shows that NgREN has no formal hierarchies, methods, procedures and policies for detecting and reporting cyber security incidents. This indicates NgREN is doing cyber security incident reporting with no formal policies and procedures. For this, there is need for centralized and publicized policies and procedures for handling and reporting security incidents

Q8. This question was posed as how does NgREN respond to Cyber Security Incident?

The predominant answer to this question was the utilization of NgREN NOC staff and individual institutions NOC admins. There is no information-sharing and incident analysis center among and in the NgREN Network.

Q9. This question was asked as how NgREN manages cyber security issues.

This is a direct question and the aim is to answer research question number two. But it was broken down to three questions for a more elaborate answer. This is shown in Q5, Q8 and Q10. The findings here shows there is no formal Authorized and Published Plans, Policies, and Procedures: Authorized and published plans, policies, and procedures and their implementation enable the strategic transfer of information for a cyber-incident to the decision makers for further action.

Q10. The NgREN believes that NOC is the one responsible for handling cyber security incidents at the center. At the same time, each member institution is responsible for handling cases within the institution and reporting same to the NOC. This shows that there is that commitment to having a unit responsible for cyber security incident handling. As mentioned in Q5, this may not be the best option going by the reasons stated in Q5 and section 2.9 of chapter II. Having one team solely

responsible for all cyber security incidents could be the best option with regard to efficiency, timeliness of response and well-built relationships and processes. For this reason we need to improve on this.

Q11. The most answers to this question showed that the head of NOC (that is AGM Network operations) is the key NgREN individual to be contacted for NgREN cyber security incident.

Q12. What it is you want the NgREN CSIRT to achieve? (Mission statement and objectives in respect to Cyber Security Incident)

To provide a platform for academic and research organizations in Nigeria connected to NgREN, to manage cyber security issues and their mitigation, Network Security Monitoring, improvement of security by identification of risks and threats and promoting computer security knowledge among NgREN members. In addition, the NgREN CSIRT needs to build trust with other global partners such as other RENs. To do this, they must see NgREN to be secured and trusted for free exchange of information to happen.

In line with the section 2.6.1 above and the mission of the NgREN, which is about providing efficient services and collaboration between member organizations of the NgREN, the response to this question further corroborate with what the team will focus as its core activities and this has not gone contrary to the overall mission of the NgREN. This can also be supported with the saying that if the team is housed inside a superior organization or is supported from an outside body, the CSIRT mission statement must supplement the missions of those organizations (West-Brown et al., 2003). It also provides a basic understanding of what the team will try to achieve. Since this is in support of the NgREN strategic mission statement and section 2.7.1 above, CSIRT framework mission statement, this has answered one of the research questions that asked about proposing of CSIRT framework where mission statement is the core.

Who do you want the NgREN CSIRT to serve? (Constituency: constituency type, members and relationship with the constituency)

After interviewing the NgREN stakeholders the constituency of the NgREN was described as those organizations that are connected to NgREN. These organizations are Higher Education institutions and many research organizations in Nigeria. Within the NgREN NOC there is Security Unit.

Taking from above, NgREN is a bounded constituency, as was defined in section 2.7.2; it provides its services only to the organizations explicitly mentioned above. Furthermore, the Network team has full authority on its constituency; the members of the NgREN are allowed to disconnect computers from the network when necessary. Nevertheless, to do this, they need the support of the Network Operation Center, making it an indirect authority, described in section 2.7.2. According to (Ruefle et al, 2013), understanding the CSIRT's constituency will help focus their needs, the assets that need to be secured, and the requirements for the CSIRT. This information will, thus, help the team figure out what services it can offer and what hierarchical model will fit the required services delivery. From this, it can be concluded that the NgREN has a clear understanding of its constituency and met the requirement of one of the cardinal components of CSIRT framework. For this reason another question has been answered.

Where do you place the NgREN CSIRT? (Place in organization: position within organizational structure)

As mentioned in section 2.7.3, the place in the organization is closely put together to the way a CSIRT can do its job, and the authorities it has. From the interview and meeting with the stakeholders, NgREN relies on the input from the security team of the NOC. This is shown in figure 2 above. Here we are going to improve this by making CSIRT as a separate independent unit directly under the CEO of the NgREN.

Are you going to relate with other CERTs in terms of sharing incidents information? (Relationship to others)

As a forming CSIRT the stakeholders understood the need for them to relate with other CERTs and CSIRTs both national and international to achieve success. This is because the NgREN is a collaboration body and therefore cooperation and coordination effort is at very heart of NGREN.

4.4 PROPOSITION OF THE FRAMEWORK

In this phase we achieved the second objective of this study that is the proposition of CSIRT conceptual framework for the NgREN. The proposed framework was based on the findings of the two phases above and possible improvements where possible. This objective was achieved by adopting and customizing CSIRT framework by (West-Brown et al, 2003) which was later reviewed and used by (Ruefle et al, 2013) for the fact that it is more generic and less complicated (Ruefle et al, 2013). The essence was to use the discussion in chapter two and the results of interviews and meeting sessions in phase II of this chapter to achieve our third objective.

4.4.1 Proposed CSIRT Framework for the NgREN (NgREN-CSIRT)

As mentioned above this framework was adopted from CSIRT framework by (West-Brown et al, 2003). The framework has four major components, they are: Mission statement, Constituency, Place in organization and Relationship to other teams. In addition, the framework has three major derivatives (Services, Quality assurance and policies) derived out of the mission statement of the CSIRT. Besides these, the framework has other major supporting components they are: Support and funding, Organizational model, Reporting and Resources.

4.4.1.1 Major NgREN-CSIRT components

(1) The mission statement

The NgREN-CSIRT missions are determined by sessions with NgREN managers (This was extracted from the finding of Q12 above in this chapter) include: To provide a secured platform for member institutions in Nigeria by managing cyber security issues and their mitigation through proactive network security monitoring, identification and reporting of threats and risks as well as promoting computer security knowledge among NgREN members.

(2) Constituency

During the meeting session with the NgREN stakeholders the constituency of the NgREN was described as those organizations that are connected to NgREN. These organizations are Higher Educational institutions and research organizations in Nigeria.

Concluding from this, NgREN-CSIRT has a bounded constituency, as was defined in section 2.7.2; it provides its services only to the ones explicitly mentioned above. Within the NgREN constituency there are different entities such as:

- All Higher Educational Institutions; which serves all users connected to these academic Networks
- All Research institutes and centers; which serve all users connected to these Research Networks.

(3) Relationship to Other Teams

As a forming CSIRT the NgREN stakeholders understood the need for them to relate with other CERTs and CSIRTs both national and international to achieve success. This is because the NgREN is a collaboration body and therefore cooperation and coordination effort is at the very heart of NgREN mission. For this reason NgREN-

CSIRT would collaborate with other CSIRTs worldwide in sharing of information base on trust.

(4) Place in Organization

From the meeting with NgREN managers security incident was managed at NOC by the staff of the NOC who also doubles as Network and systems administrators. This is not an optimal and efficient organizational structure for a CSIRT with large size and diverse entities like NgREN. Here we proposed that the team should be an independent entity directly under the NgREN CEO. Sections 2.7.3, 2.8 and table 2.8 explained this in detail. Figure below shows skeletal placement of the NgREN-CSIRT within the NgREN organizational structure.

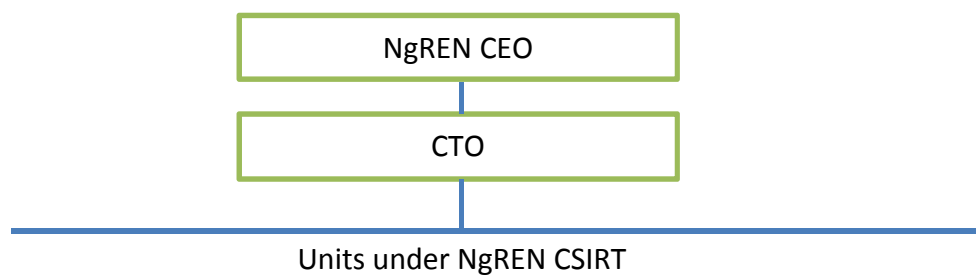


FIGURE 4.1 NgREN-CSIRT organizational placements

4.4.1.2 NgREN CSIRT organizational model

Here the research is going to focus on the organizational model or operational structure of the NgREN-CSIRT. This will involve the physical location of the NgREN-CSIRT, the place of the team in the parent organization or constituency, and how the CSIRT interacts with the rest of the constituency. Its reporting structure within the constituency and the way information flows into and out of it (Killcrece et al., 2003).

