UNDERSTANDING THE CONCEPT OF CYBER SECURITY

Policy Competition & Economic Analysis Department

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Business and individuals in every country rely on information and communications technologies for their day to day activities; computers are used to store information, process information and generate reports. Computer networks may be responsible for many crucial and back office operations and it is necessary to secure these systems and their data from cyber threat or attacks.

Cyber threats are now the most effective way to attack an organization or country and the fact is that those with malicious intent are finding ever more sophisticated ways of carrying out their activities.

Consequently, the International Telecommunications Union [ITU] and the International Multilateral Partnership against Cyber Threats (IMPACT) signed an agreement on September 3rd, 2008 which made IMPACT the Global Cyber Security Agenda (GCA) that provides expertise and resources to detect, analyze and respond effectively to cyber threats to over 193 ITU Member States and in 2011 IMPACT formally became the Cyber Security executing arm of ITU. The coalition is of particular benefit to countries that lack the resources to develop their own cyber response Centers. Through this initiative, a Regional Cyber Security Center (ITU-RCC) has been established in Sultanate of Oman in the Arabian Region and the Regional Cyber security Centre for African Region is being proposed by the ITU to be hosted in Nigeria and managed by the Commission. The ITU and IMPACT's initiative of establishing Cyber Security Centers in various regions of the world is an excellent means of addressing the growing global cyber security threats.

Many government entities are challenged with insufficiently secured infrastructure, lack of awareness, and competing funding and resource priorities. Governments around the world maintain an enormous amount of personal data and records on their citizens, as well as confidential government information, making them frequent targets. Better security helps government bodies provide reliable services to the public, maintain citizen-to-government communications, protect sensitive information as well as safeguard national security. All hands must therefore be on deck to effectively combat this menace because Cyber-attacks by their very nature simply require a loop hole or entry point through which the attack can be replicated.

As a result of this, many countries across the world in addition to the ITU initiative have taken up the responsibility of setting up Computer Emergency Response Teams [CERT] in their respective countries to combat the menace of cyber threats and attacks. Nigeria like these countries, official commissioned the Nigeria National Computer Emergency Response Team [ngCERT] operations center in Abuja on the 25th of May, 2015 and the ngCERT is domiciled in the office of the National Security Adviser.

While Nigeria has recently commissioned its ngCERT which primarily caters for the Nigerian Cyberspace, the ITU initiative of establishing a regional Cyber Security Center in Nigeria for the African Region, will equally be of immense benefit to Nigeria and the entire African region in general.

CHAPTER ONE

1.0 INTRODUCTION:

The rapid development in Information and communications technologies (ICTs) have significantly transformed how people communicate with each other even across geographical divides. In today's world which is often referred to as a global village, geographical barriers seldom impede communication as ICTs offer very effective means of communications via the World Wide Web. Notwithstanding the technological advancements recorded in the ICT sector, security while communicating or transacting business on the internet remains a major source of concern for users of these services.

The International Telecommunications Union [ITU] defines Cyber security as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment."

Basically, Cyber security is the protection of systems, networks and data in cyberspace and is essential even as more people get connected to the internet across of the world. The ITU also notes that the three broad security objectives are ensuring Availability; Integrity (which may include authenticity and non-repudiation), and Confidentiality. While these are the bedrock of a secure network, achieving these three objectives is no mean feat as it requires the integration of various functions such as robust systems engineering and configuration management; effective cyber security or information assurance policy and comprehensive training of personnel.

While rapid advancement and technological developments are constantly being recorded in the ICT sector, the volume and sophistication of cyber-attacks are also increasing, therefore serious attention must be given to the protection of personal or business information transmitted in the cyber space as this ultimately impacts on national security as well.