In this regard, a combined central coordination and security Team model for the NgREN-CSIRT will be proposed. In this model there will be a central dedicated team at the NgREN office and ad hoc security team at individual institutions. The central dedicated team will support the entire NgREN constituent and various security

teams while the ad hoc security team will support only its primary institution by providing direct onsite response. This structure is supported by (Killcrece et al., 2003), it is obvious that large organization with geographically dispersed constituency cannot reasonably provide direct and efficient response specifically onsite response. This assertion was corroborated earlier in chapter two, section 2.1. Therefore, in this case the security team will be bestowed the responsibility of handling and responding to incidents at their individual institutions and their normal day-to-day work of maintaining the availability and security of the local environment and infrastructure. The central team (NgREN-CSIRT) will be managed by the NgREN-CSIRT manager as overall officer in charge. Besides the manager there will be dedicated staff, equipment and infrastructure at the central site. The staffing, equipment and infrastructure will be explained later in this chapter. Figure, 4.2 and shows the proposed NgREN-CSIRT organizational model and figure 4.3 shows the expanded organizational model. While figure 4.4 shows the Security team structure. Besides these, there would be a Technical Working Group (TWG) on Security. This group will be made up of member representatives from among member institutions. One of its Terms of Reference would be to advise the NgREN Management and NgREN-CSIRT on issues of Cyber Security Incidents and handling and response.

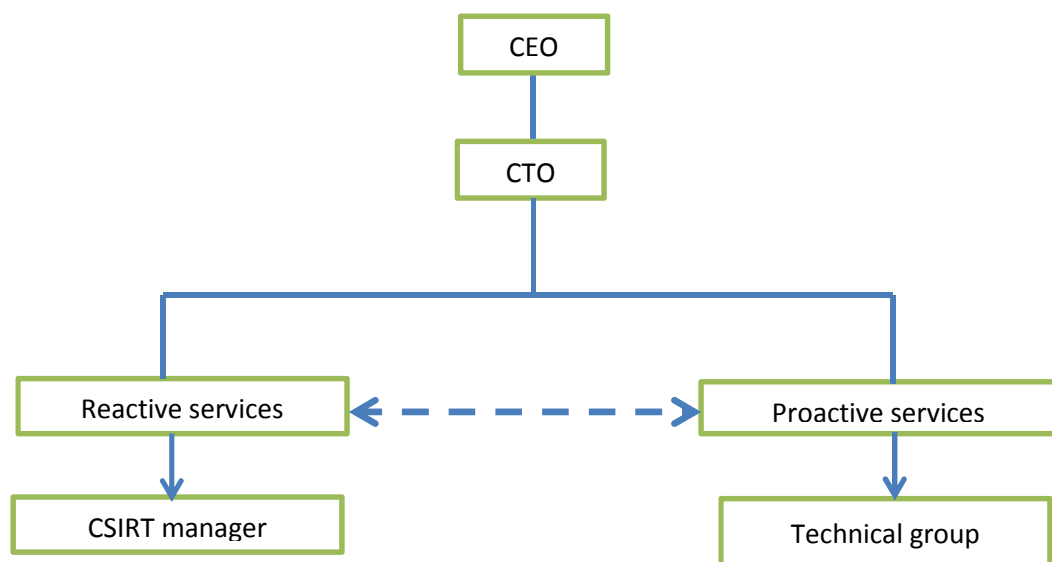


FIGURE 4.2 NgREN CSIRT Organizational model as recommended by the expert

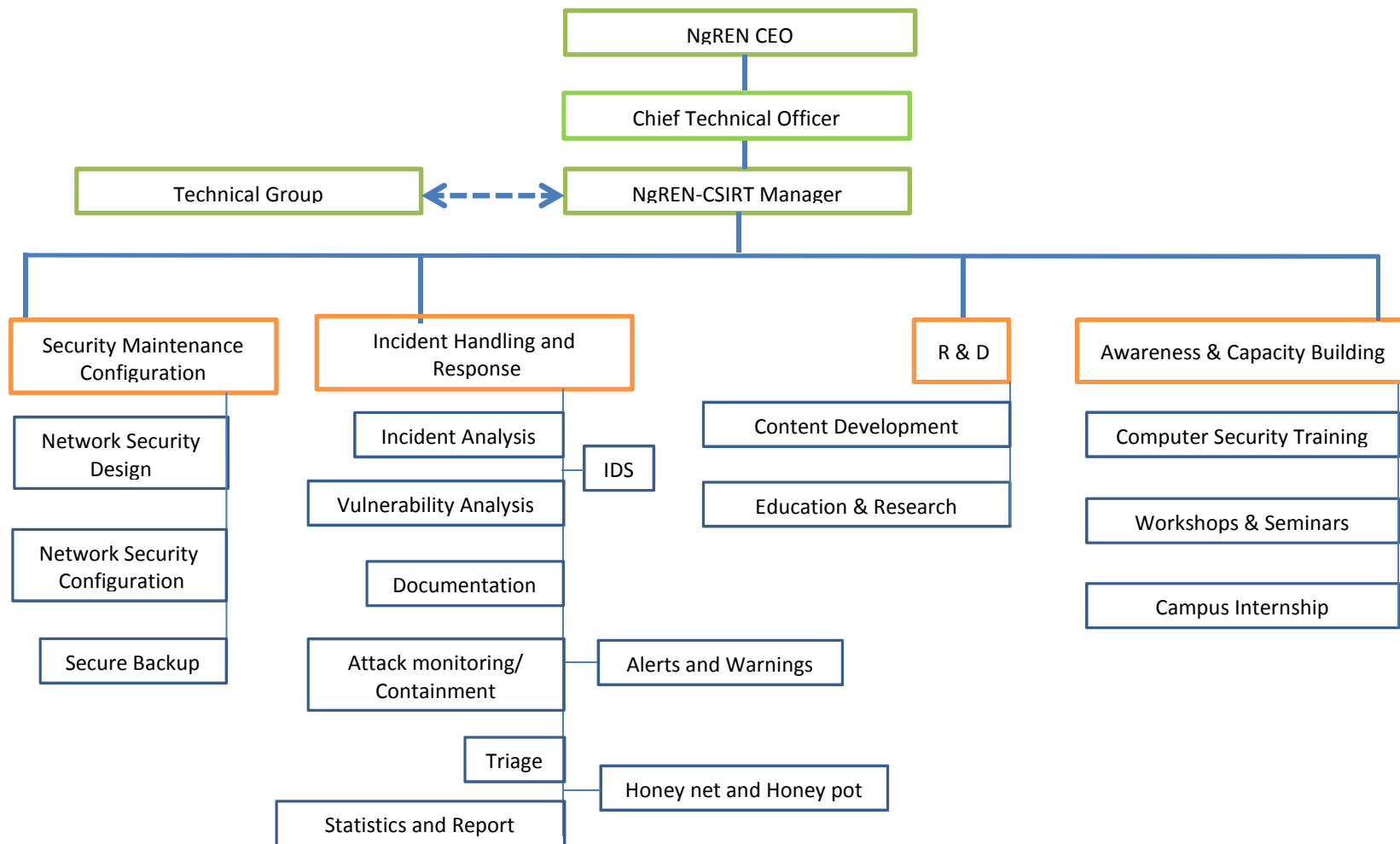


FIGURE 4.3 NgREN-CSIRT expanded organizational model as recommend by the expert

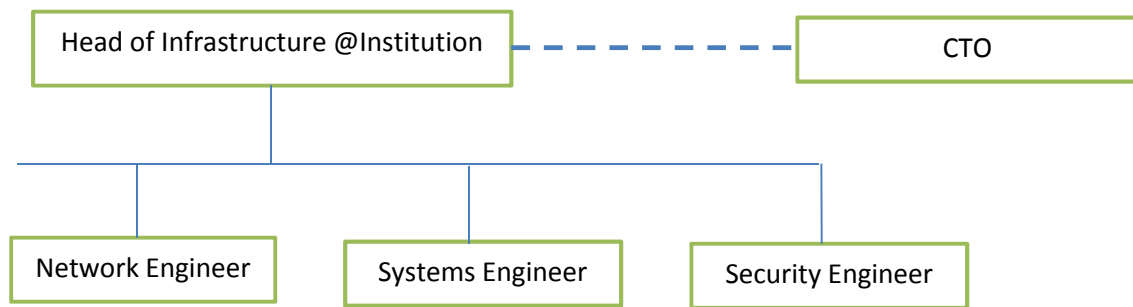


FIGURE 4.4 NgREN-CSIRT Security Team Organizational Model as recommended

4.4.1.3 Reporting and communication

Information sharing and reporting is very vital for any CSIRT to survive (Killcrece et al., 2003). The NgREN-CSIRT should have a reliable and secured reporting and communication mechanism in place to enable it to properly respond and report cyber security incidents efficiently. Here we are proposing to have a help desk that is located at central coordination center which is responsible for taking incidents reports from various security teams located at different institutions within the NgREN network. This can be done through the use of communication medium such as e-mail, phone, discussion forum and secure communication channel. The security teams report information about incidents in their various institutions whether resolved or not to the central coordination center for further analysis and documentation. The information to be received by the NgREN-CSIRT is not limited only to its internal members, information may also come from outside the CSIRT such information includes information from other CSIRTs such as alerts, warnings, results of investigation, security advisories, vulnerability/zero day attack, guidance and standards.

4.4.1.4 NgREN-CSIRT services

CSIRT Services is one of the derivatives of CSIRT framework (West-Brown et al, 2003). Going by the mission statements and findings in phase II of this chapter, three sections are needed: technical operations for incident handling and response coordination, education and research for security awareness and training, and Security maintenance and configuration. This includes the mandatory incident handling service

which is a requirement for any CSIRT to be referred to as CSIRT. Furthermore, these services are adopted from section 2.7.5 of chapter 2 of this study.

(1) Technical incident handling and response

Technical Incident handling involves receiving, prioritizing and responding to requests and reports, and analyzing incidents and events (Killcrece et al., 2003). Incidents handling includes: the action to protect, defend, mitigate and control the risks of cyber incidents which affect the systems or network. The incident handling activities are categorized as follows:

- Incident and Vulnerability Analysis

NgREN-CSIRT will be performing technical analysis and examination of vulnerabilities in hardware or software. This covers the identification of suspected vulnerability in the hardware or software, technical investigation of the vulnerability within the hardware or software to determine where it is located and how threats can exploit it. NgREN-CSIRT will analyse and review the affected system by investigating the source code, running a debugger to determine where the vulnerability occurs, or trying to reproduce the problem on a test system (Killcrece et al., 2003).

- Incident and Vulnerability Response

NgREN-CSIRT will be involved in determining the appropriate strategy to respond to mitigate or repair vulnerability. The strategy will involve developing or researching patches, fixes, and workarounds. It also involves notifying others of the mitigation strategy, possibly by creating and distributing advisories or alerts. This service can include performing the response by installing patches, fixes, or workarounds (Killcrece et al., 2003).

- Incident and Vulnerability Response Coordination

NgREN-CSIRT will alert the different parts of the constituent about the vulnerability and shares information about how to fix or mitigate the vulnerability. The NgREN-CSIRT verifies that the vulnerability response strategy has been successfully implemented by communicating with security teams within the constituent, experts, vendors and individuals or groups who first discovered or reported the vulnerability. This can be facilitated by analyzing the vulnerability or vulnerability report; patches, or workarounds; and producing technical analysis done by different parties (Killcrece et al., 2003).

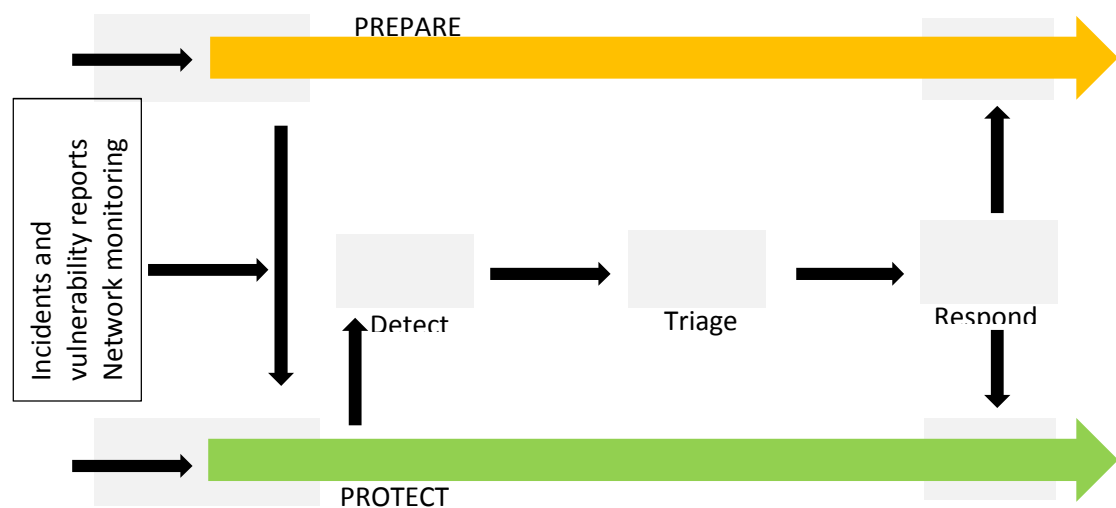


FIGURE 4.5 Incident Management Process Model adopted from (SEI, CMU)

(2) Security maintenance and configuration

NgREN-CSIRT in collaboration with individual security teams will develop security standards for the NgREN Network. The devices to be configured and maintained using the NgREN wide guidelines include firewalls, VPNs, IDS, Servers, Routers, Switches or even virus scanners. Work may also involve user account and password management or the review of network, system, security, and accounting logs. The benefit here is to have same level of protection mechanism all over the NgREN Network and less vulnerability.

If the security policies are centrally based, and the same security settings are used across the NgREN, then this will improve efficiency and timely response efforts to handling security issues throughout the network.

NgREN-CSIRT will monitor traffic that is traversing the NgREN network to ensure the security of data and infrastructure. It will use IDS systems throughout the network to collect anomalies and take necessary action.

(3) Security education and research

As discussed earlier in this study NgREN is a network of research organizations in Nigeria, therefore, security research would be one of the activities of NgREN-CSIRT. The research will include latest findings on vulnerability, threats, security tools and publication. It will also provide various training programs to the members of the constituent specifically the security teams. The training includes attacks and mitigation strategies, security configuration and incident handling and response. In addition to this, the NgREN-CSIRT will also be involved in security awareness sensitization using workshops and seminars.

4.4.1.5 Security quality assurance

NgREN-CSIRT would establish services designed to improve the overall security quality of NgREN Network. This will be done by leveraging the experiences gained during provision of the services described above. These services will incorporate feedback and lessons learned based on knowledge gained by responding to incidents, vulnerabilities, and attacks. The traditional services used for quality assurance includes Feedback, Risk Analysis, Business Continuity Planning and Security Awareness Campaign. Integrating these processes in to the security quality management can greatly improve the long-term security efforts in an organization (Killcrece et al., 2003).