The growing dependency of modern societies on information and communication technologies that are globally interconnected creates interdependencies and risks that need to be managed at national, regional and international levels. Therefore enhancing Cyber Security and protecting critical information infrastructures are essential to each nation's security and economic well-being. At the national level, this is a shared responsibility requiring coordinated action related to the prevention, preparation, response, and recovery from incidents on the part of government authorities, the private sector and citizens. At the regional and international level, this entails cooperation and coordination with relevant partners. The formulation and implementation of a national framework for Cyber Security and Critical Information Infrastructure Protection (CIIP) as well as the setting up of a Computer Incidence Response Team / Cyber Security Center is therefore critical to successfully securing a nation’s cyberspace.

In order to fully understand the concept and workings of a Cyber Security Center, we will examine various components some of which include: Cyber Security, Computer Emergency Response Team; Cyber Security Center Operations, Functions of a CERT and Cyber Security Center and the measures to be taken to ensure a secure cyber space amongst other things in subsequent sections of the research.

1.1 Key Concepts in Cyber Security:

We will briefly examine some key concepts that impact successful and effective Cyber security operations.

1.1.1 What is Cyber Security?

According to the ITU, Cyber security refers to the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment - the internet.

Cyber Security can also be described as the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

ITU also notes that the general objectives of Cyber Security are: Availability; Integrity, (which may include authenticity and non-repudiation) and Confidentiality.

In order to fully understand the concept of cyber security, we will examine the various components of cyber security and the measures to be taken to ensure a secure cyber space in the subsequent sections of the research.

1.1.2 Functions of a Cyber Security Center:

Ideally, a Cyber Security Center should strive to ensure a secure and resilient cyber and communications infrastructure that supports national/ regional security, a vibrant economy, and the health and safety of all citizens. To achieve this, a Cyber Security Center should:

- Focus on proactively coordinating the prevention and mitigation of those cyber and telecommunications threats that pose the greatest risk to the Nation;
- Pursue whole-of-nation operational integration by broadening and deepening engagement with its partners through information sharing to manage threats, vulnerabilities, and incidents.
- Break down the technological and institutional barriers that impede collaborative information exchange, situational awareness, and understanding of threats and their impact.

- Maintain a sustained readiness to respond immediately and effectively to all cyber and telecommunications incidents of national security.
- Serve stakeholders as a national center of excellence and expertise for cyber and telecommunications security issues.
- Protect the privacy and constitutional rights of the citizens in the conduct of its mission.

1.1.3 Cyber-Attack:

Farhat, et.al. (2011) define a cyber-attack as an attack initiated from a computer against a website, computer system or individual computer (collectively, a single computer) that compromises the confidentiality, integrity or availability of the computer or information stored on it. They further noted that cyber-attacks may take the following forms:

- Gaining, or attempting to gain, unauthorized access to a computer system or its data;
- Unwanted disruption or denial of service attacks, including the take down of entire web sites;
- Installation of viruses or malicious code (malware) on a computer system;
- Unauthorized use of a computer system for processing or storing data;
- Changes to the characteristics of a computer system's hardware, firmware or software without the owner's knowledge, instruction or consent;
- Inappropriate use of computer systems by employees of former employees.

Cyber-attacks could be categories by state and origin as follows:

- **Active and Passive Attacks**

An "active" attack aims to alter system resources or affect their operation. Conversely, a "passive" attack seeks to use information from a system but does not affect system resources of that system (IETF 2007). Instead, passive attacks aim to obtain data for an off-line attack. For example, hackers typically use packet inspection and analysis to facilitate offline review of security protocols and thus fine-tune exploits.

- **Inside and Outside Attacks**

We may also characterize attacks according to their initiation point. The Internet Security Glossary describes an “Inside Attack” as one that is initiated by an entity inside the security perimeter (an "insider"). Insider attacks are difficult to defend against because the culprits misuse the access privileges obtained for legitimate business functions. In contrast, unauthorized or illegitimate users initiate "outside” attacks outside the security perimeter. Outsider attackers include hackers, organized criminal groups and States. The attack types are not mutually exclusive as outsiders often rely on insiders.