4.4.1.6 Policies and procedures

As mentioned in section 2.6.7 of chapter two in this study, “All services and CSIRT functions should be supported by well-defined policies and procedures” (Ruefle et al, 2013). NgREN-CSIRT Policies and procedures are series of statements and guides that will direct how NgREN-CSIRT will operate. These policies and procedures will offer guidance on defined policies and procedures. These offer guidance for: roles and responsibilities, priorities, escalation criteria, nature of responses and NgREN-CSIRT staff recruitment (Ruefle et al, 2013). From our discussion in phase II of this chapter, we found that NgREN has no any formal policy and procedure for handling security incidents and for this reason there is need for NgREN-CSIRT to have policies and procedures in accordance with (Ruefle et al, 2013) in section 2.6.7 of chapter two in this study. The following are some of the policies and procedures required for the NgREN-CSIRT.

(1) Incident handling policy

This policy document will provide some general guidelines and procedures for dealing with computer security incidents. This will provide NgREN-CSIRT support personnel with some guidelines on what to do if they discover a security incident. The incident here could be irregular or adverse event that occurs on any part of the NgREN network. For example, compromise of system integrity; denial of system resources; illegal penetration or an intrusion; malicious use of system resources, or any kind of damage to a system (csirt.org).

(2) Server security policy

The main purpose of this policy is to establish standard guidelines for the base configuration of NgREN internal servers’ equipment that are owned and/or operated within the NgREN constituent. Effective implementation of this policy will minimize unauthorized access to NgREN proprietary information and technology (csirt.org).

(3) Internal/External communications policy

This defines whom the NgREN-CSIRT can talk with (e.g., other CSIRTs, law enforcement, Security team, constituent members and victims of attacks) and what type of information can be shared both inside and outside the NgREN-CSIRT and parent organisation (NgREN). This policy will be supported by the information disclosure policy that outlines what type of information can be released by the NgREN-CSIRT and to whom (Ruefle et al, 2013).

(4) Communication plan or policy

This policy will identify requirements for notification or communication of potential threats and detected incidents, or mitigation and resolution strategies, within the constituency or to security team, partners, or oversight agencies. This communication plan will cover who should receive the information and in what timeframe with (Ruefle et al, 2013).

4.4.1.7 NgREN CSIRT resources

Before starting to list the rudimentary technical infrastructure and human elements, a CSIRT must take attention in choosing the services it will offer. The set of services provided will establish the resources the team will need to function properly. The choice of services should support and enable the goals of the CSIRT's constituency. These can be put into human, equipment and infrastructure needs of the NgREN-CSIRT to execute its operations (Penedo, 2006).

(1) Infrastructure

NgREN-CSIRT will require technical infrastructure based on the mission and size of the NgREN constituent to achieve the objective set for the NgREN-CSIRT.

- Office accommodation

NgREN-CSIRT needs well-furnished office accommodation to allow its staff and team members to execute their daily activities. The purpose of office accommodation for the NgREN-CSIRT is to create sound working environment and to bring efficiency and rapidness in handling and responding to cyber security incidents. The number of office accommodation required depends on the number of services and staff needed to operate the NgREN-CSIRT. From phases II and III of this chapter we found that NgREN already have an office location at National Universities Commission with enough offices to accommodate the NgREN-CSIRT manager, other team members and equipment room. While at individual institutions, the security team members will utilize their existing offices.

(2) Technical infrastructure and equipment

As mentioned above, before we can start enlisting the technical infrastructure and equipment we need to know the services we are offering to the constituency. In this case NgREN-CSIRT proposed to provides three broad services to the NgREN Network they are security maintenance and configuration, incident handling and response and research and training. Figure 4.2 details these services. Besides these services other rudimentary services for successful operation of an organization will be provided and therefore, equipment is needed to achieve these services. In this study we are going to adopt (Penedo, 2006) technical infrastructure and equipment for a CSIRT.

- Telephone equipment

NgREN-CSIRT will need telephone equipment access to communicate with the NgREN constituency or for contacting other CSIRT's, vendors, external contacts etc. The purpose of telephone system will boost confidence within and outside the constituency and as well facilitate real time communication. It's important that NgREN-CSIRT to have a central phone that works as the main contact for the team, and the ability to be answered by another member at their desk (Penedo, 2006).

(3) Network infrastructure elements

NgREN-CSIRT must be connected to the Internet; with its own dedicated IP address space for security reasons.

- Domain name service (DNS)

It's suitable and helpful service for an Internet domain. NgREN-CSIRT DNS will promote the existence of the team and to provide an easy-to-remember interface for email or Web. The domain space will typically be csirt.ngren.edu.ng (Penedo, 2006).

- Email

The most common way of communication for a CSIRT is the e-mail, and so exist the necessity of gathering a good and robust email system, with good filtering capabilities, advanced search facilities and the possibility to integrate automatic response tools (Penedo, 2006). This email system must be well secured to encrypt messages. NgREN-CSIRT will use email system to communicate with its constituency and others CSIRTs, vendors and agencies (Penedo, 2006). The proposed mail address for the NgREN CSIRT could be: something@csirt.ngren.org.ng.

- Web site

We can say that Web site is the most effective way to disseminate information such as alerts and warnings and as well other information with the constituency. Going by the popularity of World Wide Web it is now mandatory for a CSIRT to have its own web site (Penedo, 2006). In this regard, it is vital that NgREN-CSIRT to have a web site for disseminating of useful information, including team's mission, notices, alerts, contacts, incident reporting form, best practices, etc. After the web site has been developed, it is good for the NgREN to implement strong security for the web site against hacking and defacement which could cause loss of trust in the constituency. The proposed url name for the NgREN CSIRT is <http://www.csirt.ngren.org.ng>

- Network security

Once CSIRT services are available on the Internet it is usual to become a target to intruders, attackers and crackers (Penedo, 2006). NgREN-CSIRT must be prepared with dedicated hardware and software designed to fully secure the external and internal services, for instance, by implementing a filtering policy in the routers. NgREN will need to deploy firewall as a mechanism to control and watch access to and from the NgREN network for the purpose of protecting it.

- Computers

The number of computer hardware equipment requirement, depends on the size of the team and services offered. The equipment should be chosen to best serve the needs of the constituency (Penedo, 2006). For this reason NgREN-CSIRT will require to host DNS, mail, web services, CSIRT tools, the team will need computer servers. For working on day-by-day operational issues the team should have desktops and/or laptops for each member, because they shouldn't share systems containing sensitive information. In addition, the security team at the various institutions will require servers for analysis tools, Test learning platform servers and laptops and/or desktops for their day-to-day activities.

NgREN-CSIRT also need systems/networks disconnected from other networks to work as a test and learning platform, to be possible for example test security vulnerabilities (Penedo, 2006).

(4) Operating systems

Choosing the right operating system platforms to use on a CSIRT network depends on many factors, the type of network used on the CSIRT's constituency, team skills and costs associated (Penedo, 2006).

Basically Linux is the choice of most hackers and security consultants. The Linux platform is versatile, and the system kernel provides low-level support for

leading-edge technologies and protocols (Penedo, 2006). In this regard, Linux would be used as the proposed platform of operation in NgREN CSIRT.

(5) Incident response tools

The number of incidents handled by team will vary according to the size of the constituency. It is very important for CSIRT to record history of each incident, all communications, log files, evidences, actions taken, etc. The choice depends on incident load, the incident tracking can be done with just mailboxes, and no perfect solution exists (Penedo, 2006).

There are many packages that can be used, from free to a lot of money. These packages provide support to the operation of a CSIRT Team. These packages include Application for Incident Response Teams (AIRT), Request Tracker for Incident Response (RTIR) and Remedy action request system (Penedo, 2006).

(6) IDS/Network scanner system

An Intrusion Detection System (IDS) and a network scanner are very useful tools for the CSIRT team. The IDS can be configured to run on alert mode to detect suspicious traffic in the backbone network. The network scanner can be used for security audit on systems. NgREN-CSIRT can choose to use snort as IDS system because it is open source software; efficient and robust tools; frequently updated; well supported with a big community of users. For the network scanner NgREN-CSIRT can use Nessus. NgREN community members are familiar with Linux operating systems.

(7) NgREN-CSIRT network infrastructure design

Base on the analysis of requirements and the aforementioned technical infrastructure, it was defined that the network system set up for NgREN-CSIRT and security teams at various institutions would count with the following basic design and components. Figure 4.5 shows network design for the central coordination team and Figure 4.6 shows for the security team.

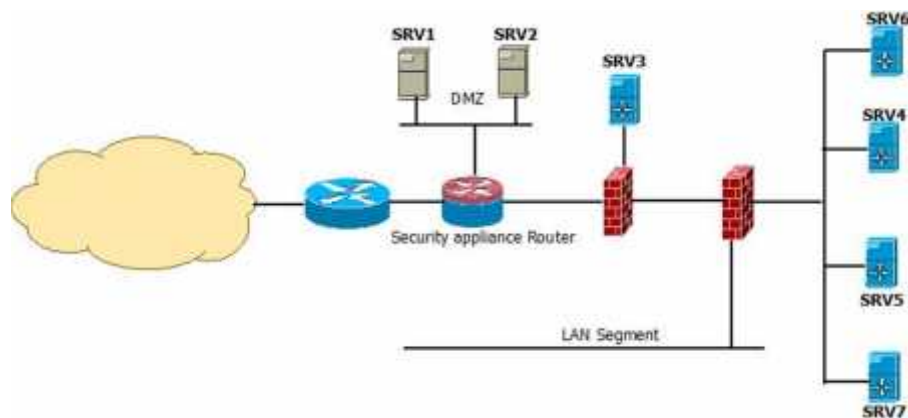


FIGURE 4.6 NgREN-CSIRT network model as recommended by expert

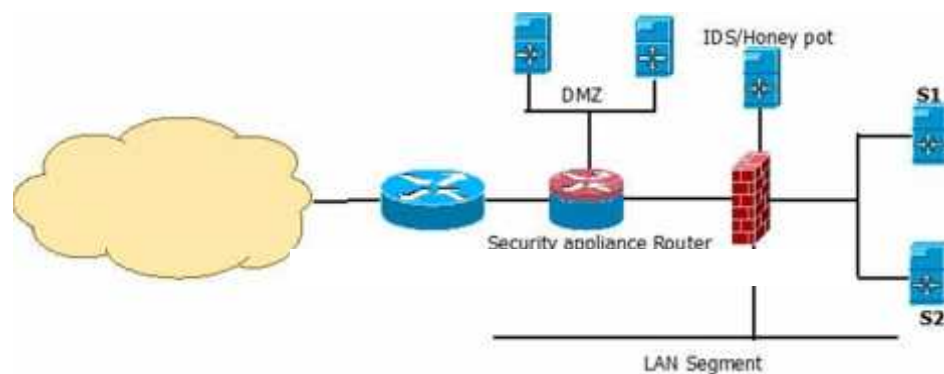


FIGURE 4.7 Security team network model as recommended by expert

- NgREN-CSIRT

Server 1 Frontend server: Running Linux operating system, Hosting web and E-mail

Server 3 IDS / Network scanner: Linux operating; Apache; Snort + SnortSnarf; Nessus.

Server 2 Middleware server: running Linux operating system; Email processing; Portal administration; Incident tracking system

Server 4 Database server: Running Linux operating system; MySQL.

Server 5 Test and learning platform: Windows server; Virtual PC.

Server 6 and 7 are backup servers running Linux operating systems

- Security Team

Server 1 Database server: Running Linux operating system; MySQL.

Server 2 Test and learning platform: Windows 2003 server; Virtual PC.

(8) NgREN-CSIRT personnel

CSIRT staffs are dedicated, creative and analytical. They should be problem-solvers, good communicators, and able to handle demanding situations. One of the most important qualities a team member must have is integrity (Ruefle et al, 2013)

CSIRT staff members have a variety of technical skills and personality qualities such as communication and people skills.

NgREN-CSIRT will have Manager and his deputy located at the central location and several technical staff with roles that include help desk, or triage staff, incident handlers, vulnerability handlers, platform specialists, trainers, network or system administrators, CSIRT infrastructure staff and web developers and maintainers. The administrators at security team will be handling the role of incident handling and response and as well communicate with the central CSIRT.

4.4.1.8 Management support and funding strategy

As mentioned in section 4.3.2 in phase II of this chapter. The management of NgREN which is the parent organization of the NgREN-CSIRT has the full desire to have the CSIRT established. This is because it is part of their mandate and framework to establish the CSIRT. In this regard, NgREN-CSIRT has the backing and support of the management. NgREN-CSIRT funding strategy will be based on main funding of the parent organization. The primary source of funding for NgREN is membership fees as well as subscription fees for services from member institutions. For instance, each institution will subscribe and pay for bandwidth that it requires. They also pay for e-books and journals as well as other connectivity services. In addition to this, there is an initiative from the Federal Government of Nigeria that mandated some agencies to continue funding the activities of NgREN.

The agencies include Federal Ministry of Communication via (NCC- National Communication Commission, NITDA- National Information Technology Development Agency) and PTDF- Petroleum Technology Development. Tertiary Education Trust Fund (TETFUND) is another Government organization in Nigeria that provides funding support for academic activities in tertiary institutions in Nigeria. In addition to this, the NgREN can also approach some donor organizations within and outside African continent for support in terms of funding, capacity building and equipment. This can be done by writing funding proposal to organizations such as World Bank, Islamic Development Bank, Nigeria Network Operators Group and Telecom companies and ISPs.

4.5 Validating the framework

In this phase the final objective of this study was achieved by validating and refining the proposed CSIRT framework for its applicability to the NgREN. The proposed framework was shared with mycert (Malaysia Computer Emergency Response Team) and the user organization (NgREN) in their capacities as experts and parent organization respectively. The above mentioned organizations were requested to provide open ended comments in respect to the proposed framework. No any guide given to the experts, but they were asked to go through the framework and make suggestion for improvement. Their inputs was taken and used. Appendix IV shows the comments of the NgREN CEO.

4.6 DISCUSSION

In this section the findings from the above sections are discussed and linked with research questions and objectives. The research questions and objectives were presented in sections 1.7 and 1.6 respectively. Not all the findings are directly linked to the research questions, but emerged from the outcome of the interview and literature. The methods for the study are based on the research approach described in sections 3.2.1, 3.2.2 and 3.2.3. Finally, section 5.2 presents our contributions for performing this study.

The central objective of this study was to propose a framework for Cyber Security Incident Response team for the Nigerian Research and Education Network (NgREN). This was achieved by adopting the generic CSIRT framework.

This study was based on four research questions and four objectives as mentioned above. The research objectives were achieved by answering the research questions which are:

- (1) What is generic CSIRT framework and its component?
- (2) How NgREN manages cyber security incidents?
- (3) How would the generic CSIRT framework be customized for Nigerian Research and Education Network?
- (4) How the proposed framework can be validated and refined?

The first objective described in section 1.6 was to conduct a critical review on cyber security incident response management. This was done by answering the question “What is generic CSIRT framework and its component?” The essence of this question was to have an insight into CSIRT framework, models, procedures, plans and current organizational practice of cyber security incident response management. For this, a comprehensive study was conducted on various literatures and technical papers to understand relevant questions asked during meeting sessions with NgREN stakeholders. This made us to have a deep insight into the components of CSIRT framework and its derivatives and as well as other models and their shortcomings. Furthermore, we are able to prepare for the second objective of the study.

To further achieve first it was very imperative to know the area of case study, common cyber threats and how it handles cyber security threats. This was done by holding meeting sessions and interviews with stakeholders to ascertain the gap from the first research question with the aim of mending and improving the gaps.

The third objective was achieved by answering the third research question “How would the generic CSIRT framework be customized for Nigerian Research and Education Network?” This was answered based on the findings of the Research questions one and two as discussed in section 4.4. The fourth and the final objective was achieved by answering the question “How the proposed framework can be validated and refined”? In answering this question and by implication to achieve the fourth objective, the proposed framework was shared with two experts namely: CEO of NgREN and Head of

Information Security Professional Development of Cyber Security Malaysia. The experts were selected based on their Educational background, years of experience and understanding of the study area. Table 4.1 below shows the specific sections affected during the validation. All the affected sections were updated.