1.1.4 Cyber Threats:

The term Cyber threats refer to persons who attempt unauthorized access to a control system device and/or network using a data communications pathway. This access can be directed from within an organization by trusted users or from remote locations by unknown persons using the Internet. Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and malicious intruders (ICS-CERT). Cyber threats could be further differentiated by character, impact, origin and actor as follows:

- **Accidental or Intentional Threats**

Accidental threats occur without premeditated intent. For example, system or software malfunctions and physical failures. However, intentional threats result from deliberate acts against the security of an asset. Intentional threats range from casual examination of a computer network using easily available monitoring tools, to sophisticated attacks using special system knowledge. Intentional threats that materialize become *attacks.*

- **Active or Passive Threats**

Active threats are the ones that result in some change to the state or operation of a system, such as the modification of data and the destruction of physical equipment. Conversely, passive threats do not involve a change of state to the equipment. Passive threats aim to glean information from a system without affecting the resources of the system. Common passive threat techniques include eavesdropping, wiretapping and deep packet analysis or inspections. Successful passive threats become passive attacks.

- **Threat Source**

A threat source could be regarded as an entity that desires to breach information or physical assets' security controls. The threat source ultimately aims to benefit from the breach for example financially. Identified main threat sources are depicted in figure 1 below:

- **Threat Actor**

A Cyber threat actor is an entity that actually performs the attack or, in the case of accidents, will exploit the accident. For example, if an organized crime group corrupts an employee, then the group is the *Threat Source* and the employee is the *Threat Actor*.

- **Vulnerability**

The intentions of threat sources and threat actors often materialise into attacks largely because they exploit weaknesses in the security controls. The weakness may include lack of software patching and poor configuration. Even sound technical controls may fail if social engineering attacks dupe staff with weak knowledge into breaching security.

1.1.5 Security Risk:

Security Risk refers to the probability that a threat will exploit a vulnerability to breach the security of an asset. It is important for States to manage cyber risks. However, as most readers know, functional IT systems operate with a degree of exposure to threats because full elimination of risk is either too expensive or undesirable. As such, a national cyber security strategy is the first step in ensuring that all stakeholders assume responsibility for and take steps to reduce risk.

1.1.6 Computer Emergency Response Team [CERT]:

A Computer Emergency Response Team [CERT] is basically an expert group which handles computer security incidents. They are human counterparts to anti-virus software in the sense that when new viruses or computer security threats are discovered, these teams document these problems and work to fix them. Being that these teams are made up of people who can react to new situations, they are much more capable of dealing with new virus threats than anti-virus programs would be by themselves.

According to Cert.org the primary goals of CERT include:

- Establishing a capacity to quickly and effectively coordinate communication among experts during security emergencies in order to prevent future incidents;
- Building awareness of security issues across the internet community.

Other functions include:

- Developing the cyber incident response plan;
- Identifying and classifying cyber- attack scenarios;
- Determining the tools and technology used to detect and prevent attacks;
- Promoting cyber-security awareness;

- Determining scope for investigations and conducting investigations within the scope once attack occurs.

1.1.7 Cyber Incident Response Team [CIRT]:

A Cyber Response Team is responsible for developing the written cyber incident response plan, investigating and responding to cyber-attacks in accordance with that plan. More specifically, some of the roles of CIRT are outlined below:

- Developing the cyber incident response plan;
- Identifying and classifying cyber- attack scenarios;
- Determining the tools and technology used to detect and prevent attacks;
- Promoting cyber-security awareness;
- Determining scope for investigations and conducting investigations within the scope once attack occurs.

1.2 ITU- IMPACT Alliance:

ITU and the International Multilateral Partnership against Cyber Threats (IMPACT) signed an agreement on September 3rd 2008, which made IMPACT the Global Cyber Security Agenda (GCA) operational home and had tasked IMPACT with the responsibility to operationalize the various initiatives under the GCA. The GCA is an international Cyber Security framework that was formulated following deliberations by more than 100 leading experts worldwide. The GCA contains many recommendations, which when adopted and appropriately implemented, would result in improved Cyber Security for the global community of nations.

Furthermore on September 8th 2011, IMPACT formally became the Cyber Security executing arm of ITU in a landmark agreement that was signed during the World Summit for Information Society 2011 (WSIS) Forum in Geneva, May 2011.