TABLE 4.1 Experts suggestions on the framework

Comments by CEO NgREN expert	Comments by expert from CSM expert
INTERVIEW RESPONSE	
Interview Responses were corrected and noted	
FUNDING AND SUPPORT	
Direct funding from member Institutions by paying for services	No comment and accepted
MISSION STATEMENT	
The mission statement was reframed to capture other areas that were mistakenly left out	The mission statement was reframed to cover national CERT for escalation
ORGANIZATIONAL STRUCTURE	
Incorporating a technical working group in form of advisory body in to NgREN CSIRT organizational structure	A technical group to be providing proactive services. The role of manger was replaced with CTO and two major units were created directly under the CTO (CSIRT manager and TWG). Add R&D and Training/Development as separate units under NgREN-CSIRT organizational model.
FRAAMEWORK DIAGRAM	
No comment	The framework was divided in to two sections namely: Functional framework and process flow. Create a link within the framework to show how incidents can be escalated to other CERT

All the comments on table 4.1 were implemented on section 4.4 and figures therein. The final framework is described in figures 4.8 and 4.9.

Figure 4.8 described the main framework of the NgREN CSIRT. As explained in sections 2.8 and 4.4.1.8 as well as figure 4.8, senior management support must be secured

first before establishing CSIRT for an organization. The figure further describes synergy between the various major internal components of the framework.

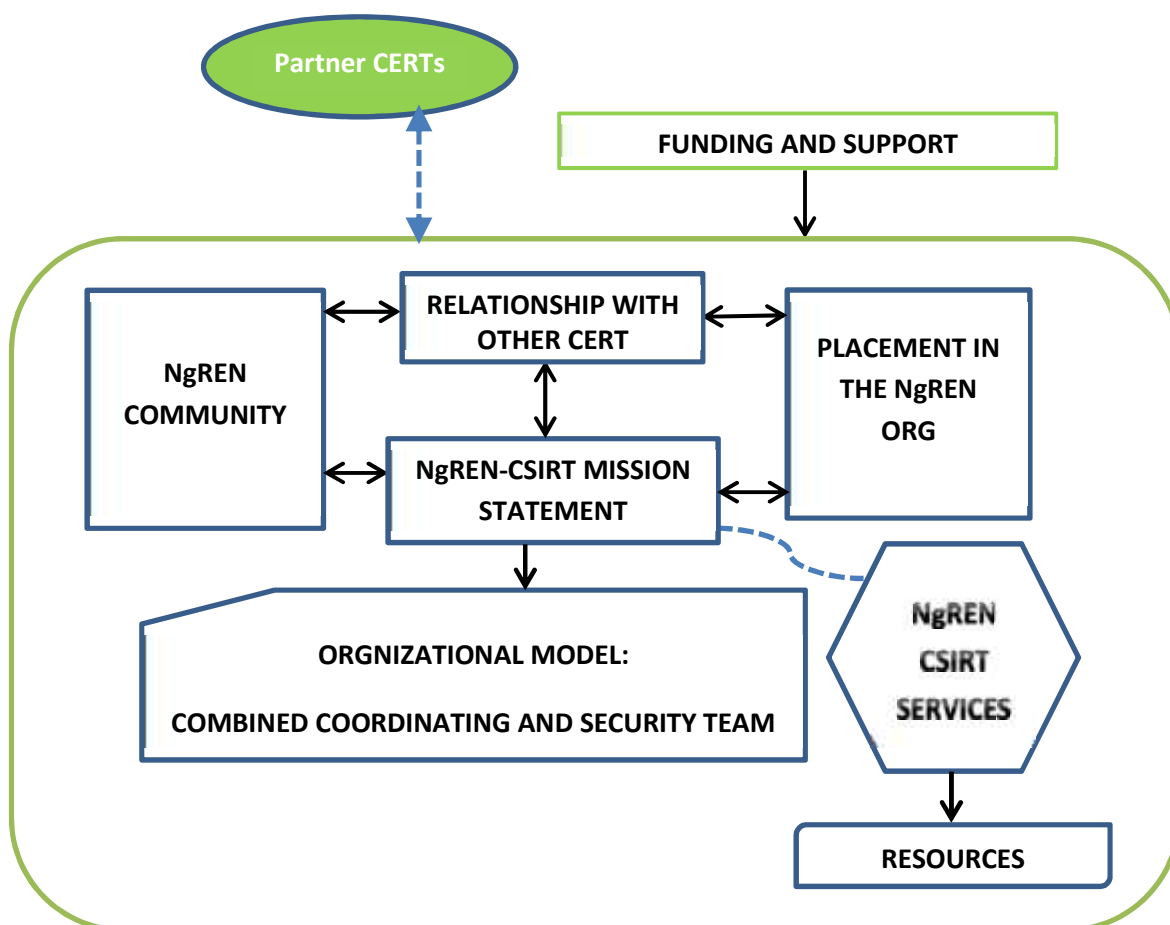


FIGURE 4.8 NgREN-CSIRT functional framework as recommended by expert

As indicated in sections 2.7 and 4.4.1, these four elements (mission, constituency, place in organization and relationship with other certs) are closely identified with one another. If for example, the CSIRT mission statement changes, definitely the other components must get affected. Cyber Security Incident management Resources to be deployed in the CSIRT is directly related to the services to be provided in the constituency. This relationship also applies between Mission statement and organizational model. Finally, it is important NgREN CSIRT sign an MOU or bilateral agreement with an external CERT for technical support and security incident escalation.

Figure 4.9 described the process flow of NgREN-CSIRT framework. The diagram explains the relationships between the CSIRT mission statement and policy and quality

assurance for an efficient service. This is possible by the use of policy and procedure documents to support the CSIRT mission statement. Sections 2.7 and 4.4.6 explained detail information about the components of the process flow.

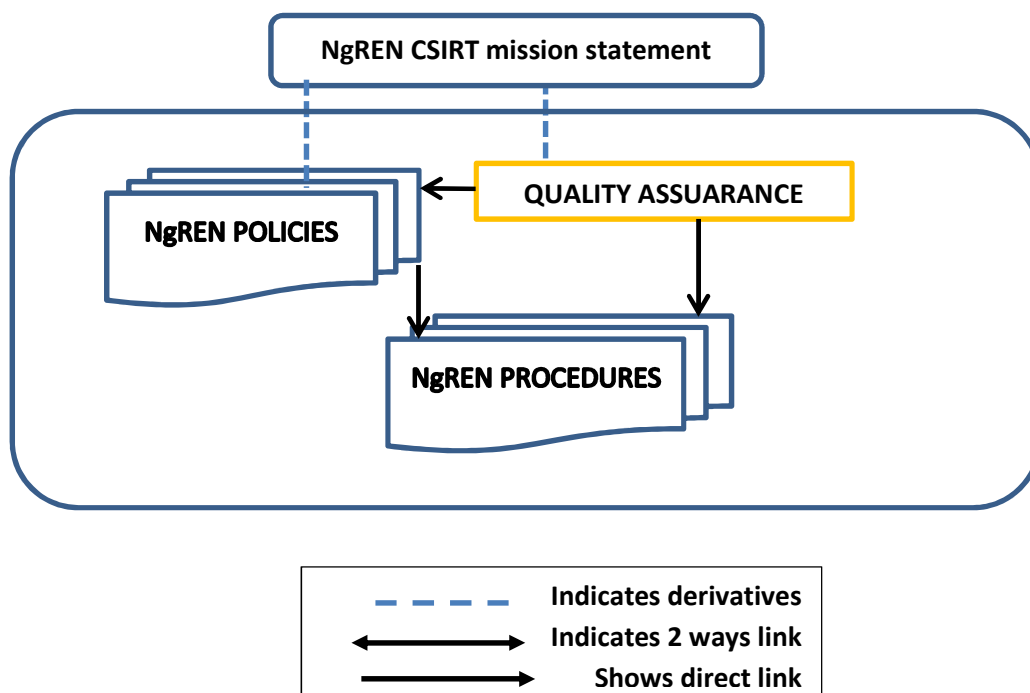


FIGURE 4.9 NgREN CSIRT process flow as recommended by expert

4.6 SUMMARY

In this chapter the objectives and a method of this study were reiterated. Next we presented and analyzed our findings on the literature review; this enabled us to achieve our first objective. Again, we presented and analyzed data from the meeting session and finally presented our findings this also, made us to achieve our second objective. The third objective of this study was achieved by using the findings of objectives one and two to proposed NgREN-CSIRT framework for the Nigerian Research and Education Network. We finally, we validated and refined the framework based on open ended comments from experts.

CHAPTER V

CONCLUSION

5.1 INTRODUCTION

In this study, we proposed the CSIRT framework for the Nigerian Research and Education Network for handling and responding to cyber security incidents.

In order to propose the CSIRT organizational framework, different research objectives that were put in phases have been accomplished, including reviewing a wide range of scientific and industry papers, meeting session/interview with NgREN stakeholders to ascertain the needs regarding cyber security incident handling and response within the NgREN, integrating the literatures and information extracted from the meeting session in the framework, and undertaking the refinement of the proposed framework.

In this chapter, we summarized the main contributions of the study, discuss research limitations, recommendations and propose potential ideas for future work.

5.2 MAIN CONTRIBUTIONS

We identified the following contributions of this study as follows:

- (1) We are able to achieve our first and second objectives of this study by diving into cybersecurity incident handling challenges of national research and

Education network and finds the needs of organize cyber security incident handling in mitigating cyber security issues.

- (2) We achieved the second objective by proposing NgREN-CSIRT framework that integrates key findings from the literature and meeting session and address every identified challenge, assuring rigor and relevance of this study. The proposed CSIRT organizational framework designed components such as organizational model; policies, infrastructure and network design will hasten the process of implementing cyber security incident respond team.

Though, the framework is organization specific, but it establishes a base line from which any developing NREN can easily adjust and use the framework for its operational cyber security incident handling and response. The refined CSIRT organizational framework structure can be found in sections 4.8 and 4.9.

Besides the above mentioned contributions the following are also recommended for the proper implementation of the study outcome. These were achieved in the final objective of this study.

The management of NgREN CSIRT specifically the NgREN top level management should have a working relationship with two or more CSIRTs within and outside the country of resident. This can be done by having an MOU (Memoranda of Understanding) or through bilateral agreement in case of international CSIRTs. The agreement should contain incident escalation and support, training of staff and sharing of security incident information.

From chapter four we found that the NgREN CSIRT has a full management support this is a key element for any successful project. Management support should last throughout the project: from the planning to the implementation, through to the project closure. In addition, it is important that management support be wide-ranging and displayed publicly in support of the project team.

The team needs to ensure that there is enough funding for the entire project and that the funding can be allocated for the required purpose. Changes to the original project plan and scope creep are common and therefore the funding should be flexible in that regard. The team should also reserve enough funding for contingency costs. This involves the creation of a well-defined annual budget that is separated into activities and functions.

Human and technical resources are a particular part of the functional framework component outlined in chapter 4. These play a very important role in CSIRT operations.

The team implementing the NgREN CSIRT should ensure that the team is able to purchase all needed equipment, accessories and systems. CSIRT operations heavily relies on specialized computer and IT equipment.

The team implementing the NgREN CSIRT framework should develop its own ICT policy and to avoid conflict with mother organization (NgREN). It is also important for the team develop a good relation with the main NgREN technical team.

Policies and operational and technical procedures are part of process flow prescribed by the NgREN framework, to ensure an intended result. Operational and technical procedures and policies are necessary to ensure that the CSIRT members handle incidents in a consistent way. The process of information handling during incident handling is very similar to that used during the compilation of alerts, warnings and announcements.

It is not easy to provide real number of technical staff needed from the number of services to be provided, but the following approach should be used:

- (1) During the initial set up two core services of the distribution of advisory bulletins as well as incident handling: a minimum of four full time employees (it is important that the team focus on the incident handling services in order to be called a CSIRT). A minimum of six to eight full time employees for full CSIRT services during working hours and maintaining systems

- (2) Minimum of 12 Full time staffed 24/7 shift (two shifts during out-of-office hours).

These numbers include redundancies to provide for sick leave and vacation leave, etc. When the CSIRT is properly established, the NgREN CSIRT team should ask the host organization's management (NgREN management) to make a formal announcement, both to the existing constituency as well as the general public. This step includes the distribution of flyers, meetings and incident reporting guidelines explaining how the constituency should interact with the CSIRT.

At this stage, the CSIRT team should also concentrate on ways to disseminate information about the CSIRT services, using intranets, web sites, discussion groups, social media, brochures, seminars and training workshops.

5.3 LIMITATIONS

This study is not without some limitations. The major one is the time constrain for the study.

Secondly, lack of empirical testing of the framework in a realistic environment. It requires large commitment in time and resources from the NgREN organization, which in the time frame of this research was not feasible to organize. As of now, feedback was received from the CEO of the NgREN that the framework is quite in line with NgREN structure and requirement. This indicates positive interest, so there are opportunities to implement the framework in the near future.

Finally, in this study we do not discuss in detail how the framework tools, such as network infrastructure and servers, policies organizational structure and funding strategies should be implemented to ensure the overall effectiveness of the framework.

5.4 FUTURE WORK

This study is a first of its kind around cyber security incident handling and response framework for Nigerian research and education network. There is still a lot to investigate, discover and implement.

The limitations mentioned in the previous section serve as the base to continue investigating and refining the framework. More experts could be requested to validate the framework for more refinements and future adjustments. Finally, the scope of this study only considers Nigeria research and education network. However, the framework can be adopted for other NRENs by modifying it through needs assessment.

5.5 CONCLUSION

CSIRT is an organization of devoted and responsible cyber security experts that plans and responds to cyber security incidents. Due to sophistication of cyber-attacks and lack of cyber security coordination within the developing NRENs, particularly in Nigeria, managers have to strategize to contain these attacks in coordinated and organized way by implementing Cyber Security Incident Response Teams (CSIRT).

This study brainstormed on the steps to take when creating a structure for a CSIRT within an educational network. The study proposed a CSIRT framework for the Nigerian research and education network.

The significance of this study lies in the practical hands-on guidance on what to do before, during and after establishing a CSIRT. Although the study was intended for the establishment of a CSIRT on a Research and education network within a developing nation, all of the steps and challenges are also relevant when establishing a sector-specific or organizational CSIRT. Additionally, other NRENs worldwide can also adopt the framework for their operation through modifications of its components.

REFERENCES

- Charles DeVoe, Syed Shawon & Rahman, M. 2013. Incident Response Plan for a small to medium size hospital. *International Journal of Network Security & Its Application* 5(2):
- Papulova, Z. 2014. The Significance of Vision and Mission Development for Enterprises in Slovak Republic. *Journal of Economics, Business and Management* 2(1):
- CERT/CC. 2014. About CERT Carnegie Mellon University. (Online) <http://www.cert.org/about/index.cfm>. (15 December 2014).
- Pinar Altıok. 2011. Applicable vision, mission and the effects of strategic management on crisis resolve. *Procedia Social and Behavioral Sciences* 24: 61–71.
- 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.
- Rajasekar, S. Research Methodology. (Online). <http://www.scribd.com/doc/6949151/>. (10 February 2014).
- Newmeyer, K.P. 2014. Cyber Security Strategy in Developing Nations: A Jamaica Case Study. PhD. thesis, USA: UMI dissertation and publishing.
- Sen, O.N. 2001. Criminal Justice responses to emerging computer crime problems. M.Sc thesis. Texas, USA.
- Dehlaw, Z. & Abokodair, N. 2013. Saudi Arabia's Response to Cyber Conflict: A case study of the Shamroon Malware incident. 978-1-4673-6214-6 C2013 *IEEE*: 73-75.
- CSIRT, 2014. CSIRT Sample Policies. (Online) https://www.csirt.org/sample_policies/index.html. (02 March 2015. Robin

- Ruefle, Ken van Wyk & Lana Totic. 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.
- 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.
- Moir J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece Robin Ruefle & Mark Zajicek. 2003. Handbook for Computer Security Incident Response Teams (CSIRTs).
- 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.
- 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.
- Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle & Mark Zajicek. 2003. Organizational Models for Computer Security Incident Response Teams (CSIRTs).
- Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle & Mark Zajicek. 2003. State of the Practice of Computer Security Incident Response Teams (CSIRTs). TECHNICAL REPORT CMU/SEI-2003-TR-001 ESC-TR-2003-001.
- John W. O'Neill, 2001. The Use of Organizational Culture and Structure to Guide Strategic Behavior: An Information Processing Perspective. *The Journal of Behavioral and Applied Management Winter/Spring 2001* 2(2): 131-150.