IMPACT is tasked by ITU with the responsibility of providing Cyber Security assistance and support to ITU's 193 Member States and also to other organizations within the UN system.

CHAPTER TWO

2.0 LITERATURE REVIEW:

In the 2013 edition of the Journal of Computer Engineering Volume *12*, the Internet is acclaimed as one of the fastest - growing areas of technical infrastructure development. In today's business environment, applications or technologies such as cloud computing, social computing, and next-generation mobile computing are fundamentally changing how organizations utilize information technology for sharing information and conducting commerce online. Today, more than 80% of total commercial transactions are done online, therefore, this field requires a high level of security for such online transactions. The scope of Cyber Security extends not only to the security of IT systems within the enterprise, but also to the broader digital networks upon which they rely including cyber space itself and critical infrastructures. Cyber security plays an important role in the development of information technology, enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being. Society has become dependent on cyber systems across the full range of human activities, including commerce, finance, health care, energy, entertainment, communications, and national defense.

Recent research findings also show that the level of public concern for privacy and personal information has increased since 2006. Internet users are worried that they give away too much personal information and want to be forgotten when there is no legitimate grounds for retaining their personal information.

Cyber security depends on the care that people take and the decisions they make when they set up, maintain, and use computers and the Internet.

Cyber-security covers physical protection (both hardware and software) of personal information and technology resources from unauthorized access gained via technological means.

According to IT Governance.co.uk, while rapid technological developments have provided vast areas of new opportunity and potential sources of efficiency for organizations of all sizes, these new technologies have also brought unprecedented threats with them. Albert Einstein was quoted as saying ―Problems cannot be solved with the same level of awareness that created them. The problem of End-User mistakes cannot evolve by adding more technology; it has to be solved by a joint effort and partnership between the Information Technology community of interest as well as the general business community along with the critical support of government or national regulatory authorities.

In recognition of the need to secure our Internet, the International Telecommunication Union (ITU), through its collaboration with International Multilateral Partnership against Cyber Threats (IMPACT) and partnerships with Member States around the world has been trying to mitigate these threats and attacks at various levels using various means and methodologies. Towards achieving its goal of safe cyberspace across the globe, The ITU has established a Regional Cyber Security Center (ITU-RCC) in Oman in collaboration with Oman Government, represented by the Information Technology Authority, within the framework of the ITU-IMPACT initiative. The vision for the ITU-RCC in Oman is to create a safer and cooperative cyber security environment within the Arab Region and strengthening the role of ITU in building confidence and security in the use of information and communication technologies in the region.

In the same vein, and in order to combat cyber threats, the Australian Cyber Security Centre (ACSC) was established by the Australian Government. The initiative is primarily to ensure that Australian networks are amongst the hardest in the world to compromise. The Centre brings together existing cyber security capabilities across Defense, the Attorney-General's Department, Australian Security Intelligence Organization, Australian Federal Police and Australian Crime Commission in a single location. It created a hub for greater collaboration and information sharing with the private sector, state and territory governments and international partners to combat the full breadth of cyber threats.

The ACSC is responsible for raising awareness of cyber security, reports on the nature and extent of cyber threats, encourages reporting of cyber security incidents, analyses and investigates cyber threats, coordinates national cyber security operations and capability, and leads the Australian Government's operational response to cyber incidents.

CHAPTER THREE

3.0 INFORMATION ANALYSIS:

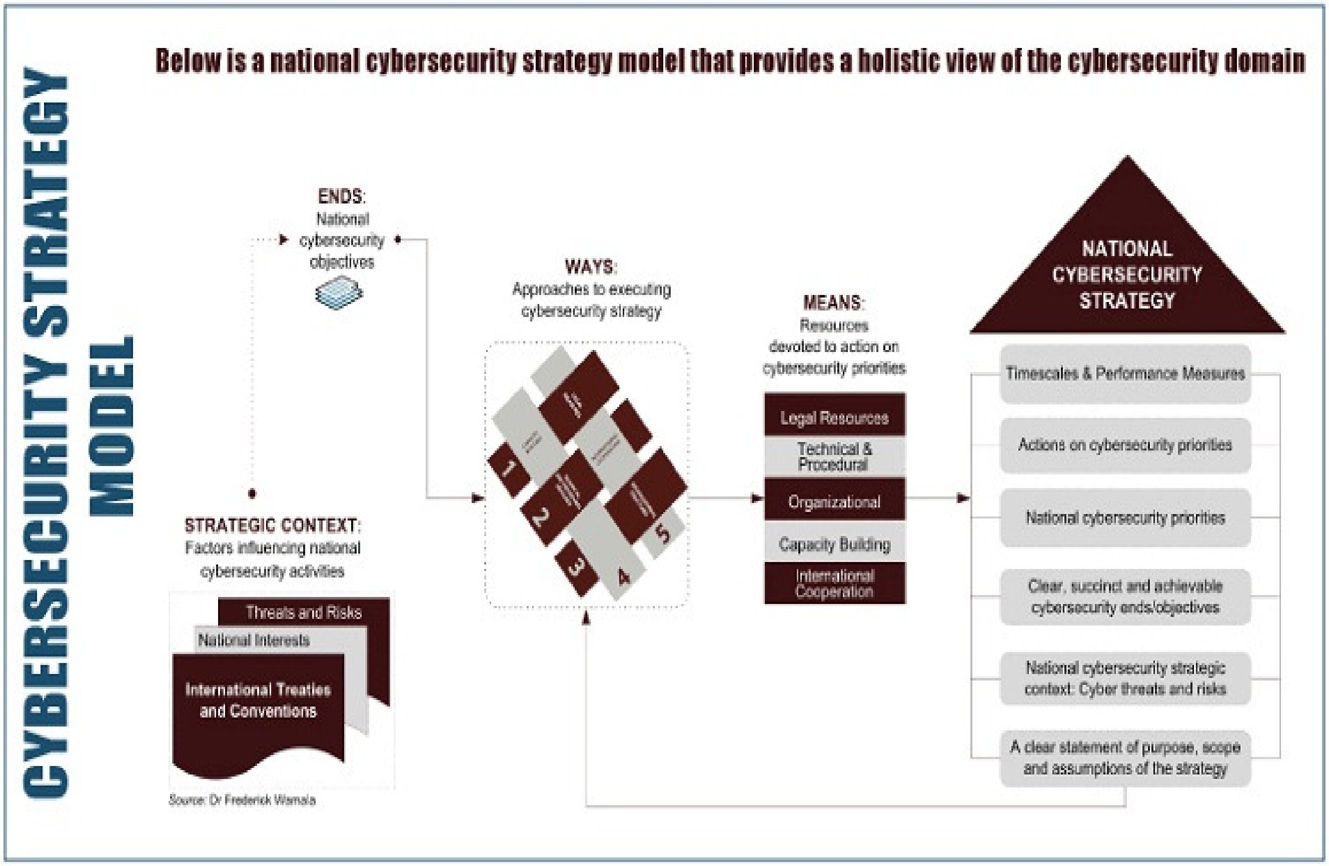
3.1 Cyber Security Strategy:

The ITU acknowledges that even prominent tech-savvy companies are not immune anymore to cyber threats as large companies like Google, RSA, Sony, Lockheed Martin, PBS, Epsilon, Citibank and even security companies, defense contractors and some of the brightest lights in technology have also fallen victim to such cyber-attacks. It is expected that the list may be longer as many organizations do not report cyber-attacks due to legal and reputational risk concerns. Worse still, a worrying number of organizations lack the capacity to detect attacks.