- Cathrine Hove & Marte Tarnes. 2013. Information Security Incident Management: Case study of three large Norwegian organizations. M.Sc. thesis. Norwegian University of Science and Technology (NTNU).
- Michael D. Myers & Michael Newman. 2007. The qualitative interview in IS research: Examining the craft. *Information and organization* 17(1):2–26
- Catherine Cassell & Gillian Symon. 2004. Essential Guide to Qualitative Methods in Organizational Research. Sage Publications Limited.
- Kennedy, M. 2006. A guide to interview guides. MSU Doctoral Program in Teacher Education. (Online).
<http://edweb3.educ.msu.edu/digitaladvisor/Research/interviewing.htm>. (10 February 2015)
- Michael R. Mulligan. 2012. State methods for a Cyber Incident. M.Sc thesis. Monterey California Naval Postgraduate School.
- Gabriela Judith Silvestre. 2008. A case study of the tensions between policy-making and implementation of higher education reform policies that affect the professoriate at two Argentinean Universities. PhD thesis. University of Pittsburgh.
- David Penedo. 2006. Technical Infrastructure of a CSIRT. *IEEE*: 0-7695-2649-7/06
- Marthie Grobler and Harri Bryk. 2010. Common Challenges Faced During the Establishment of a CSIRT. *IEEE*: 978-1-4244-5495-2/10
- Rahayu Azlina Ahmad and Mohd Shamir Hashim. 2011. The Organisation of Islamic Conference – Computer Emergency Response Team (OIC-CERT). 978-0-615-51608-0/11 ©2011
- Maria B. Line, Inger Anne Tønne and Martin G. Jaatun. 2014. Information security incident management: Planning for failure. 978-1-4799-4328-9/14 © 2014 *IEEE*

APPENDIX I

Introductory letter to Conduct Research at NgREN



Fakulti Teknologi dan Sains Maklumat • Faculty of Information Science & Technology

3 December 2014

To:
Whom It May Concern

Dear Sir,

CONDUCTING RESEARCH
- **YAHYA MOHAMMED WARA (GP02547)**

The above named student is currently pursuing **MASTERS DEGREE IN CYBER SECURITY** with Cyber Security Unit, Faculty of Information Sciences and Technology, Universiti Kebangsaan Malaysia. The following is the detail information on the student:

Type of Study:	Full Time
Registration Number:	GP02547
Master Degree Topic:	Adopting CSIRT framework for the Academic and Research Networks in Nigeria.

For your information, YAHYA MOHAMMED WARA is currently in the process of collecting data and information for his Masters dissertation.

Since your organization has the required information for the student, it is hope that you can give some assistance to Mr. YAHYA MOHAMMED WARA in acquiring the relevant information for his Masters Dissertation study.

Your corporation is very much appreciated.

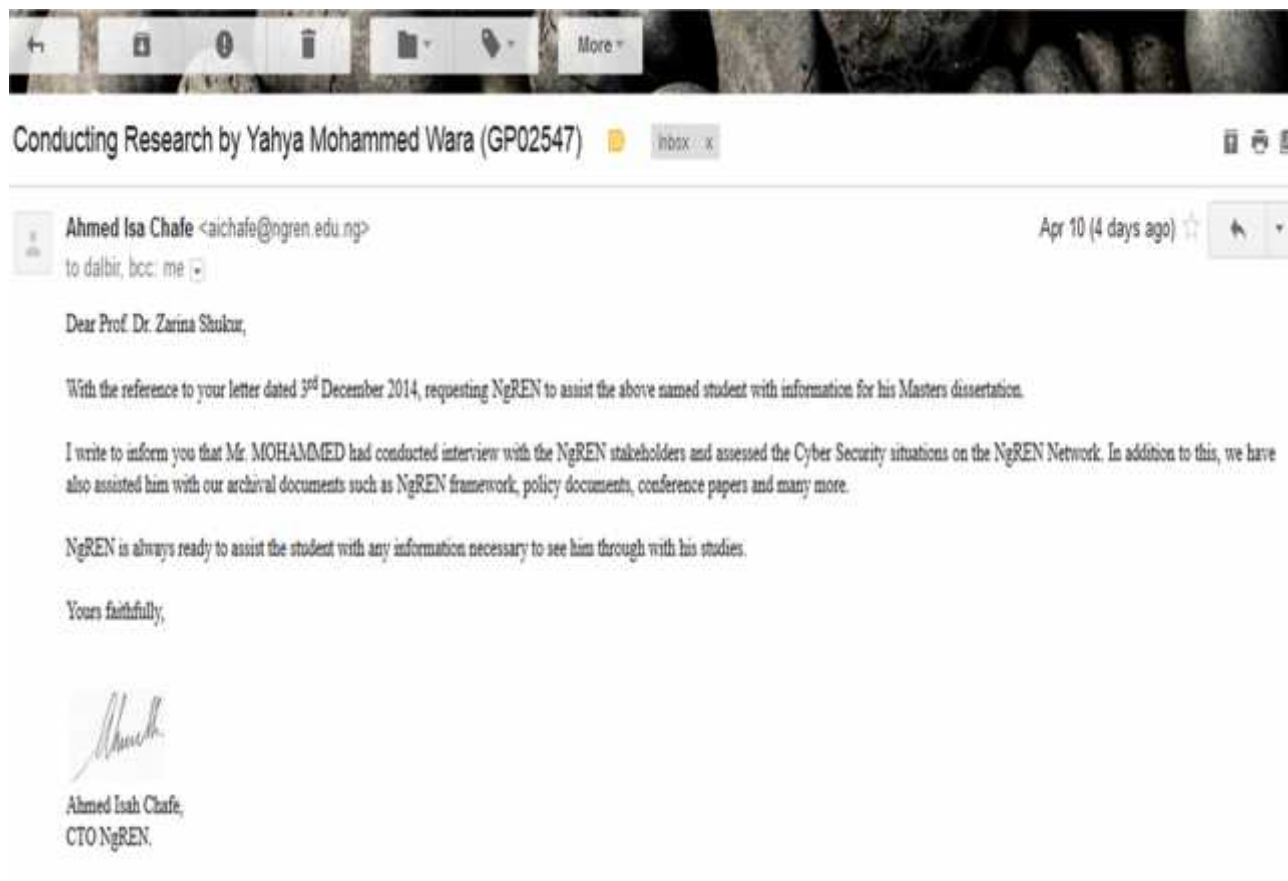
Thank you.

Regards,

Prof. Dr. Zarina Shukur
Head of Cyber Security Unit
Faculty of Information Science and Technology
Universiti Kebangsaan Malaysia

APPENDIX II

Confirmation letter of conducting interview



APPENDIX III

Interview Questions

1. How familiar are you with CSIRT?
2. How can CSIRT be useful to NgREN?
3. How is NgREN managed?
4. Who are the members of NgREN Constituent?
5. How does NgREN coordinate cyber security incidents?
6. How does NgREN define Cyber Security Incident?
7. How does NgREN gather reports on Cyber Incident?
8. How does NgREN respond to Cyber Security Incident?
9. How does NgREN manage cyber security issues?
10. Which Office/Department/Section is responsible for the monitoring of Cyber Incident under NgREN?
11. What will be the position of NgREN CSIRT within your organizational structure?
12. How can the components of CSIRT framework by West-Brown et al, 2003 be reformulated for the NgREN?
13. How can the derivatives of CSIRT framework by West-Brown et al, 2003 be reformulated for the NgREN?

APPENDIX IV

Report of framework validation from NgREN