The UK National Cyber Security Strategy emphasizes the importance of partnerships among government, industry and academia, (both domestic and international), to meet the primary objective of the strategy which is "making the UK one of the most secure places in the world to do business in cyber space". Cyber threat is broad and complex, and focuses on networks and data in both the public and private domain largely to steal money and intellectual property. Threats will grow in frequency and sophistication because adversaries can afford new technology and techniques, including cloud and mobile computing, big-data analytics and artificial intelligence. But no single organization has the necessary capabilities to mitigate all the risks. Partnerships are therefore critical and must include information-sharing, governance, research and education. While today's threats are significant, threats to critical infrastructure will be even greater by 2020. At the rate industries are accelerating digitization to improve their services and reduce costs, there will be many new cyber threats to contend with.

ITU recognizes five (5) essential pillars that will enable the success of the strategy for the Global Cyber Security agenda. These pillars include:

- Legal measures;
- Technical and procedural measures
- Organizational structures
- Capacity building; &
- International Cooperation.


CYBERSECURITY STRATEGY MODEL
Below is a national cybersecurity strategy model that provides a holistic view of the cybersecurity domain
ENDS:
National cybersecurity objectives
WAYS:
Approaches to executing cybersecurity strategy
1
2
3
4
5
MEANS:
Resources devoted to action on cybersecurity priorities
Legal Resources
Technical & Procedural
Organizational
Capacity Building
International Cooperation
NATIONAL CYBERSECURITY STRATEGY
Timescales & Performance Measures
Actions on cybersecurity priorities
National cybersecurity priorities
Clear, succinct and achievable cybersecurity ends/objectives
National cybersecurity strategic context: Cyber threats and risks
A clear statement of purpose, scope and assumptions of the strategy
STRATEGIC CONTEXT:
Factors influencing national cybersecurity activities
Threats and Risks
National Interests
International Treaties and Conventions
Source: Dr Frederick Wamala

Source: ITU- National Cyber Security Strategy

3.2 ITU Cyber-Security Activities

- In 2003, world leaders at the World Summit on the Information Society (WSIS) entrusted *ITU as sole facilitator for WSIS Action Line C5 - "Building Confidence and Security in the use of ICTs".*
- Since the 2006 ITU Plenipotentiary Conference, ITU Secretary-General has set cyber security as one of his top three priorities.
- On 17 May 2007, in response to the decision of the ITU Membership and in fulfillment of ITU's role as sole facilitator for WSIS Action Line C5, ITU Secretary-General launched the *Global Cyber security Agenda (GCA)* – a framework for international cooperation in cyber security
- ITU World Conferences and the 2010 ITU Plenipotentiary Conference further strengthened the role of ITU in cyber security and endorsed the *GCA* as the ITU-wide strategy on international cooperation. The *GCA* is a set of defined challenges in five (5) broad domains: Legal, Technical, Organizational, Capacity Building and International Cooperation, and proposes solutions aimed at addressing these challenges within a framework of international cooperation and in collaboration with all relevant stakeholders. The *GCA* goes beyond listing the tasks to be done or the challenges to be faced. Rather, it proposes strategies and solutions developed with the support and participation of relevant stakeholders, while taking account of existing initiatives.

3.3 ITU Regional Cyber Security Center:

ITU and the International Multilateral Partnership against Cyber Threats (IMPACT) signed an agreement on September 3rd 2008, which made IMPACT the Global Cyber Security Agenda (GCA) operational home and executing arm on behalf of ITU. This was done at the cost of US$13m. The venture avails expertise and resources to detect, analyze and respond effectively to cyber threats to over 193 ITU Member States. The coalition is of particular benefit to countries that lack the resources to develop their own cyber response Centers.

Through these initiatives, Regional Cyber Security Center (ITU-RCC) have been established in the following Countries:

- **SULTANATE OF OMAN**

The ITU-IMPACT in collaboration with Information Technology of Authority (ITA) of Oman has established an ITU-RCC in Oman with a vision of creating a safer and cooperative cyber security environment in the Arab Region and strengthening the role of ITU in building confidence and security in the use of information and communication technologies in the region. The establishment of this Centre is in line with the objectives of the ITU Global Cyber security Agenda (GCA), and the ITU-IMPACT initiative, as well as to enhance capacity, capability, readiness, skill and knowledge in Cyber security at the cost of US$2m. It will act as ITU's Cyber security hub in the region localizing and coordinating Cyber security initiatives. This project is hosted, managed and operated by Oman National CERT (OCERT).

- **NIGERIA**

The first African Regional Cyber security Centre will be established in Nigeria. Memorandum of Understanding (MoU) with the Nigerian Communications Commission to set up a Regional Cyber security Centre in Nigeria was endorsed in July 2013.

The Centre is currently in its planning stage and will be hosted by the Nigerian Communications Commission.

3.4 Strategies for Effective Cyber Security Centre Operations:

The MITRE Corporation in its 2014 publication suggested ten strategies for effective Cyber security operation centers regardless of their size, offered capabilities or type of constituency served. These strategies include the following:

1. Consolidate functions of incident monitoring, detection, response, coordination, and computer network defense tool engineering, operation, and maintenance under one organization: the CSOC.
2. Achieve balance between size and visibility/agility, so that the CSOC can execute its mission effectively.
3. Give the CSOC the authority to do its job through effective organizational placement and appropriate policies and procedures.
4. Focus on a few activities that the CSOC practices well and avoid the ones it cannot or should not do.
5. Favor staff quality over quantity, employing professionals who are passionate about their jobs, provide a balance of soft and hard skills, and pursue opportunities for growth.

6. Realize the full potential of each technology through careful investment and keen awareness of—and compensation for—each tool's limitations.
7. Exercise great care in the placement of sensors and collection of data, maximizing signal and minimizing noise.
8. Carefully protect CSOC systems, infrastructure, and data while providing transparency and effective communication with constituents.
9. Be a sophisticated consumer and producer of cyber threat intelligence, by creating and trading in cyber threat reporting, incident tips and signatures with other CSOCs.
10. Respond to incidents in a calm, calculated, and professional manner.

3.5 Set up and Operations of a Cyber Security Centre:

A Cyber Security Center and Computer Emergency Response Team manage incidents, ensuring they are properly identified, analyzed, communicated, actioned/defended, investigated and reported. The Cyber Security Center and the Computer Emergency Response Team also monitor applications to identify possible cyber-attacks or intrusion.

Cyber Security Center and Computer Emergency Response Team typically are based around a security information and event management (SIEM) system which aggregates and correlates data from security feeds such as network discovery and vulnerability assessment systems; governance, risk and compliance (GRC) systems; web site assessment and monitoring systems, application and database scanners;

penetration testing tools; intrusion detection systems (IDS); intrusion prevention system (IPS); log management systems; network behavior analysis and threat intelligence; wireless intrusion prevention system; firewalls, enterprise antivirus and unified threat management (UTM). The SIEM technology creates a "single pane of glass" for the security analysts to monitor.

Cyber Security Centers are well protected with physical, electronic, computer, and personnel security. Centers are often laid out with desks facing a video wall, which displays significant status, events and alarms; ongoing incidents. Cyber Security Center staff include analysts, security engineers, and Cyber Security managers who should be seasoned IT and networking professionals. The staff are usually trained in computer engineering, cryptography, network engineering, or computer science and may have other independent information security certification governed by the International Information Systems Security Certification Consortium. Such credentials may include Certified Information Systems Security Professional (CISSP) or Global Information Assurance Certification (GIAC) is the leading provider and developer of Cyber Security Certifications

Processes and procedures within a Cyber Security Center should clearly spell out roles and responsibilities as well as monitoring procedures. These processes include business, technology, operational and analytical processes. They lay out what steps are to be taken in the event of an alert or breach including escalation procedures, reporting procedures, and breach response procedures.

3.6 Nigeria and the Global Cyber Security Agenda:

Nigeria like most other country recognizes the importance of cyber security and is actively involved in the implementation of the Global Cyber Security Agenda and has taken concrete steps to secure its cyber space.

In December, 2014 Nigeria published its National Cyber Security Strategy which clearly mapped out Nigeria's National Cyber Security Vision and the strategies for achieving this vision. Furthermore, in May, 2015 the President of the Federal Republic of Nigeria signed into law the Nigeria Cybercrime (Prohibition, Prevention, etc.) Act. The Act provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. The Act also ensures the protection of critical national information infrastructure, and promotes Cyber Security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights. The Nigeria National Computer Emergency Response Team (ngCERT) Operations Center was also officially commissioned in May, 2015 by the National Security Adviser.

CHAPTER FOUR

4.0 CONCLUSION

With the growing volume and sophistication of cyber-attacks, Cyber security is a necessary consideration for individuals and families, businesses, as well as governments. All hands must therefore be on deck to effectively combat this menace because Cyber-attacks by their very nature simply require a loop hole or entry point through which the attack can be replicated. Infected devices have a way of infecting other devices and compromised systems ultimately make everyone vulnerable.

The process of cyber security is continuous; it must be continuously updated. As new programs and cyber intruders develop and exploit new vulnerabilities in computer programs and systems, the network defenders have a continuous struggle to defeat their attempts. The basic principles for cyber security are the same as with physical and general security. It starts with a vulnerability assessment. The elements of vulnerability assessment include risk assessment and threat identification, and documenting the findings and preparing an action plan. Internet vulnerability is potentially one of the greatest threats to cyber security. Through a combination of e-mail, web browsers, and other programs, there are substantial security holes in any web-based system.

Governments around the world maintain an enormous amount of personal data and records on their citizens, as well as confidential government information, making them frequent targets. Yet many government entities are challenged with insufficiently secured infrastructure, lack of awareness, and competing funding and resource priorities. Better security helps government bodies provide reliable services to the public, maintain citizen-to-government communications, protect sensitive information as well as safeguard national security.

The ITU and IMPACT's initiative of establishing Cyber security centers in various regions of the world is an excellent means of addressing the growing cyber security incidences faced globally. Some countries like Unites States of America, Australia and Kenya, Canada, Ghana, Nigeria to mention a few have set up National Computer Emergency Response Teams and centers in their respective countries to combat cyber threats. The establishment of a regional Cyber Security Center in Nigeria would therefore be beneficial to Nigeria as a country and the rest of the African region in general.

Nigeria has taken concrete steps towards ensuring its cyber space is secure with recent publication of its National Cyber Security Strategy, the signing in Law of the Nigeria Cybercrime (Prohibition, Prevention, etc.) Act as well as the official commissioning of the Nigeria National Computer Emergency Response Team (ngCERT) Operations Center.

REFERENCES

Ravi Sharma, Study of Latest Emerging Trends on Cyber Security and its challenges to Society. International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June -2012 1 ISSN 2229-5518 IJSER © 2012

Abraham D. Sofaer, David Clark, Whitfield Diffie, Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy http://www.nap.edu/catalog/12997.htmlCyber Security and International Agreements, Internet Corporation for Assigned Names and Numbers pg185 -205

Thilla Rajaretnam Associate Lecturer, School of Law, University of Western Sydney, The Society of Digital Information and Wireless Communications (SDIWC), International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3): 232-240 2012 (ISSN: 2305-0012)

Thomas H. Karas, Lori K. Parrott , Judy H. Moore, Metaphors for Cyber Security, Sandia National Laboratories P.O. Box 5800 Albuquerque, NM 87185-0839

BinaKotiyal, R H Goudar. A Cyber Era Approach for Building Awareness in Cyber security for Educational System in India PritiSaxena, IACSIT International Journal of Information and Education Technology, Vol. 2, No. 2, April 2012
IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 2 (May. - Jun. 2013), PP 67-75

http://www.itu.int/en/ITUT/studygroups/com17/Pages/cybersecurity.aspx

Steffani A. Burd, The Impact of Information Security in Academic Institutions on Public Safety and Security: Assessing the Impact and Developing Solutions for Policy and Practice, October 2006.

International Telecommunications Commission [ITU] "Making the Online World Safer" document here: http://www.itu.int/net/itunews/issues/2011/05/38.aspx